Genetec™
Security Center.

Security Center Administrator Guide 5.11

Document last updated: June 12, 2023

Genetec™

Legal notices

Genetec Inc. distributes this document with software that includes an end-user license agreement and is furnished under license and may be used only in accordance with the terms of the license agreement. The contents of this document are protected under copyright law.

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

This publication may not be copied, modified, or reproduced in any form or for any purpose, nor can any derivative works be created therefrom without Genetec Inc.'s prior written consent.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein.

Genetec™, AutoVu™, AutoVu MLC™, Citywise™, Cloud Link Roadrunner™, Community Connect™, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™, KiwiSecurity™, Omnicast™, Privacy Protector™, Sipelia™, Stratocast™, Streamvault™, Streamvault Edge™, Synergis™, Valcri™, their respective logos, as well as the Mobius Strip Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.

Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

Patent pending. Genetec™ Security Center, Omnicast™, AutoVu™, Stratocast™, Genetec Citigraf™, Genetec Clearance™, and other Genetec™ products are the subject of pending patent applications, and may be the subject of issued patents, in the United States and in other jurisdictions worldwide.

All specifications are subject to change without notice.

Document information

Document title: Security Center Administrator Guide 5.11

Original document number: EN.500.003-V5.11.3.0(1)

Document number: EN.500.003-V5.11.3.0(1)

Document update date: June 12, 2023

You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.

About this guide

This guide provides the information you need to set up and configure your Security Center system. It explains the basic settings you must configure before your system can be used, as well as other settings you'll need to change such as adding additional users and resources (servers) to your system.

Notes and notices

The following notes and notices might appear in this guide:

- **Tip:** Suggests how to apply the information in a topic or step.
- **Note:** Explains a special case or expands on an important point.
- **Important:** Points out critical information concerning a topic or step.
- **Caution:** Indicates that an action or step can cause loss of data, security problems, or performance issues.
- **Warning:** Indicates that an action or step can result in physical harm, or cause damage to hardware.

IMPORTANT: Content in this guide that references information found on third-party websites was accurate at the time of publication, however, this information is subject to change without prior notice from Genetec Inc.

Contents

Preface

Part I: Introduction

Chapter 1: Security Center at a glance

Chapter 2: Tasks

Chapter 3: Reports

Chapter 4: Keyboard shortcuts

Part II: Common Security Center administration

Chapter 5: Entities

Chapter 6: Servers and roles

Chapter 7: Databases and networks

Chapter 8: High availability

Chapter 9: System automation

Chapter 10: Unit management

Chapter 14: Plugins

Chapter 15: Health monitoring

Chapter 16: System audits

Chapter 17: Mobile access

Chapter 18: Web access

Part III: System security

Chapter 19: Introduction to system security

Chapter 20: Partitions

Chapter 21: Users and User groups

Chapter 25: Fusion stream encryption

Part IV: Video

Chapter 26: Video at a glance

Chapter 27: Video deployment

Chapter 28: Cameras

Chapter 29: Video archives

Chapter 30: Cloud storage

Chapter 31: Troubleshooting and maintenance for video

Part V: Access control

Chapter 32: Access control at a glance

Chapter 33: Access control deployment

Chapter 34: Access control units

Chapter 35: Areas, doors, and elevators

Chapter 36: Cardholders

Chapter 37: Credentials

Chapter 38: Global cardholder management

Chapter 39: Import tool

Chapter 40: Testing your access control system

Chapter 41: Troubleshooting access control

Chapter 45: AutoVu third-party data exporter

Chapter 46: AutoVu fixed systems

Chapter 47: Free-Flow

Chapter 48: AutoVu mobile systems

Chapter 49: AutoVu Law Enforcement systems

Chapter 50: AutoVu City and University Parking Enforcement systems

Chapter 51: AutoVu Mobile License Plate Inventory systems

Chapter 52: Federated reads matching

Chapter 53: Troubleshooting ALPR

Part VII: Alarms and critical events

Chapter 54: Alarms

Chapter 55: Threat levels

Chapter 56: Zones and intrusion detection

Part VIII: Config Tool reference

Chapter 57: Entity types

Chapter 58: Role types

Chapter 59: Administration tasks

Chapter 60: Events and actions

Appendices

Part I

Introduction

This part includes the following chapters:

- Chapter 1, " Security Center at a glance " on page 2
- Chapter 2, " Tasks " on page 41
- Chapter 3, " Reports " on page 51
- Chapter 4, " Keyboard shortcuts " on page 70

1

Security Center at a glance

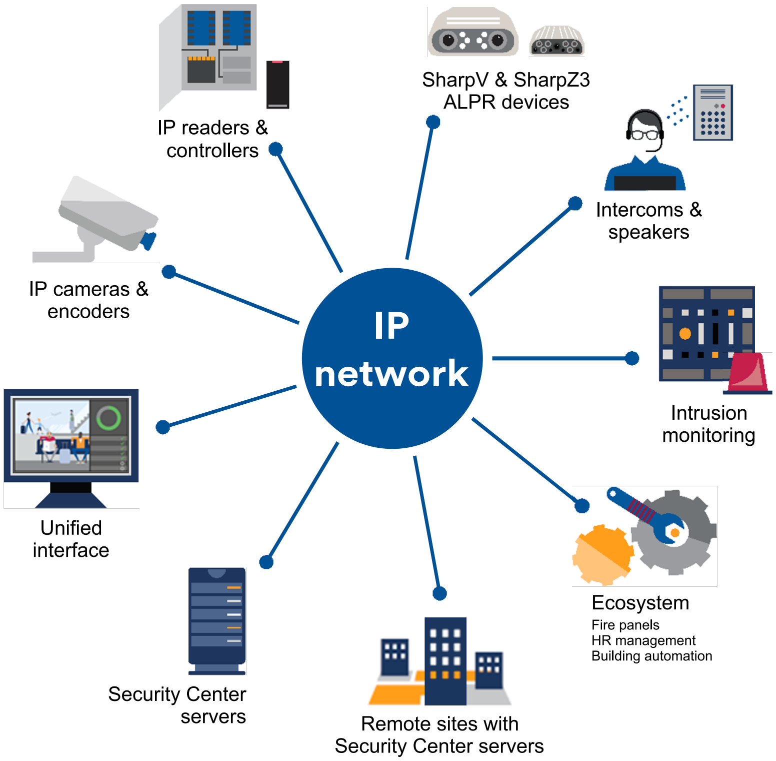
This section includes the following topics:

About Security Center

Security Center is a truly unified platform that blends IP video surveillance, access control, automatic license plate recognition, intrusion detection, and communications within one intuitive and modular solution. By taking advantage of a unified approach to security, your organization becomes more efficient, makes better decisions, and responds to situations and threats with greater confidence.

The Security Center unified security platform provides the following:

- One platform controlling and managing video, access control, and ALPR edge devices.
- One user interface for monitoring, reporting, and managing events and alarms for video surveillance, access control, and ALPR - Security Desk.
- One user interface for configuring video surveillance, access control, and ALPR - Config Tool.
- Unified live video viewing with video searches and video playback.
- Integration with a variety of third-party ecosystems and devices.



Security Center features are divided into four main categories: Common, Video surveillance (Omnicast™), Access control (Synergis™), and License plate recognition (AutoVu™).

Common/Core features

- Alarm management
- Zone management
- Federation™
- Intrusion panel integration
- Report management
- Schedule and scheduled task management
- User and user group management
- Windows Active Directory integration

- Programmable automated system behavior

Omnicast – Video surveillance features

- Full camera configuration and management
- View live and playback video from all cameras
- Full PTZ control using the PC or CCTV keyboard, or on screen using the mouse
- Digital zoom
- Motion detection
- Bookmark any important scene to ease future video archive search and retrieval
- Save and print video snapshots
- Search video by alarm, bookmark, event, motion, or date and time
- View all cameras on independent or synchronized timelines
- Visual tracking: follow individuals or moving objects across different cameras
- Export video
- Protect video against accidental deletion
- Protect video against tampering by using digital signatures
- Protect privacy of individuals in video

Synergis – Access control features

- Cardholder management
- Credential management
- Visitor management
- Door management
- Access rule management
- People counting

AutoVu – Automatic license plate recognition (ALPR) features

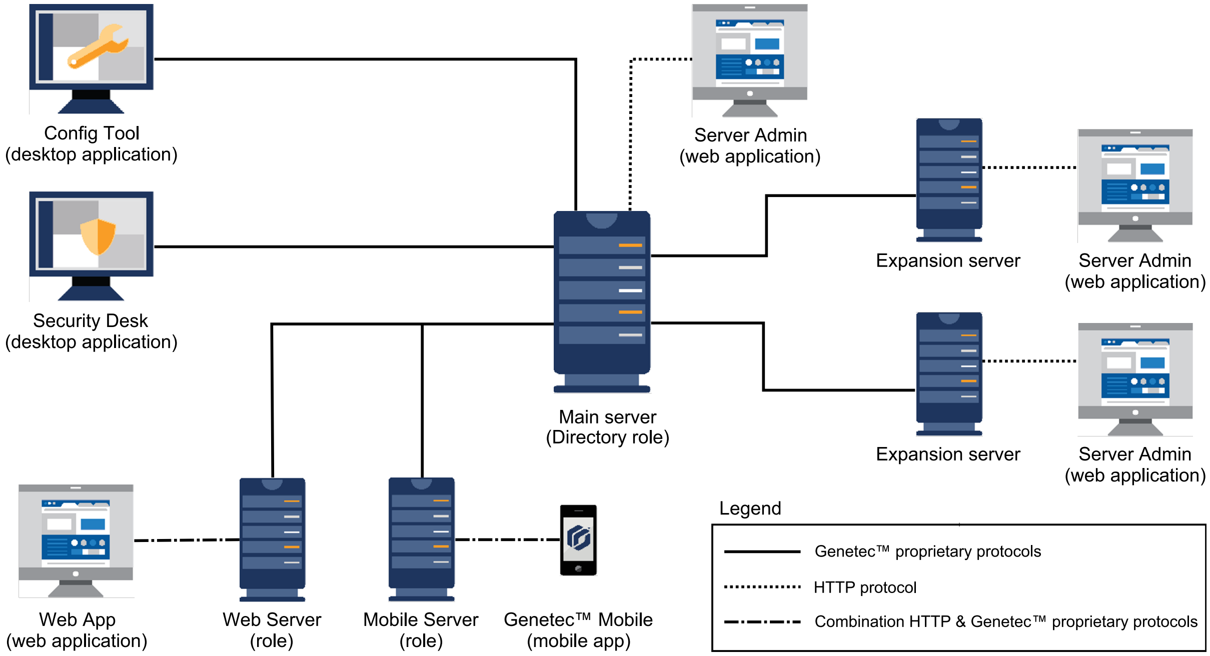
- Fixed and mobile (with Genetec Patroller™) ALPR solution management
- Automatic identification of stolen (or scofflaw) vehicles
- Enforcement of city parking regulations (not involving permits)
- Enforcement of parking lot regulations (involving permits)
- License plate inventory in large parking facilities

Security Center architecture overview

The Security Center architecture is based on a client-server model, where all system functions are handled by a pool of server computers distributed over an IP network.

Every Security Center system must have its own pool of servers. Their number can range from a single machine for a small system to hundreds of machines for a large-scale system.

NOTE: In the diagram, the blue server icons represent the Security Center servers, which also run the Config Tool and Security Desk client applications.



How Security Center is organized

Security Center is organized by tasks. All tasks can be customized and multiple tasks can be carried out simultaneously. You might not see all the tasks and commands described about Security Center, depending on your license options and user privileges. There are user privileges for each task, and for many commands in Security Center.

Tasks in the homepage are organized into the following categories:

- **Administration:** (Config Tool only) Tasks used to create and configure the entities required to model your system.
- **Operation:** Tasks related to day-to-day Security Center operations.
- **Investigation:** (Security Desk only) Tasks allowing you to query the Security Center database, and those of federated systems, for critical information.
- **Maintenance:** Tasks related to maintenance and troubleshooting.

Under each major category, the tasks are further divided as follows:

- **Common tasks:** Tasks that are shared by all three Security Center software modules. These tasks are always available regardless of which modules are supported by your software license.
- **Access control:** Tasks related to access control. Access control tasks are displayed with a red line under their icons. They are only available if *Synergis*™ is supported by your software license.
- **ALPR:** Tasks related to *automatic license plate recognition (ALPR)*. ALPR tasks are displayed with an orange line under their icons. They are only available if *AutoVu*™ is supported by your software license.
- **Video:** Tasks related to video management. Video tasks are displayed with a green line under their icons. They are only available if *Omnicast*™ is supported by your software license.

Logging on to Security Center through Config Tool

To log on to Security Center, you must open Config Tool and connect to the Security Center Directory.

Before you begin

Make sure that you have your username, password, and the name of the *main server* that you want to connect to.

What you should know

Logging on to Security Center typically involves a two-way authentication:

- The *Directory* (main server) must be authenticated by the party requesting the connection (the user).
- The party requesting the connection must be *authenticated* and *authorized* by the Directory.

Security Center offers different options to handle the authentication process. Your logon procedure might take on different paths depending on how the administrator has set up your system.

After you are logged on, you can disconnect from the Directory without closing Config Tool. Logging off without closing the application is helpful if you plan to log on again using a different username and password.

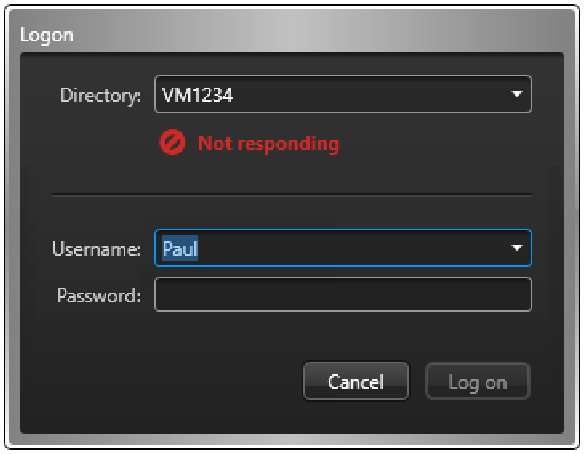
To log on to Security Center:

1 Open Config Tool by clicking **Start** > **All Programs** > **Genetec Security Center 5.11** > **Config Tool**.

2 In the *Logon* dialog box, enter the name or the IP address of your main server as **Directory**.

NOTE: If you are running Config Tool on the main server, you can enter `Localhost` instead of the main server name.

If the Directory is not responding, make sure the server is online and that your network configuration allows your computer to contact the main server (check hostname, IP address, and firewall rules).



Logon

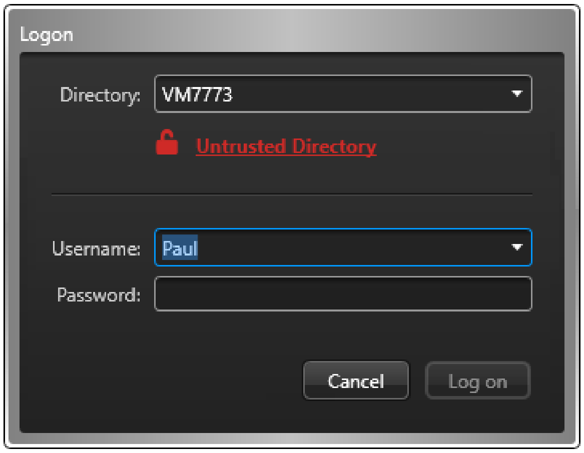
Directory: VM1234

Not responding

Username: Paul

Password:

If the Directory is not trusted, it could be the sign of a man-in-the-middle attack. Do not proceed unless you (or your administrator) are certain that the server you are contacting is secure.



Logon

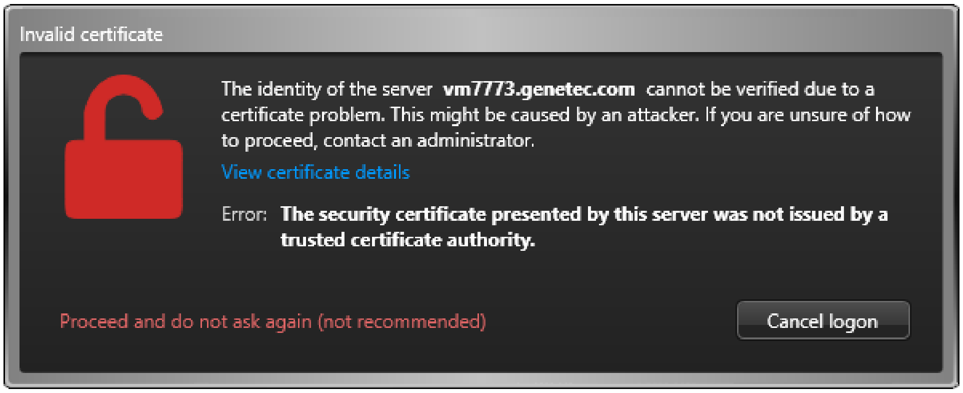
Directory: VM7773

Untrusted Directory

Username: Paul

Password:

Click the padlock icon for more information.



Invalid certificate

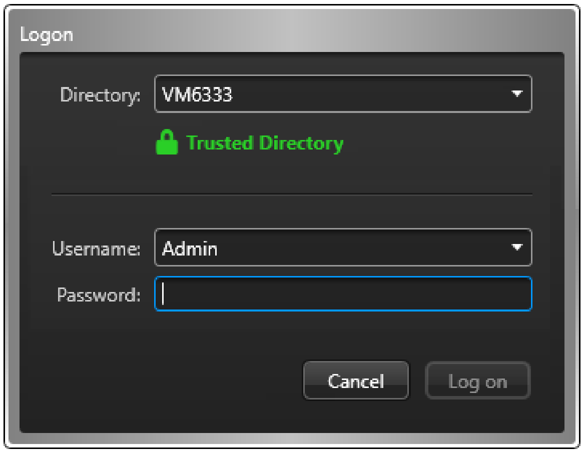
The identity of the server **vm7773.genetec.com** cannot be verified due to a certificate problem. This might be caused by an attacker. If you are unsure of how to proceed, contact an administrator.

View certificate details

Error: **The security certificate presented by this server was not issued by a trusted certificate authority.**

If your administrator confirms that you can trust that server, click **Proceed and do not ask again**. The certificate of that machine will be stored on your machine and future connections to that same Directory will be trusted, as long as its certificate does not change.

3 Enter your Security Center username and password.
If you have just installed Security Center, enter `Admin` with a blank password.



Logon

Directory: VM6333

Trusted Directory

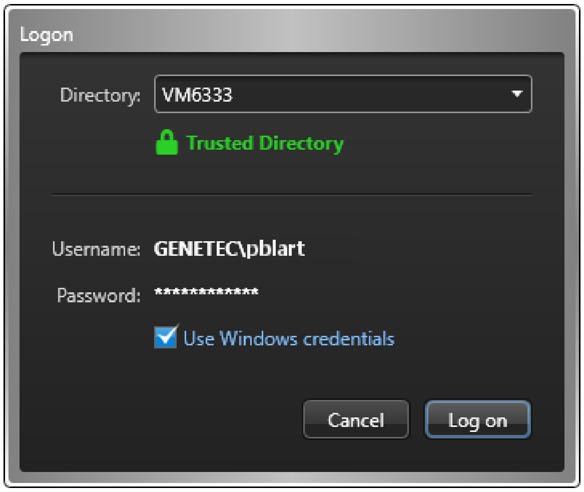
Username: Admin

Password:

If single sign-on is deployed using *third-party authentication*, you must click the **Sign in** button for your *identity provider*, or append your domain name to the end of your username, such as `Username@DomainName`. You will then be redirected to your identity provider for authentication. Skip to Logging on using web-based authentication on page 11.

4 To log on using your Windows user account, select **Use Windows credentials**.

This option is only available if Active Directory is set up on your system.



Directory: VM6333

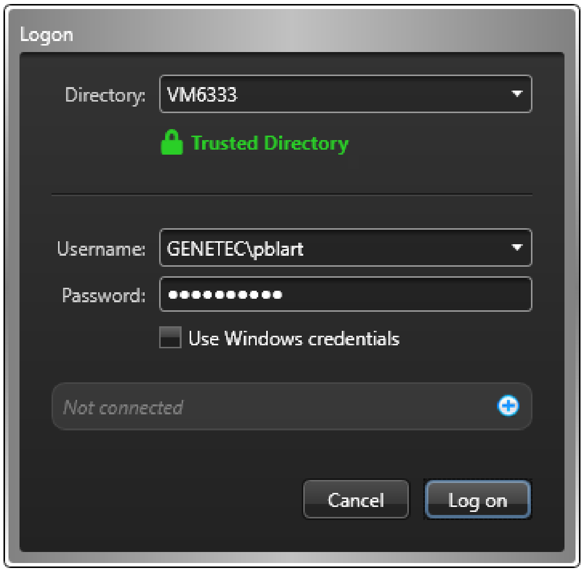
Trusted Directory

Username: GENETEC\pblart

Password: *************

☑ Use Windows credentials

NOTE: If your client workstation is not on the same domain as your server, or if you want to log on to Security Center with a different Windows account, you must clear the **Use Windows credentials** option and type your username in the format *DOMAIN\Username*.



Directory: VM6333

Trusted Directory

Username: GENETEC\pblart

Password: ●●●●●●●●●●

☐ Use Windows credentials

Not connected

5 Click **Log on**.

6 To log off, click the home (🏠) tab, and then click **Log off**.

Related Topics

What is Directory authentication? on page 462

Integration with Windows Active Directory on page 473

What is third-party authentication? on page 492

Customizing user logon options on page 452

Logging on using web-based authentication

If you click a **Sign in** button or Security Center detects that your domain has web-based authentication enabled, you will be redirected to a web form to enter your credentials.

Before you begin

Open Config Tool and enter the name of the **Directory** in the *Logon* dialog box.

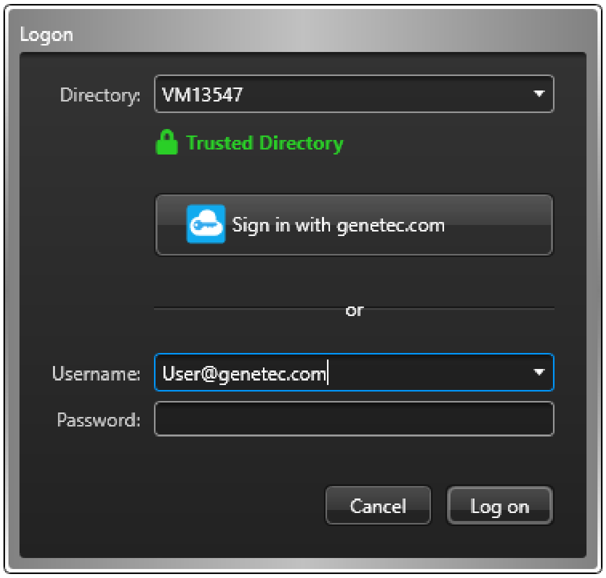
What you should know

Web-based authentication (also known as passive authentication) is when the client application redirects the user to a web form managed by a trusted identity provider. The identity provider can request any number of credentials (passwords, security tokens, biometric verifications, and so on) to create a multi-layer defense against unauthorized access. This is also known as multi-factor authentication.

NOTE: Config Tool remembers all valid logon parameters used and automatically calls up the parameters used for the last logon attempt.

To log on using web-based authentication:

1 In the **Username** field, enter your username followed by your domain name, in the format *Username@DomainName*, or click the **Sign in** button for your identity provider.



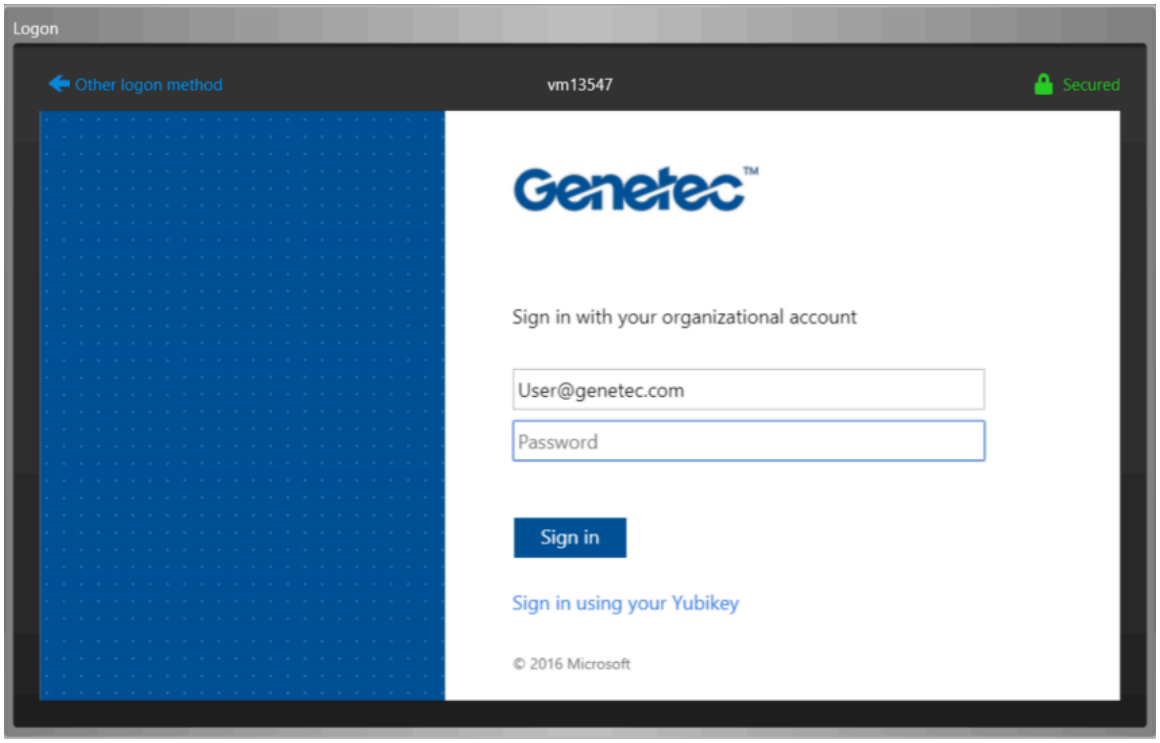
Directory: VM13547

Username: User@genetec.com

Password:

2 If you entered your username and domain, click the **Password** field or press the Tab key.

If Security Center detects that *web-based authentication* is enabled on your domain, you will be redirected to a web form. The following screen capture is an example. Your logon page might look different.



3 In the web form, enter the required information and click **Sign in**.

NOTE: You cannot log on as the built-in *Admin* user using web-based authentication. To log on as the *Admin* user, click **Other logon method** to go back to the Security Center *Logon* dialog box.

Closing Config Tool

You can close Config Tool and save your workspace for the next time you log on.

What you should know

There are also some options that you can customize for when you are closing Config Tool from the *Options* dialog box.

To close Config Tool:

1 In the upper-right corner of the Config Tool window, click **Exit** (⊗).

If you have unsaved tasks in your workspace, you are prompted to save them.

2 To automatically load the same task list the next time you open Config Tool, click **Save**.

Related Topics

Saving your workspace automatically when closing the client on page 13

Saving your workspace automatically when closing the client

When you close your client application, you are prompted to save unsaved changes to your workspace. You can configure your client application to save or discard unsaved changes automatically.

What you should know

This setting is saved with your user profile and applies to both Security Desk and Config Tool.

To save your workspace automatically when closing the client:

1 From the homepage, click **Options** > **User interaction**.

2 In the *On application exit* section, click **Save the task list** and select one of the following options:

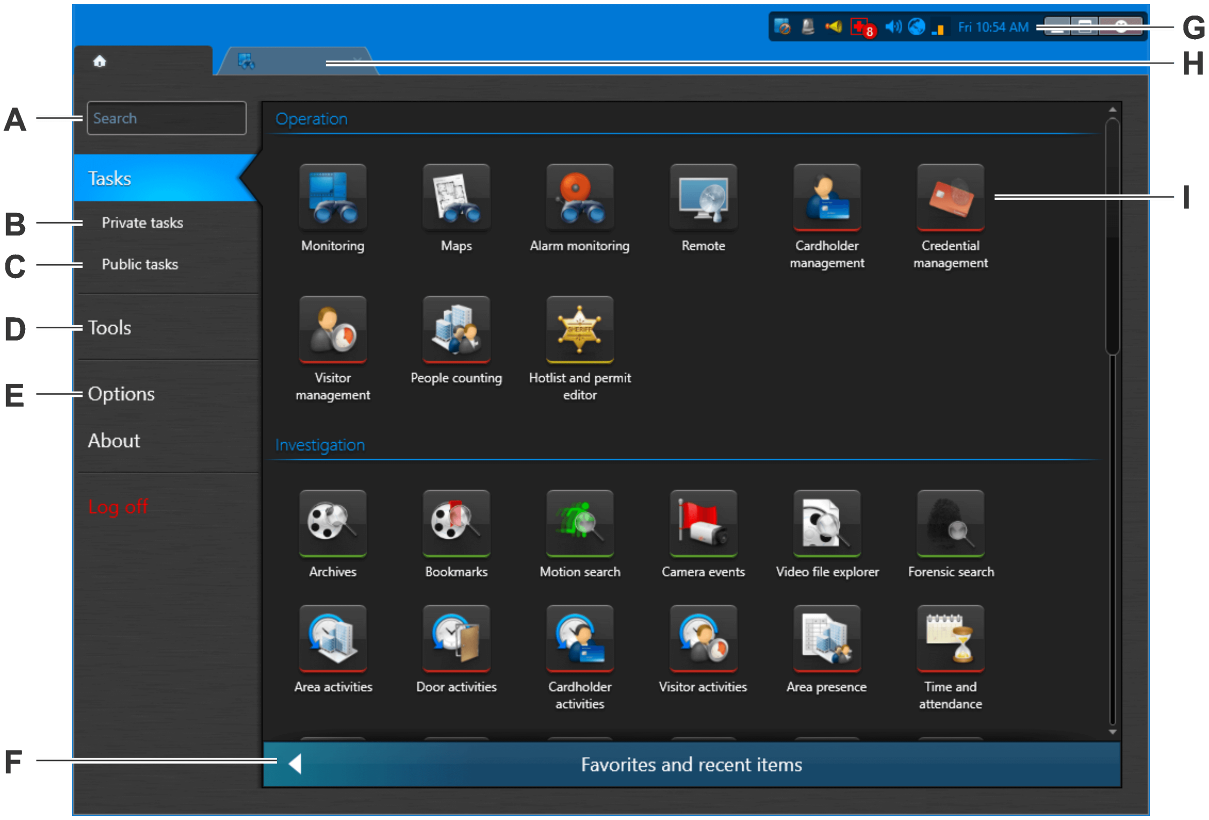
- **Ask user**: Always ask before saving your workspace.
- **Yes**: Always save the workspace without asking you.
- **No**: Never save the workspace.

3 Click **Save**.

Homepage overview

The homepage is the main page in Security Center.

To open the homepage, click the home tab (⌂).



A	**Search box**	Type the name of the task that you are looking for. All tasks containing that text in their category, name, or description, are shown.
B	**Private tasks**	Lists the saved tasks that you created and are only visible to your user.
C	**Public tasks**	Lists the saved tasks shared among multiple Security Center users.
D	**Tools**	Lists the standard Security Center tools, external tools, and applications you can start from your homepage.
E	**Options**	Click to configure the options for your application.
F	**Favorites** and **Recent items**	Lists the tasks and tools that you have used recently or added to your **Favorites**.
G	**Notification tray**	Displays important information about your system. Hover mouse over an icon to view system information, double-click to perform an action.
H	**Task tabs**	Shows the tasks that you have that open in individual tabs. Click to switch tasks.
I	**Tasks page**	Lists all tasks available to you. Select a task to open. If you have multiple instances of the task, you are asked to type a name.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

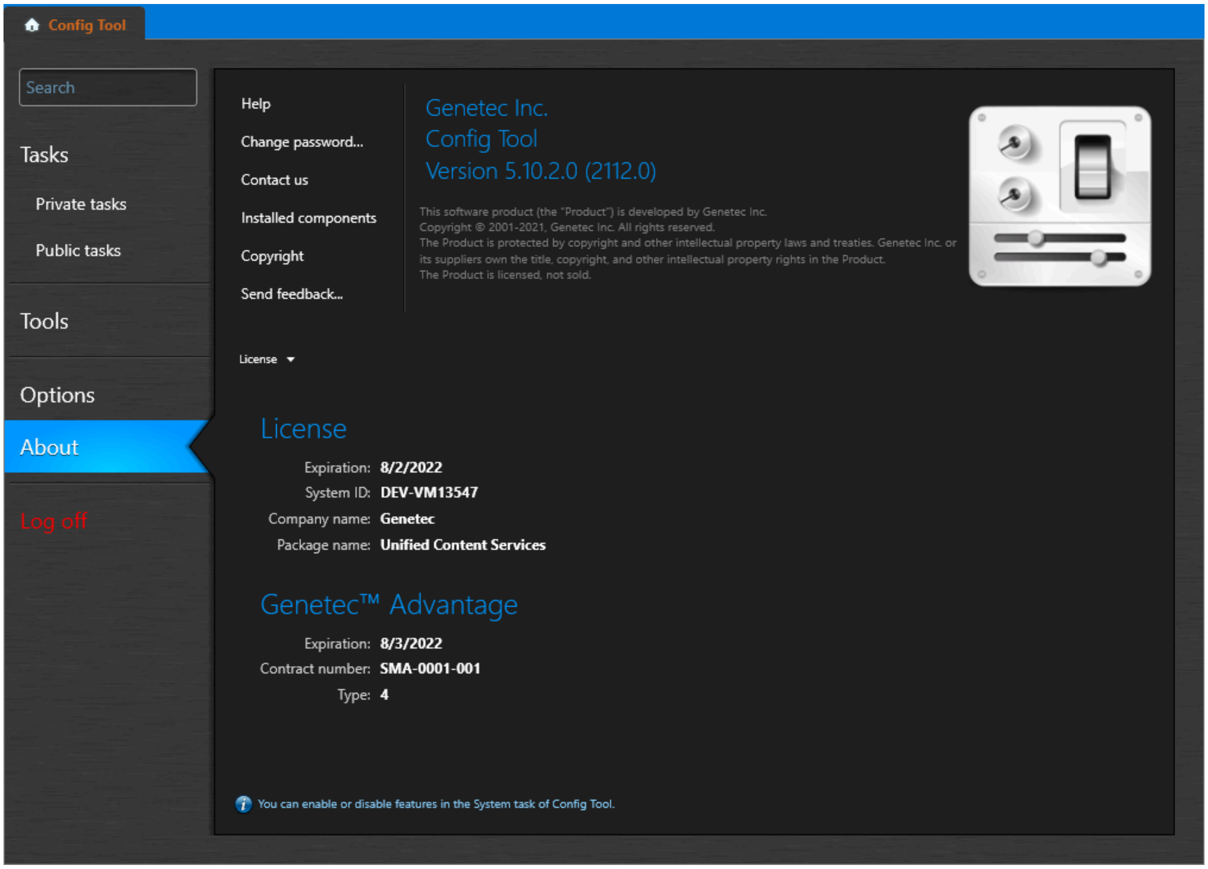
Related Topics

Configuring the notification tray on page 29
Saving tasks on page 44
Opening tasks on page 42
Shortcuts to external tools on page 38

Overview of the About page

The About page displays information regarding your Security Center software, such as your purchased license, license expiration date, Genetec™ Advantage contract number, software version, and so on.

All license options are either supported, unsupported, or limited by a maximum use count. For options with a maximum use count, Config Tool shows the current use vs. the maximum allowed.



Genetec Inc.
Config Tool
Version 5.10.2.0 (2112.0)

This software product (the "Product") is developed by Genetec Inc.
Copyright © 2001-2021, Genetec Inc. All rights reserved.
The Product is protected by copyright and other intellectual property laws and treaties. Genetec Inc. or its suppliers own the title, copyright, and other intellectual property rights in the Product.
The Product is licensed, not sold.

License

Expiration: 8/2/2022
System ID: DEV-VM13547
Company name: Genetec
Package name: Unified Content Services

Genetec™ Advantage

Expiration: 8/3/2022
Contract number: SMA-0001-001
Type: 4

You can enable or disable features in the System task of Config Tool.

The following tabs are available, depending on what your license supports:

- **License:** Indicates when your software license expires, and gives you the information you need to provide when contacting Genetec Technical Assistance Center: System ID, Company name, Package name, and your Genetec Advantage contract number.

  IMPORTANT: Thirty days before the expiry of either your license or your Genetec Advantage contract, you'll receive a message in Config Tool alerting you that your license or your Advantage contract is about to expire. Config Tool connects to GTAP to validate the Advantage contract.
- **Security Center:** This tab shows all generic Security Center options.
- **Synergis:** This tab shows all the access control options. It is shown only if *Synergis™ (access control)* is supported.
- **Omnicast:** This tab shows all the video options. It is shown only if *Omnicast (video surveillance)* is supported.
- **AutoVu:** This tab shows all the ALPR options. It is shown only if *AutoVu (ALPR)* is supported.
- **Plan Manager:** This tab shows the Plan Manager options.
- **Mobile:** This tab shows all the Security Center mobile and web access options.
- **Certificates:** This tab lists the *SDK certificates* included in this license key.
- **Purchase order:** This tab reproduces your order.

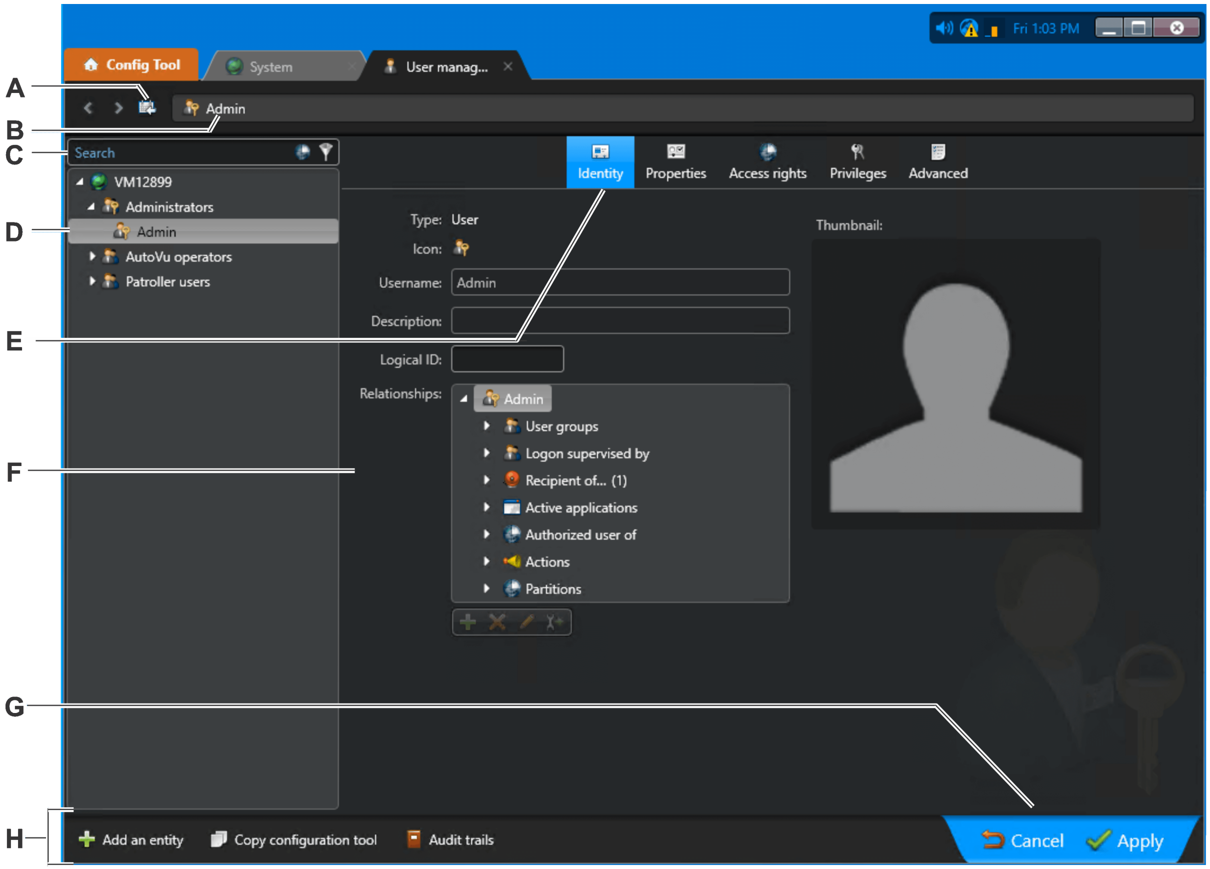
On the About page, the following buttons are also available:

- **Help:** Click to open the online help. You can also click F1.
- **Change password:** Click to change your password.
- **Contact us:** Click to visit GTAP or the GTAP forum. You need an Internet connection to visit these websites.
- **Installed components:** Click to view the name and version of all installed software components (DLLs).
- **Copyright:** Click to display software copyright information.
- **Send feedback:** Click to send us feedback.

Administration task workspace overview

Administration tasks are where you create and configure the entities required to model your system.

This section describes the common elements of most administration tasks. The *User management* task is used in the following example. You can open the *User management* task by typing its name in the search box on the home page.



Type: User

Icon:

Username: Admin

Description:

Logical ID:

Relationships: Admin

A	**Entity history**	Use these buttons to browse through recently used entities within this task.
B	**Current entity**	The icon and name of the selected entity is displayed here.
C	**Entity filter**	Type a string in this field and press Enter to filter the entities in the browser by name. Click *Apply a custom filer* (▽) to pick the entities you want to show in the browser.
D	**Entity browser**	Click an entity in the browser to show its settings on the right.
E	**Configuration tabs**	The entity settings are grouped by tabs.
F	**Configuration page**	This area displays the entity settings under the selected configuration tab.

G	**Apply/cancel changes**	You must *Cancel* or *Apply* any changes you make on the current page before you can move to a different page.
H	**Contextual commands**	Commands related to the selected entity are displayed in the toolbar at the bottom of the workspace.

Contextual commands in administration tasks

Commands related to the selected entity in the browser are displayed at the bottom of the task workspace in administration tasks.

The following table describes all the contextual commands in alphabetical order.

Icon	Command	Applies to	Description
	Activate role	All roles	Activates the selected role.
	Add a cardholder	Access rules and cardholder groups	Creates a cardholder and assign it to the selected entity.
	Add a credential	Cardholders	Creates a credential and add it to the selected cardholder.
✚	**Add an entity**	All entities	Creates an entity.
	Assign to new door	Access control units	Creates a door and assign it to the selected access control unit.
	Audit trails	All entities	Creates an Audit trails task for the selected entity to find out which users made changes on the system.
⚠	**Conflict resolution**	Active Directory role	Opens the Active Directory conflict resolution dialog box to resolve conflicts caused by imported entities.
❐	**Copy configuration tool**	All entities	Opens the Copy configuration tool.
	Creates an access rule	Areas, doors, elevators	Creates an access rule and assign it to the selected entity.
	Deactivate role	All roles	Deactivates the selected role.
✖	**Delete**	All entities	Deletes the selected entity from the system. Discovered entities can only be deleted when they are inactive.
✚	**Diagnose**	All roles, and some entities	Performs a diagnosis on the selected role or entity.
	Disable support logs	Access Manager and access control units	Disables support logs if requested by Genetec™ Technical Assistance.
	Enable support logs	Access Manager and access control units	Enables support logs if requested by Genetec Technical Assistance.

Icon	Command	Applies to	Description
	Health statistics	Roles and physical devices	Creates a Health statistics task for the selected entity to view the health status and availability of entities.
	Identify	Video units	Flashes an LED on the selected unit to help find it on a rack.
	Live video	Cameras	Opens a dialog box showing live video from the selected camera.
	Maintenance mode	Roles, physical devices, and alarms	Sets a role, device, or alarm in maintenance mode so that its downtime does not affect its availability calculation from the Health Monitor.
	Move unit	Video and access control units	Opens the Move unit tool, where you can move units from one manager to another.
	Ping	Video units	Pings the video unit to check if you can communicate with it. This is helpful for troubleshooting purposes.
	Print badge	Cardholders and credentials	Selects a badge template and print a badge for the selected cardholder or credential.
	Reboot	Video and access control units	Restarts the selected unit.
	Reconnect	Video units	Disconnects the selected video unit from the Archiver and then reconnect it to the Archiver.
	Run macro	Macros	Runs the selected macro.
	Trigger alarm	Alarms	Triggers the selected alarm so it can be viewed in Security Desk.
	Unit enrollment tool	Video and access control units	Opens the Unit enrollment tool, where you can find IP units connected to your network.
	Unit's web page	Video units	Opens a browser to configure the unit using the web page hosted on the unit.

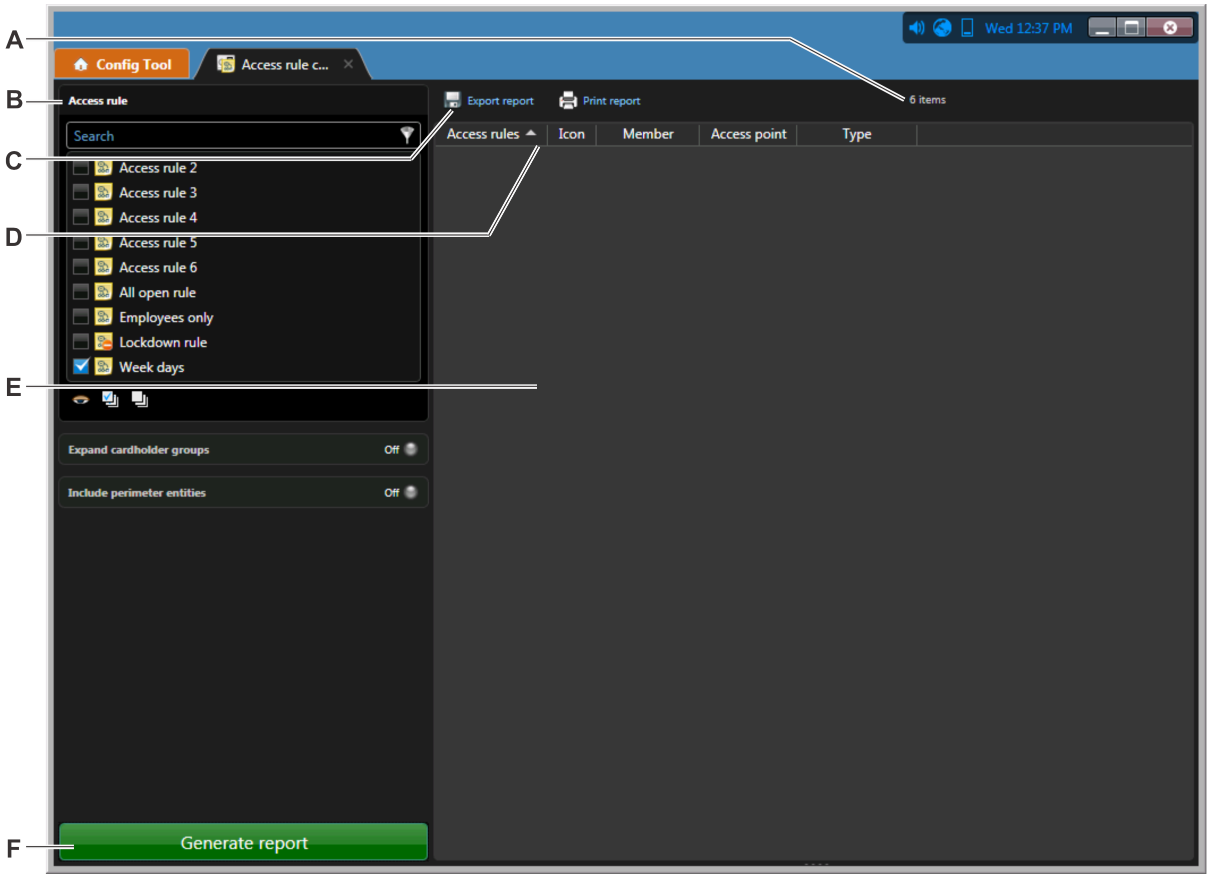
Related Topics

Finding out what changes were made to the system configuration on page 398
Resolving conflicts caused by imported entities on page 487
Copying configuration settings from one entity to another on page 82
Setting entities to maintenance mode on page 366
Creating macros on page 224
Testing alarms on page 1181

Maintenance task workspace overview

Maintenance tasks are where you generate customized queries on the entities, activities, and events in your Security Center system for maintenance and troubleshooting purposes.

This section takes you on a tour of the maintenance task layout, and describes the common elements of most maintenance tasks. The *Access rule configuration* task was used as an example. You can open the Access rule configuration task by typing its name in the *Search* box on the homepage.



Expand cardholder groups Off

Include perimeter entities Off

A	**Number of results**	Displays the number of returned results. A warning is issued when your query returns too many rows. If this happens, adjust your query filters to reduce the number of results.
B	**Query filters**	Use the filters in the query tab to set up your query. Click a filter heading to turn it on (●) or off. Invalid filters display as *Warning* or *Error*. Hover your mouse over the filter to view the reason it is invalid.
C	**Export/print report**	Click to export or print your report once it is generated.
D	**Select columns**	Right-click a column heading to select which columns to display.

E	**Report pane**	View the results of your report. Drag an item from the list to a tile in the canvas, or right-click an item in the list to view more options associated with that item, if applicable.
F	**Generate report**	Click to run the report. This button is disabled if you have not selected any query filters, or when you have invalid filters. While the query is running, this button changes to *Cancel*. Click *Cancel* to interrupt the query.

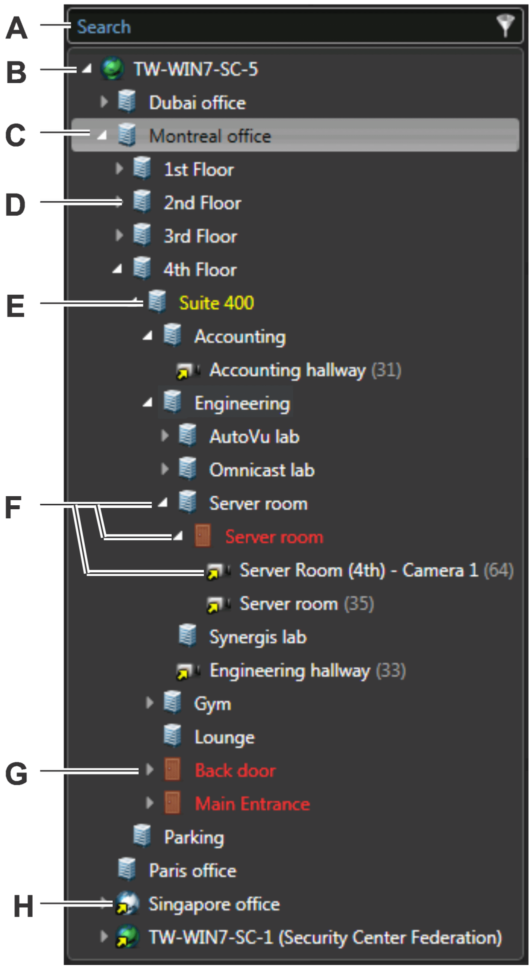
About the area view

Using the area view, you can find and view all the entities in your system quickly.

The *entities* in the area view are organized in a hierarchy (or *entity tree*) according to their logical relationships with *areas*. For example, the doors leading to an area, and other devices located within the area, such as cameras, are displayed below that area in the hierarchy as *child entities*.

From the area view, you can do the following:

- Find entities you want to view in the canvas.
- Drag multiple entities from the area view into the canvas.
- Rename local entities.
- Jump to entity configuration pages, if you have the required privileges.



A	**Search box**	Type in the *Search* box to find the entities containing that text in their category, name, or description.
B	**System entity**	The system entity (🌐) cannot be viewed in the canvas.
C	**Additional commands-**	Right-click an entity in the area view to use additional commands, such as creating or deleting entities, diagnosing the selected entity, launching a report on the selected entity, or refreshing the area view.

D	**Area entity**	Area entities (🏢) can represent a concept or physical location. It is a logical grouping.
E	**Yellow entity**	Whenever an entity name is displayed in yellow, it means that there is a problem with the settings.
F	**Arrow icons**	Click the arrows in the entity tree to show or hide child entities.
G	**Red entity**	Indicates that the entity is offline and the server cannot connect to it, or the server is offline.
H	**Federated entity**	All entities imported from *federated systems* are shown with a yellow arrow superimposed on the regular entity icon (🏢). They are called *federated entities*.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

About areas

In Security Center, an area entity represents a concept or a physical location (room, floor, building, site, and so on) used for grouping other entities in the system.

You can use areas to group system entities logically or to prevent unauthorized users from viewing selected system entities. A secured area is an area entity that represents a physical location where access is controlled. A secured area consists of perimeter doors (doors used to enter and exit the area) and access restrictions (rules governing the access to the area).

Related Topics

Organizing the area view on page 26
Defining who can access Security Center on page 417
About secured areas on page 792

Organizing the area view

As the system administrator, you need to create an area view structure that is easy for everyone to understand and navigate.

What you should know

You can re-organize the entities in the area view by dragging them to another area, selecting multiple entities at once and drag them to another area, renaming entities, and copying entities. You can also create and delete entities.

NOTE: You cannot edit the names of federated entities.

The way you structure the area view in Config Tool is also how it is displayed in Security Desk.

To organize the area view:

1. From the Config Tool home page, open the *Area view* task.

   NOTE: The area view *task* in Config Tool is the only place where you can change the area view structure. Do not confuse this administrative task with the area view *tab* found in most investigation tasks available in Security Desk.

2. To move entities under another area, do one of the following:

   - Select an area or entity, and then drag it to a different area.
   - Hold the Shift key, select multiple entities, and then drag them to a different area.

   The selected entities are now a child entities of that area (below that area in the hierarchy).

3. To rename an entity, select the entity, press **F2**, type a new name, and press Enter.

   TIP: You can rename any entity from the area view of any task as long as you have the administrative privilege to modify that entity.

4. To copy an entity into another area, hold the Ctrl key, and then drag the entity into that area.

   A copy of the entity is created under the area. If you copied an area under another area, all its child entities (entities below that area) are also copied.

5. If necessary, create new areas for grouping entities.
6. If necessary, delete entities.

Creating areas

To organize the area view, use areas to group entities based on their logical or physical relationship.

What you should know

- An area is a concept or a physical location (room, floor, building, site, and so on) that is used for the logical grouping of entities in the system.
- You can create areas anywhere in the area view hierarchy.

To create an area:

1. Open the *Area view* task.
2. Click a partition (🌐) or an area entity (🏢) you want to create the new area under.
3. Click **Add an entity** (➕) > **Area**.
4. Type a name for the area, and press Enter.

After you finish

If you are defining an area for access control, then secure the area.

Related Topics

Organizing the area view on page 26

Turning features on and off

To simplify your interface, you can turn off the features you are not using.

To turn features on or off:

1 Open the *System* task, click **General settings** > **Features**.

2 Select the features you want to use and clear the options of the features you want to turn off.

NOTE: You can only select the features that are supported by your license. Unsupported features are not listed.

3 Click **Apply**.

Example

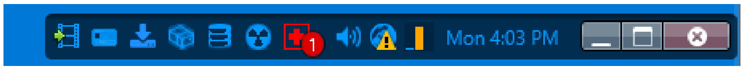
Active Directory integration is a feature that is supported by default in your license. However, if you do not plan on importing users from a Windows Active Directory, then you can turn off the Active Directory feature so the Active Directory role is no longer available.

Configuring the notification tray

You can choose which icons to display in the notification tray.

What you should know

The notification tray appears in the upper-right corner of the application by default.



The notification tray settings are saved as part of your user profile and apply to Security Desk and Config Tool.

Clicking on most of the notification tray icons opens a dialog box with more information. You can pin some of these dialog boxes to the side of your application workspace by clicking the pin (📌) button.

BEST PRACTICE: It is a good idea to show the icons that you use on a daily basis, so you can easily jump to the associated tasks.

To customize the notification tray icons:

1 From the homepage, click **Options** > **Visual**.

2 From the drop-down list beside the icons in the *Tray* section, select how you want to display each item:

- **Show:** Always show the icon.
- **Hide:** Always hide the icon.
- **Show notifications only:** Only show the icon when there is a notification.

3 Click **Save**.

Related Topics

Homepage overview on page 14

Backing up and restoring your user options on page 40

Notification tray icons

The notification tray contains icons that allow quick access to certain system features, and also displays indicators for system events and status information. The notification tray display settings are saved as part of your user profile and apply to both Security Desk and Config Tool.

The following table lists the notification tray icons, and what you can use them for:

Icon	Name	Description
9:53 AM	**Clock**	Shows the local time. Hover your mouse pointer over the clock to see the current date in a tooltip. You can customize the time zone settings.
📊	**Resources meter**	Shows the usage of your computer resources (CPU, memory, GPU, and network). Hover your mouse pointer over the icon to view the usage of resources in percentages. Click to open the *Hardware information* dialog box to view additional information and troubleshooting hints.

Icon	Name	Description
	Session info	Shows the current username and Security Center Directory name. Double-click to toggle between the long and short display. With the *View GUS notifications* privilege, the icon also behaves as follows: • If software updates are available, or there are other *GUS* notifications, the icon displays a yellow triangle (⚠). • If there are GUS errors, the icon displays a red triangle (⚠). Click to show the notifications and open GUS from Config Tool.
	Volume	Shows the volume setting (0 - 100) of Security Desk. Click to adjust the volume using a slider, or to mute the volume.
	Record types	Shows the number of *record types* for which the *record provider* is offline (4). In Security Center, a record type defines the data format and display properties of a set of records that you can share across the entire system through the Record Fusion Service role. Click to view which record types and providers are offline. For more information, see About data ingestion on page 255.
	System messages	Shows the number of current system messages (health issues, warnings, messages, and health events). Click to open the *System messages* dialog box to read and review the messages. If there are health issues, the icon turns red (6). If there are warnings, the icon turns yellow. If there are only messages, the icon turns blue. For more information, see Reviewing system messages on page 371.
	Upgrade firmware	Appears when there are unit firmware upgrades underway. The upgrade count is displayed over the icon. Click the icon to view the details.
	Database actions	Appears when there are database upgrades underway. The upgrade count is displayed over the icon. Click the icon to view the details.
	unit enrollment	Appears when there are newly added units in the system. The unit count is displayed over the icon. Click the icon to view the details.
	Updates	Appears when there are critical firmware updates required. Click the icon to view the details.
	Background process	Indicates that a process is running in the background, such as a video file export. Click the icon to view more details about the specific process that is running.
	Card requests	Shows the number of pending requests for credential cards to be printed (1). Click to open the *Card requests* dialog box and respond to the request. For more information, see Responding to credential card requests on page 873.
	Video file conversion	Shows the number of video file conversion requests that are pending and in progress (1), or complete ✓). Click to open the *Conversion* dialog box. For more information about converting G64 files to ASF or MP4 format, see the *Security Center User Guide*.
	Retrieve cloud archives	Shows the number of video requests from long-term Cloud Storage that are in progress (1), or complete ✓). Click to open the *Retrieve cloud archives* dialog box. For more information about requesting video archives from long-term Cloud storage, see the *Security Center User Guide*.

Related Topics

Creating databases on page 140
Deleting databases on page 141
Backing up databases on page 147
Restoring databases on page 151

Changing passwords

After you log on to Security Center, you can change your password.

What you should know

As a best practice, it is recommended to change your password regularly.

To change your password:

1 From the homepage, click **About**.

2 In the *About* page, click **Change password**.

3 In the *Change password* dialog box, enter your old password, then enter your new password twice.

4 Click **OK**.

Opening Security Desk from Config Tool

You can open the Security Desk application from the *Tools* page in Config Tool.

What you should know

When you open Security Desk application from Config Tool, you are logged on using the same credentials you are currently logged on with.

To open Security Desk from Config Tool:

- From the Config Tool home page, click **Tools** > **Security Desk** ().

Sending feedback

You can send feedback to Genetec Inc. if there is something you want to bring to our attention, such as an issue in the interface or a setting that is unclear.

To send feedback:

1 From the homepage, click **About** > **Send feedback**.

2 In the *Send feedback* dialog box, type your feedback.

3 To add attachments, click **Attachments** and select from the following options:

- To attach system information, select **System information**.
- To attach files such as a log file, select **Files**, click ➕, select a file, and click **Open**.
- To attach a screen capture of your current screen, select **Screenshots**, and click ➕.

  TIP: You can move the feedback dialog box over to the side and navigate to the relevant screen to take your screen capture while it is still open.

4 Click **Send**.

Collecting diagnostic data

For troubleshooting purposes, the *Diagnostic data collector* conveniently collects and packages system information so that you can easily send it to Genetec™ Technical Assistance Center.

Before you begin

To run the Diagnostic data collector:

- You must have Windows administrative privileges on your computer.
- You must have Security Center administrative privileges.

What you should know

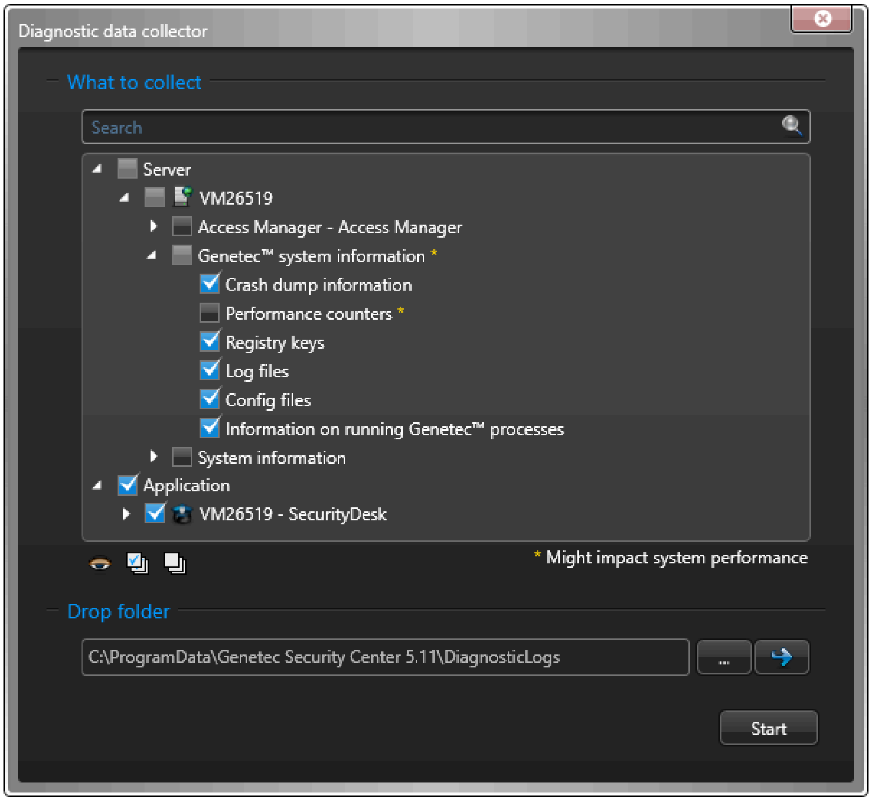
- The tool collects different types of system information (collection types), such as Genetec system information. You can expand these collections and select only a few items of interest.
- Running the Diagnostic data collector might temporarily impact system performance.

To collect diagnostic information:

1 From the homepage, click **Tools** > **Diagnostic data collector**.

The *Diagnostic data collector* dialog opens.

2 From the dialog box, expand the **Server** node and the **Application** node, and select the information types you want to collect.

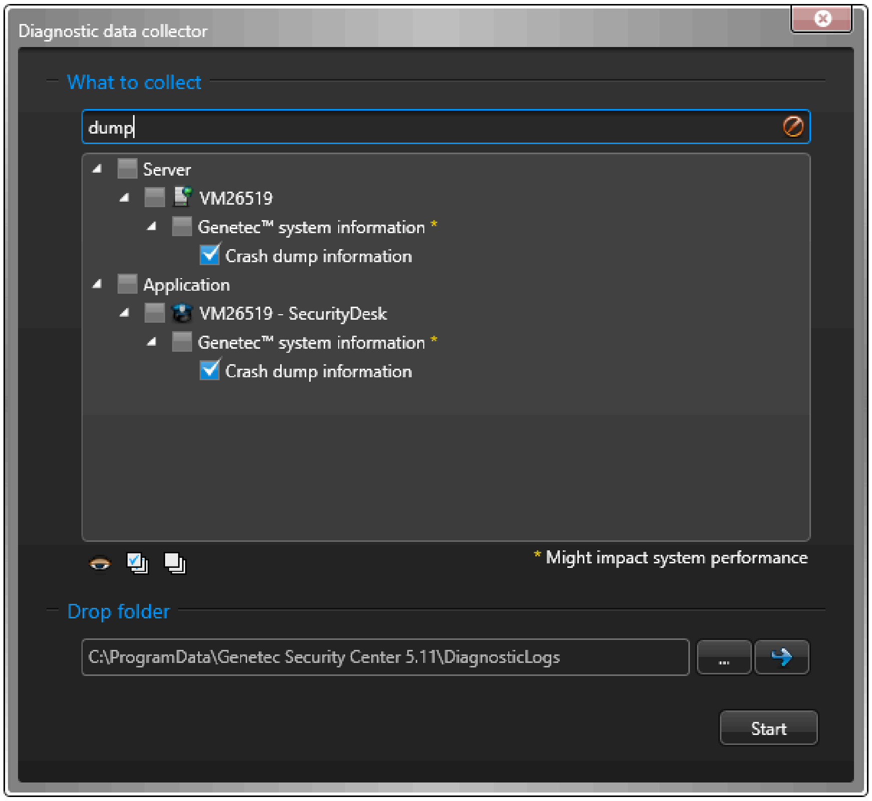


- ▨ Server
  - ▨ VM26519
    - □ Access Manager - Access Manager
    - ▨ Genetec™ system information *
      - ☑ Crash dump information
      - □ Performance counters *
      - ☑ Registry keys
      - ☑ Log files
      - ☑ Config files
      - ☑ Information on running Genetec™ processes
    - □ System information
- ☑ Application
  - ☑ VM26519 - SecurityDesk

Drop folder: C:\ProgramData\Genetec Security Center 5.11\DiagnosticLogs

From the **Server** hierarchy, select the information you want to gather regarding specific servers. From the **Application** hierarchy, select the information you want to gather regarding the application (Security Desk or Config Tool) you are running. If you want to gather information about another application, you must start the *Diagnostic data collector* from that application.

3 If you know what types of information you are interested in, you can use the **Search** field to filter the list of information types.



Diagnostic data collector

What to collect

dump

- □ Server
  - □ VM26519
    - □ Genetec™ system information *
      - ☑ Crash dump information
- □ Application
  - □ VM26519 - SecurityDesk
    - □ Genetec™ system information *
      - ☑ Crash dump information

* Might impact system performance

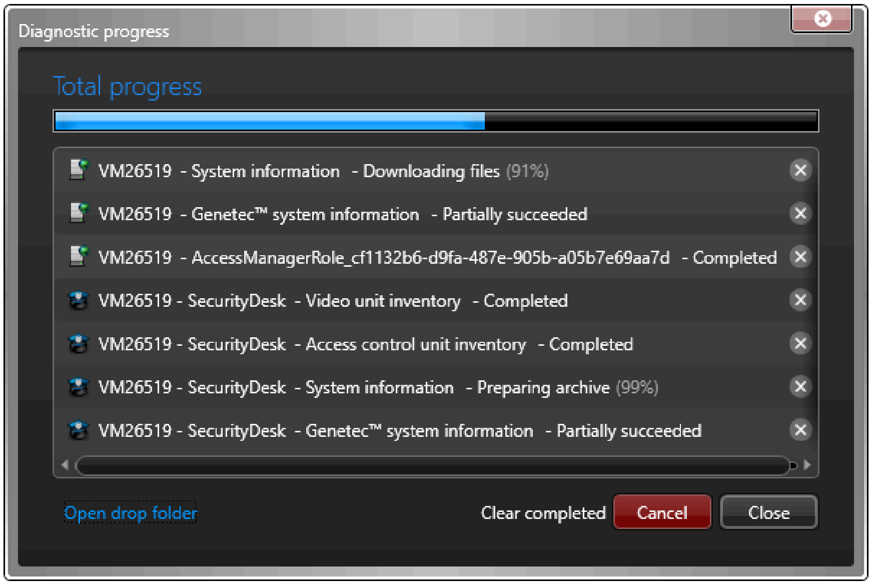
Drop folder

C:\ProgramData\Genetec Security Center 5.11\DiagnosticLogs

You can repeat this process multiple times. Your selections are cumulative.

4 (Optional) In the **Drop folder** field, enter the folder where you want the diagnostic data to be saved. The default is *C:\ProgramData\Genetec Security Center 5.11\DiagnosticLogs*.

5 Click **Start**.
The *Diagnostic progress* window opens.



Diagnostic progress

Total progress

VM26519 - System information - Downloading files (91%)
VM26519 - Genetec™ system information - Partially succeeded
VM26519 - AccessManagerRole_cf1132b6-d9fa-487e-905b-a05b7e69aa7d - Completed
VM26519 - SecurityDesk - Video unit inventory - Completed
VM26519 - SecurityDesk - Access control unit inventory - Completed
VM26519 - SecurityDesk - System information - Preparing archive (99%)
VM26519 - SecurityDesk - Genetec™ system information - Partially succeeded

6 Click **Open drop folder** to find the collected diagnostic data in a compressed file.

The file is named *Diagnostics_yyyy-mm-dd_hh-mm-ss.zip*, where *yyyy-mm-dd_hh-mm-ss* is the time when the file was created.

CAUTION: The resulting file can be very large and might affect the storage space of your hard drive. Remember to delete it when it is no longer needed.

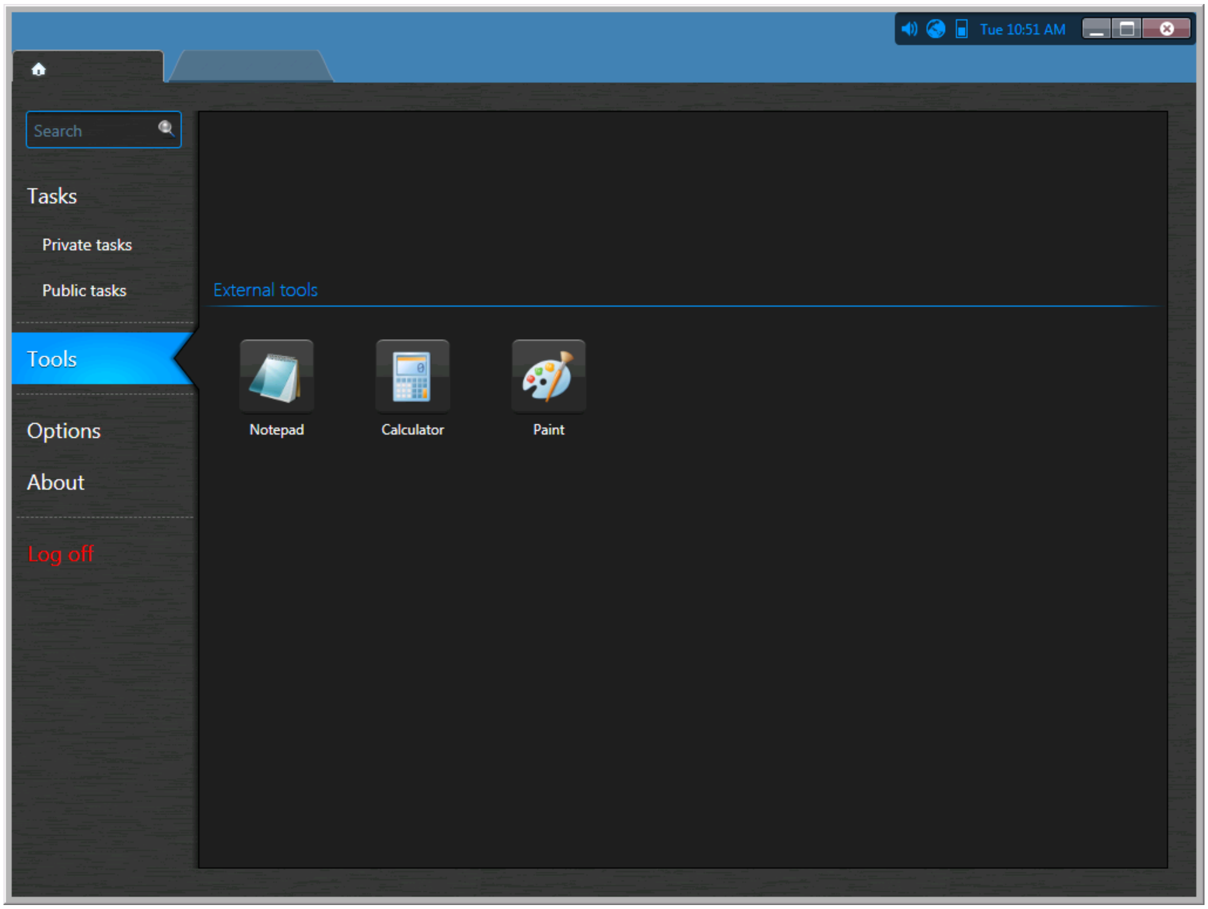
After you finish

Send the diagnostic information to Genetec Technical Assistance Center.

Shortcuts to external tools

You can add shortcuts to frequently used external tools and applications to the *Tools* page in Security Center, by modifying the *ToolsMenuExtensions.xml* file.

This file is located in *C:\Program files (x86)\Genetec Security Center 5.11* on a 64-bit computer, and in *C:\Program files\Genetec Security Center 5.11* on a 32-bit computer.



The original content of this file looks as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<ArrayOfToolsMenuExtension xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
 xmlns:xsd=http://www.w3.org/2001/XMLSchema>
    <ToolsMenuExtension>
    </ToolsMenuExtension>
</ArrayOfToolsMenuExtension>
```

Each shortcut is defined by an XML tag named <ToolsMenuExtension>. Each <ToolsMenuExtension> tag can contain four XML elements:

- <Name> – Command name displayed in the *Tools* page.
- <FileName> – Command to execute (executable file).
- <Icon> – (Optional) Alternate icon file (.ico). Use this element to override the default icon extracted from the executable file.
- <Arguments> – (Optional) Command line arguments when applicable.

All XML tag names are case-sensitive. You can edit this XML file with any text editor. Changes to this file only become effective the next time you launch Security Desk.

NOTE: If a full path is not provided in the <FileName> tag, the application is not able to extract the icon associated with the executable. In this case, explicitly supply an icon with the <Icon> tag.

Example

The following sample file adds the three shortcuts (*Notepad*, *Calculator*, and *Paint*) to the *Tools* page. The *Notepad* shortcut is configured to open the file *C:\SafetyProcedures.txt* when you click it.

```
<?xml version="1.0" encoding="UTF-8"?>
<ArrayOfToolsMenuExtension xmlns:xsi="http://www.w3.org/2001/XMLSchema-...>
    <ToolsMenuExtension>
        <Name>Notepad</Name>
        <FileName>c:\windows\notepad.exe</FileName>
        <Arguments>c:\SafetyProcedures.txt</Arguments>
    </ToolsMenuExtension>
    <ToolsMenuExtension>
        <Name>Calculator</Name>
        <FileName>c:\windows\system32\calc.exe</FileName>
    </ToolsMenuExtension>
    <ToolsMenuExtension>
        <Name>Paint</Name>
        <FileName>c:\windows\system32\mspaint.exe</FileName>
    </ToolsMenuExtension>
</ArrayOfToolsMenuExtension>
```

Backing up and restoring your user options

You can back up your Security Desk or Config Tool user options to an XML file and use it to restore your settings, either on a new workstation or on the same one following a reset of your machine.

What you should know

The backup includes all the user options listed in the *Options* window, except those for plugins. While Security Desk and Config Tool have different sets of user options, some apply to both applications. When restoring user options, common settings from the backup are applied to both Security Desk and Config Tool.

To back up the configuration for your user options:

1. From the homepage, click **Options**.
2. At the lower left of the window, click **Backup**.
3. In the dialog box that opens, choose a file name and click **Save**.

To restore the configuration for your user options:

1. From the homepage, click **Options**.
2. At the lower left of the window, click **Restore**.
3. In the dialog box that opens, select the file and click **Open**.
4. Restart the application to apply the changes.

   NOTE: If your user options are restored on a workstation running a different version of Security Desk or Config Tool than the one from where they were backed up, it might not work.

Related Topics

Customizing how entities are displayed in the canvas on page 87

Configuring the notification tray on page 29

Customizing report behavior on page 67

Customizing task behavior on page 50

2

Tasks

This section includes the following topics:

Opening tasks

To do most things in Security Center, you must first open your tasks.

What you should know

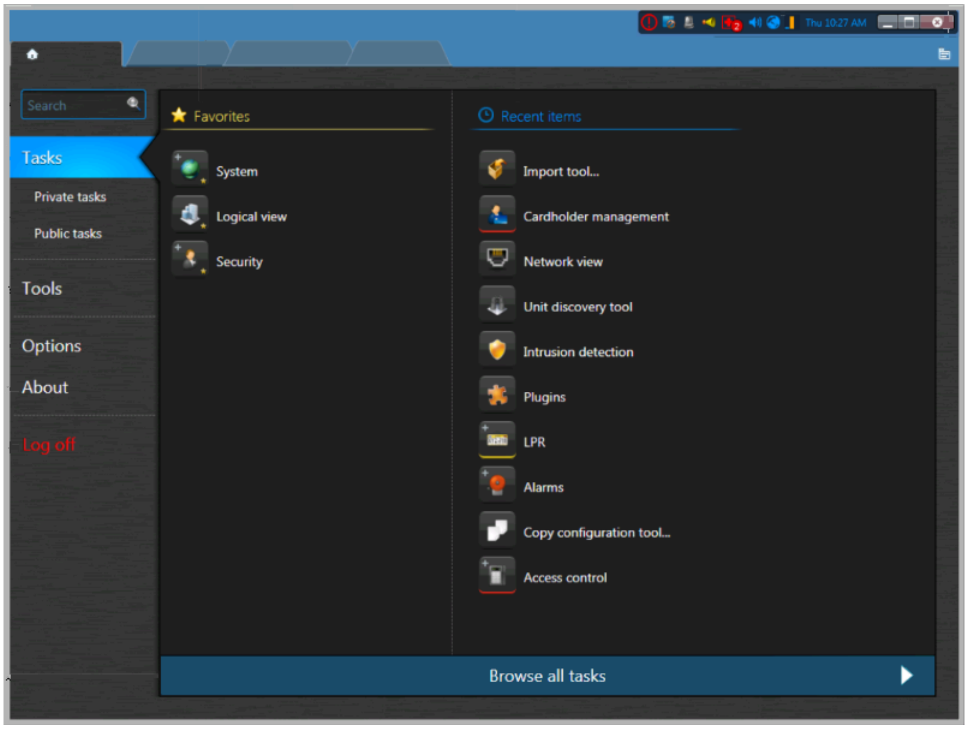
Some Security Center tasks can only have one instance, and other tasks can have multiple instances that can be duplicated. Single-instance tasks cannot be renamed.

To open a task:

1 From the homepage, do one of the following:
   - Enter the task name in the *Search* box.
   - Click the **Tasks** tab and browse all tasks.
   - To open a saved task, click the **Private tasks** or **Public** tab.

2 Click the task.
   NOTE: To open the task in the background, press Ctrl and click the task.
   If only one instance of the task is allowed, the new task is created.

3 If more than one instance of the task is allowed, enter the task name, and click **Create**.
   The new task opens and is added to your task list.



4 (Only Administration tasks) If the task contains more than one entity view, select a view to configure.
   Tasks that allow you to configure more than one entity are indicated with a plus sign on the task icon.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

Related Topics

Homepage overview on page 14

Saving tasks

You can save your tasks in a private task list that only you can access, or in a public task list that everyone can access.

What you should know

When you save a task, the query filter settings, the task layout (report pane column order, canvas layout, and so on), and the entities displayed in each tile are also saved.

NOTE: The query results are not saved. They are regenerated every time you run the query.

The benefits of saving a task are as follows:

- You can close your task, and reload it with the same layout when you need it.
- You can share public tasks with other users.
- You can use public tasks as a report template with the *Email a report* action.

To save a task:

1 Right-click the task tab, and click **Save as**.

NOTE: The **Save as** button is only available if your report query filters are valid. You know that your query is valid when the **Generate report** button is activated.

2 In the *Save task* dialog box, select how you want to save the task:

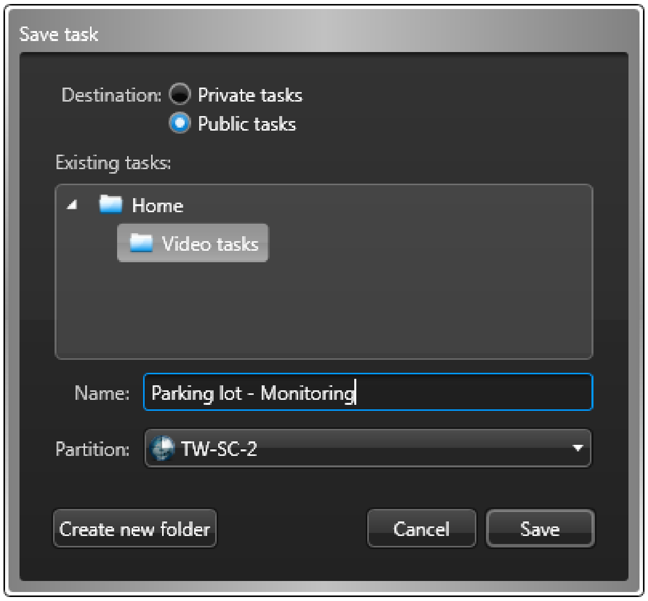
- **Private tasks:** A private task is a saved task that is only visible to the user who created it.
- **Public tasks:** A public task is a saved task that can be shared and reused among multiple Security Center users.

3 (Optional) To save the task in a folder on the *Private tasks* or *Public tasks* page, click **Create new folder**, type a name for the folder, and then click **Create**.

If you select the **Home** folder, or if you do not select a folder, the task is saved on the main page of the *Private tasks* or *Public tasks* page.

4 Enter a name for the saved task, or select an existing one to overwrite it.

Example: You can save a monitoring task that displays your parking lot cameras with the name *Parking lot - Monitoring*, or save an investigation task that searches for video bookmarks added within the last 24 hours with the name *Today's bookmarks*.



Destination: ○ Private tasks ● Public tasks

Name: Parking lot - Monitoring

Partition: TW-SC-2

5 (Only public tasks) Select the *partition* that you want the task to belong to.

   Only users that are members of the partition can view or modify this public task.

6 Click **Save**.

After you finish

- To save changes you make to the task, right-click the task tab, and click **Save**.
- If you change the task layout (for example, resize or hide report columns), you can revert to the layout used when the task was saved by right-clicking the task tab, and clicking **Reload**.

Related Topics

Homepage overview on page 14

Organizing your saved tasks

If you have many saved private tasks or public tasks in Security Desk or Config Tool, you can organize them in folders to easily find them.

What you should know

A private task is a saved task that is only visible to the user who created it. A public task is a saved task that can be shared and reused among multiple Security Center users.

To organize your saved tasks:

1. From the home page in Security Desk or Config Tool, click **Private tasks** or **Public tasks**.
2. To move a task to a folder, do the following:
   a) Right-click a task, and then click **Move**.
   b) In the *Move to* dialog box, click **Create new folder**.
   c) Enter a name for the folder, and then click **Create**.
   d) In the *Move to* dialog box, select the new folder, and then click **Move**.

   To rename the folder, right-click the folder and click **Rename**.

   NOTE: Folders are only created when you move a task of another folder into them. You cannot create empty folders.
3. To move a folder, do the following:
   a) Right-click a folder, and then click **Move**.
   b) In the *Move to* dialog box, select an existing folder, or create a new folder and select it, then click **Move**.
4. To sort the tasks, right-click a folder, click **Sort**, and then select one of the following options:
   - **Sort by type:** Sort the saved tasks that are not in folders by their task type.
   - **Sort by name:** Sort the folders and saved tasks in alphabetical order.
5. To delete a folder, right-click the folder and click **Delete**.

Adding tasks to your Favorites list

You can add tasks and tools to your *Favorites* so they are listed beside the *Recent items* in your home page instead of the full task list.

What you should know

The tasks you add to the *Favorites* list are specific to your user account. The tasks that appear in the *Favorites* list do not appear in the *Recent items* list.

To add a task to your *Favorites* list:

1 Do one of the following:

- On the home page, move the mouse pointer over a task, and click **Add to Favorites** (☆).
- On the home page, drag a task from the **Recent items** list into the **Favorites** list.
- Right-click the task tab, and click **Add to Favorites**.

2 To remove a task from the **Favorites** list, do one of the following:

- On the home page, move the mouse pointer over a task, and click **Remove from Favorites** (★).
- Right-click the task tab, and click **Remove from Favorites**.

Hiding the *Favorites* and *Recent items* lists from your homepage

You can turn off the display of the **Remove from Favorites** and *Recent items* lists in your homepage so the full task list is always displayed instead.

What you should know

When you turn off the display of the *Favorites* and *Recent items* lists in your homepage, the system does not forget the items that are registered in those lists. Even when this feature is turned off, the system continues to keep track of your recently used items.

To hide the *Favorites* and *Recent items* lists from your home page:

1 From the homepage, click **Options** > **Visual**.

2 Clear the option **Display recent items and favorites in home page**.

3 Click **Save**.

From now on, only the full task list will be displayed when you click **Tasks** from the homepage.

Sending tasks

If you have selected specific entities to monitor or if you have configured specific query filters for an investigation task, you can share the task layout with another user or a Security Desk monitor by sending the task.

Before you begin

By default, when a task is received a confirmation window appears on the workstation, and a user must accept the task before it loads in Security Desk. If you are sending tasks to a Security Desk monitor and do not want the confirmation window to appear, disable the **Ask for confirmation when opening tasks sent by other users** option in the *Options* dialog box on the receiving workstation.

To send a task, the recipients must be online. If you are sending a task to a Security Desk monitor, a user must be logged on at that workstation.

What you should know

Sending tasks to a Security Desk monitor is typically used for workstations with multiple monitors, such as a video wall. With this feature, you can send a task directly to a specific monitor on the wall, without requiring intervention from an operator.

To send a task:

1. Open the task you want to send.
2. Configure the task.

   Example: You can modify the tile layout, display certain cameras, configure query filters, add entities to be monitored, and so on.
3. Right-click the task tab, and then click **Send**.
4. In the *Send task* dialog box.
5. Select whether to send the task to a **User** or a Security Desk **Monitor**.
6. In the **Select destination** list, select which users or monitors to send the task to.
7. (Optional) If you are sending the task to a user, write a message in the **Message** field.
8. Click **Send**.

If the **Ask for confirmation when opening tasks sent by other users** option is enabled on the receiving workstation, the confirmation request appears and the recipient must accept the task before it loads.

Moving the taskbar

You can configure the taskbar to appear on any edge of the application window. You can also set it to auto-hide and only appear when you hover your mouse over the taskbar location.

What you should know

When you auto-hide the taskbar, the notification tray is also hidden. These settings are saved as part of your user profile and apply to Security Desk and Config Tool.

To change the taskbar position:

1 From the homepage, click **Options** > **Visual**.

2 From the **Taskbar position** list, select the edge where you want the taskbar to appear.

3 To auto-hide the taskbar, select the **Auto-hide the taskbar** option.

4 To show the current task name when *task cycling* is enabled and the taskbar is hidden, select the **Show task name in overlay** option.

5 Click **Save**.

Customizing task behavior

Once you are familiar with how to work with tasks in Security Center, you can customize how the system handles tasks, from the *Options* dialog box.

What you should know

The task settings are saved as part of your Security Center user profile and apply to Security Desk and Config Tool.

To customize task behavior:

1. From the homepage, click **Options** > **User interaction**.
2. In the *System messages* section, set the following options as desired:
   - **Ask for a name when creating a task:** Select this option if you want Security Desk to ask you for a name every time you create a task that accepts multiple instances.
   - **Ask for confirmation before closing a task:** Select this option if you want Security Desk to ask for confirmation every time you remove a task from the interface.
   - **Ask for confirmation when opening tasks sent by other users:** Select this option if you want Security Desk to ask for confirmation every time you open a task sent by another user.
3. In the *Reload task* section, specify how you want Security Desk to behave when someone updates a *public task* you currently have open:
   - *Ask user*. Ask you before loading the updated task definition.
   - *Yes*. Reload the task without asking.
   - *No*. Never reload the task.
4. Click **Save**.

Related Topics

Backing up and restoring your user options on page 40

3

Reports

This section includes the following topics:

About visual reports

In Security Desk, dynamic charts and graphs provide visual data that can be used to perform searches, investigate situations, and identify activity patterns.

Visual reports can display data in a graph or chart format along a specified axis by using lines or bars to visually represent the report data. The X axis represents all the labels (group by), and the Y axis shows the total number of instances relative to the X axis.

On the X axis, two types of grouping can be achieved:

- **Nominal values:** Can separate the data in multiple columns on the X axis. For example, the X axis values can be sorted by the number of instances, and the user can choose the grouping (**Top 3**, **Top 5**, or **Top 10**).
- **Dates:** Can separate the X axis based on a timeline. For example, the user can change the date interval grouping (**Hour**, **Day**, **Week**, **Month**, or **Year**).

Visual chart types

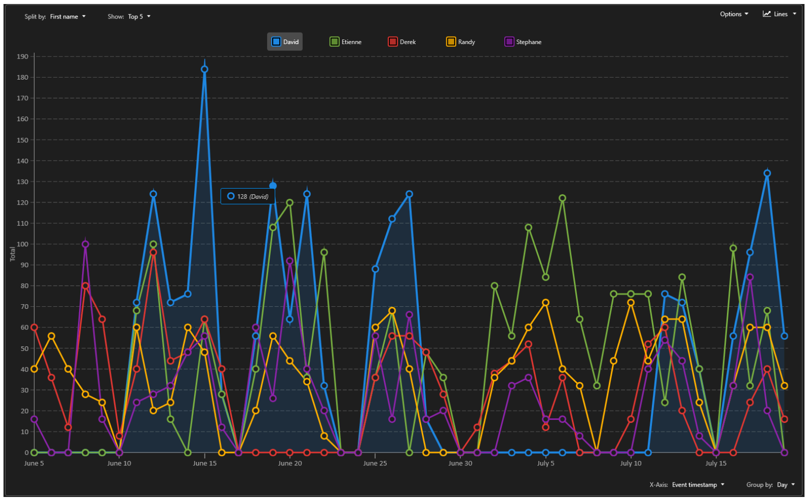
The following chart types are supported in Security Center when using the **Generate report** functions in Security Desk: **Lines**, **Columns**, **Stacked columns**, **Rows**, **Stacked rows**, **Doughnut**, and **Pie**.

Lines chart

Use a **Lines** chart when you want to track changes over a short or long period of time. For example, the total instances of the selected report data in relation to a timeline.

- Line charts can represent the data better than row or column charts when the difference in changes is small.
- Line charts can also be used to compare changes over the same period for more than one group.

The following example shows a Cardholder events report, Split by: **First name**, Show: **Top 5** and X-Axis: **Event timestamp**, Group by: **Day** as a **Lines** chart.



Split by: First name

Show: Top 5

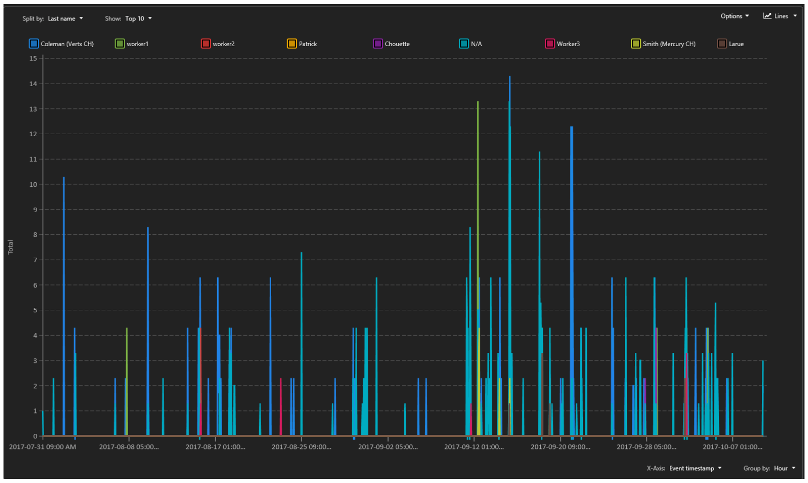
X-Axis: Event timestamp

Group by: Day

Lines chart (simplified)

When the time range is too wide or too precise, a lot of data has to be computed and displayed on screen. In this situation, a simplified version of the lines chart is displayed.

The following example shows a simplified version of a **Lines** chart.



Split by: Last name

Show: Top 10

X-Axis: Event timestamp

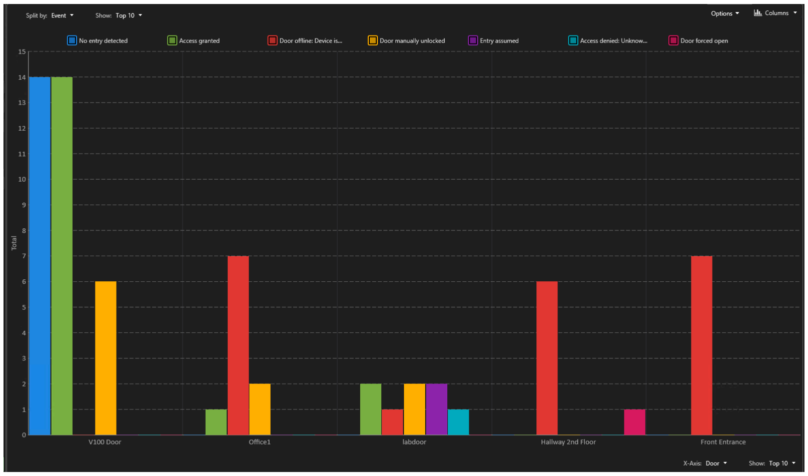
Group by: Hour

NOTE: The simplified version of a lines chart does not support interaction with the mouse or indication of Y value for a specific point.

Columns chart

Use a **Columns** chart when you want to group the data by category and display the results using vertical bars.

The following example shows a Door access report, Split by: **Event**, Show: **Top 10** and X-Axis: **Door**, Show: **Top 10** as a **Columns** chart.



Split by: Event

Show: Top 10

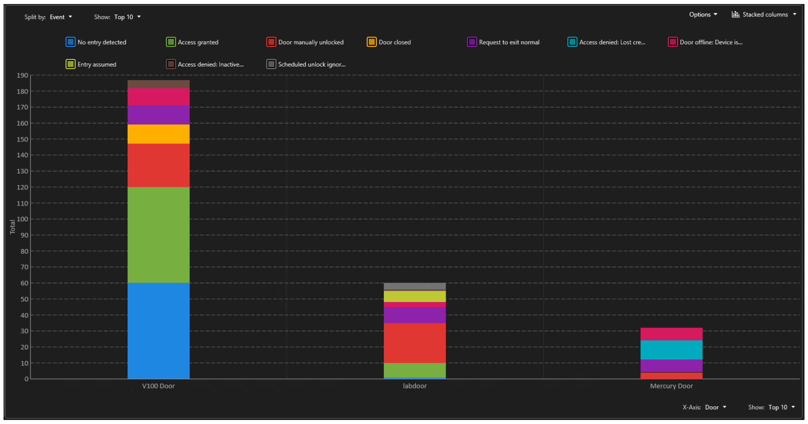
X-Axis: Door

Show: Top 10

Stacked columns

Use a **Stacked columns** chart when you want to group the data by category and display the results using vertical bars. The Y axis can be used to split the data and have more precise information in relation to the X value.

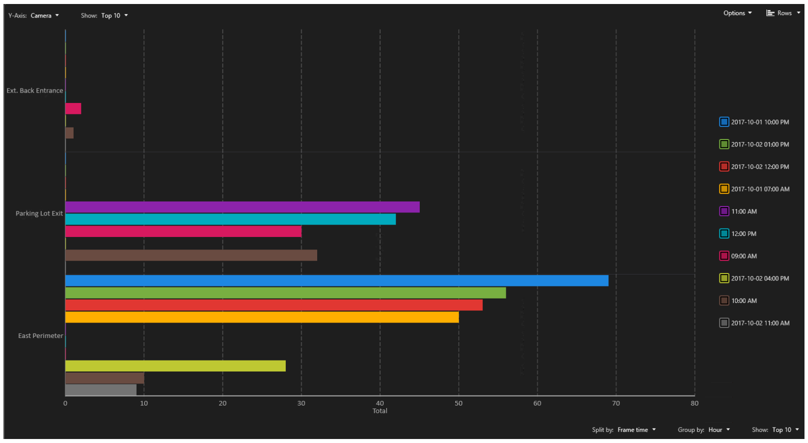
The following example shows a Door activities report, Split by: **Event**, Show: **Top 10** and X-Axis: **Door**, Show: **Top 10** as a **Stacked columns** chart.



Rows

Use a **Rows** chart when you want to group the data by category and display the results using horizontal bars.

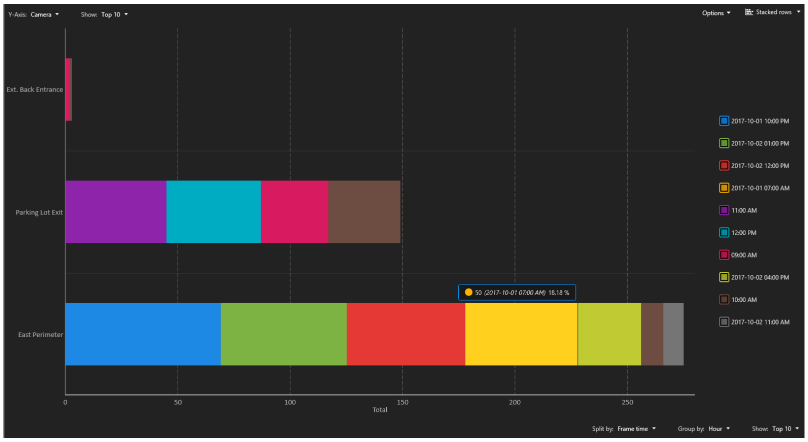
The following example shows an Intrusion detector report, Y-Axis: **Camera**, Show: **Top 10** and Split by: **Frame time**, Group by: **Hour**, Show: **Top 10** as a **Rows** chart.



Stacked rows

Use a **Stacked rows** chart when you want to group the data by category and display the results using horizontal bars. The X axis can be used to split the data and have more precise information in relation to the Y value.

The following example shows an Intrusion detector report, Y-Axis: **Camera**, Show: **Top 10** and Split by: **Frame time**, Group by: **Hour**, Show: **Top 10** as a **Stacked rows** chart.



Y-Axis: Camera ▾ Show: Top 10 ▾

Options ▾ Stacked rows ▾

Split by: Frame time ▾ Group by: Hour ▾ Show: Top 10 ▾

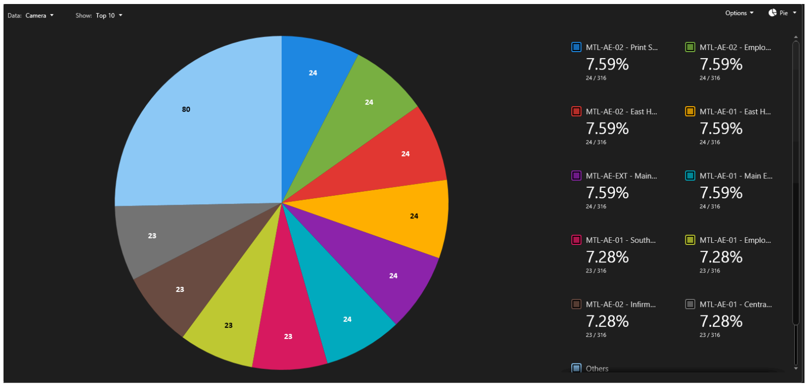
Pie and Doughnut charts

Use a Pie or Doughnut chart when you want to compare report data as a whole.

NOTE: Pie or Doughnut charts do not show changes over time.

Pie chart

The following example shows a Camera events motion report, Data: **Camera**, Show: **Top 10** as a **Pie** chart.

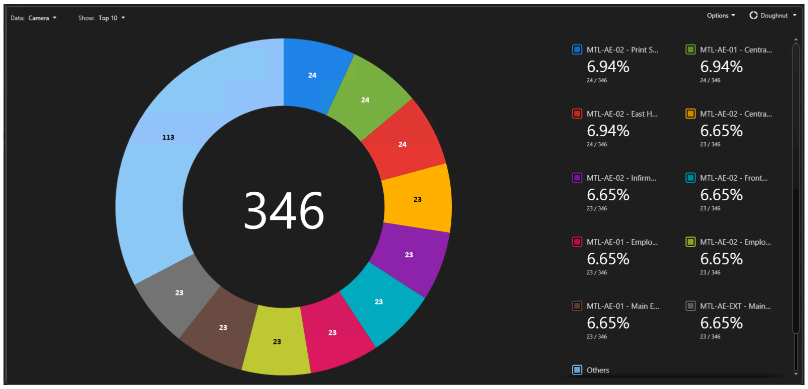


Data: Camera ▾ Show: Top 10 ▾

Options ▾ Pie ▾

Doughnut chart

The following example shows a Camera events report, Data: **Camera**, Show: **Top 10** as a **Doughnut** chart.



Data: Camera ▾ Show: Top 10 ▾

Options ▾ Doughnut ▾

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

Related Topics

Generating visual reports on page 62

Generating reports

To generate a report in any reporting task, you must set the query filters and then run the query. After you generate a report, you can work with your results.

What you should know

Reporting tasks are where you generate customized queries about the entities, activities, and events in your Security Center system for investigation or maintenance purposes. Most investigation and maintenance tasks are reporting tasks.

The maximum number of report results you can receive in Security Center is 50,000. By default, the maximum number of results is 500. You can change this value in the *Performance* section of the *Options* dialog box in Security Center.

NOTE: If you use an action to generate reports, the maximum number of results is set in the *Properties* page of the Report Manager role. This setting applies only to PDF and Excel formats. There is no limit for CSV format. For more information, see "Using a manual action to generate and export reports" in the *Security Center User Guide*.

To generate a report with more than 50,000 results, use the **Generate and save report** command. For more information, see Generating and saving reports on page 65.

These steps only describe the general process for running a report.

To generate a report:

1 Open a reporting task.

2 In the *Filters* tab, use the query filters to create a customized search.

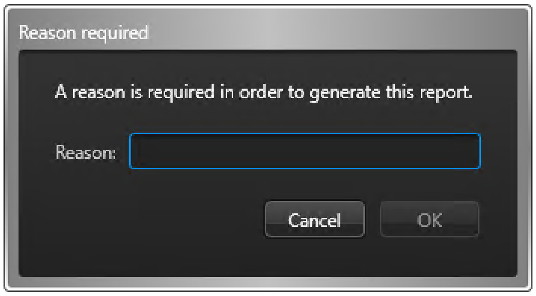
NOTE: Some of the filters have a **Select all** button. This button does not appear if there are more than 500 entities to select from. For example, if you have a list of 1500 cardholders. Queries with over 500 entities take longer to generate.

3 Set a date and time range for the report.

4 Click **Generate report**.

If there are invalid filters, this button is unavailable.

IMPORTANT: The *Reason required* dialog box is displayed when generating any report that contains ALPR data. The reason entered is logged and included in Activity trail (Report generated) audit logs to comply with State laws.



Reason required

A reason is required in order to generate this report.

Reason:

The query results are displayed in the report pane.

TIP: You can right-click a column heading to select which columns you want to show. It also allows you to configure a custom sort order for the results using multiple columns as the sorting criteria.

5 Analyze the query results.

The query results depend on the type of reporting task. When video sequences or ALPR data are attached to the query results, you can view them in the canvas by dragging a report item to a tile.

6 Work with the query results.

   Depending on the items in the query results, you can perform the following actions:

   a. Print the report.
   b. Save the report as a PDF, Excel, or CSV document.
   c. Export the video sequences.

7 (Optional) Save the report as a task.

   If you save the report layout (query filters and report columns) as a public task, you can share it with other users or use it as a report template with the *Email a report* action.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

Related Topics

Customizing the report pane on page 66
Customizing report behavior on page 67
Generating visual reports on page 62
ALPR task - General settings view on page 1395

Exporting generated reports

In every reporting task, you can export your results as a list or as a chart.

Before you begin

- To export generated reports, you need the *Print/export reports* and *Single user print/export* privileges.
- To export PDFs with Japanese or Chinese (simplified or traditional) characters on a machine running a Windows OS in a different language, you must install supplemental fonts.

What you should know

- If a report does not include images, the maximum number of results you can export in Security Center is 50,000.
- If a report includes images, the maximum number of results you can export in Security Center is 10,000.
- The option to export as a graph is only available if the report is viewed as a visual report, using **Charts**. The Charts function is not supported for the following reports: Door Troubleshooter, Video File Explorer, and Motion Search.
- To export the report data as a list (CSV, Excel, or PDF format), use the **Data** option. To export the report data as a chart (JPEG or PNG), use the **Graph** option. Alternatively, you can select both options to generate a report list and chart.

TIP: If you have the *Single user print/export* privilege, you can also automate the export of a report using a scheduled task. For more information, see Scheduling a task on page 221.

To export a generated report:

1 At the top of the report pane, click **Export report** (💾).

   NOTE: If you do not have the *Single user print/export* privilege, the *Authorization* window opens. From here, a second user who does have that privilege must enter their credentials to authorize the export.

2 In the dialog box, select either **Data**, **Graph**, or both and set the following options:

- **File format:** (Data only) Select the file format (CSV, Excel, or PDF).

  (Graph only) Select the file format (JPEG or PNG).
- **Destination file:** Select the file name.
- **Orientation:** (PDF only) Select whether the PDF file should be in portrait or landscape mode.
- **Attached files folder:** (CSV only) Specify where the attached files, such as cardholder pictures or license plate images, are saved.

3 Click **Export**.

The report is saved in the location that you specified.

Printing generated reports

In every reporting task, you can print your report after it is generated. To print the report data as a list use the **Print data** option. To print a visual report or chart use the **Print graph** option.

Before you begin

To print generated reports, you need the *Print/export reports* privilege.

What you should know

NitroPdf is not currently supported. Also, the option to print the report as a list or as a graph is only available if the report is viewed as a visual report, using **Charts**. Otherwise, the report is printed as a list by default. The Charts function is not supported for the following reports: Door Troubleshooter, Video File Explorer, and Motion Search.

To print a report (Print data):

1 At the top of the report pane, click **Print report** (🖨).

NOTE: If you do not have the *Single user print/export* privilege, the *Authorization* window opens, and a second user who does have that privilege must enter their credentials to authorize the printing.

2 Click **Print data**.

3 In the *Print report* dialog, select a printer, choose which pages to print, and make any desired changes related to the orientation, size, color, and margins of the document.

4 Click **Print**.

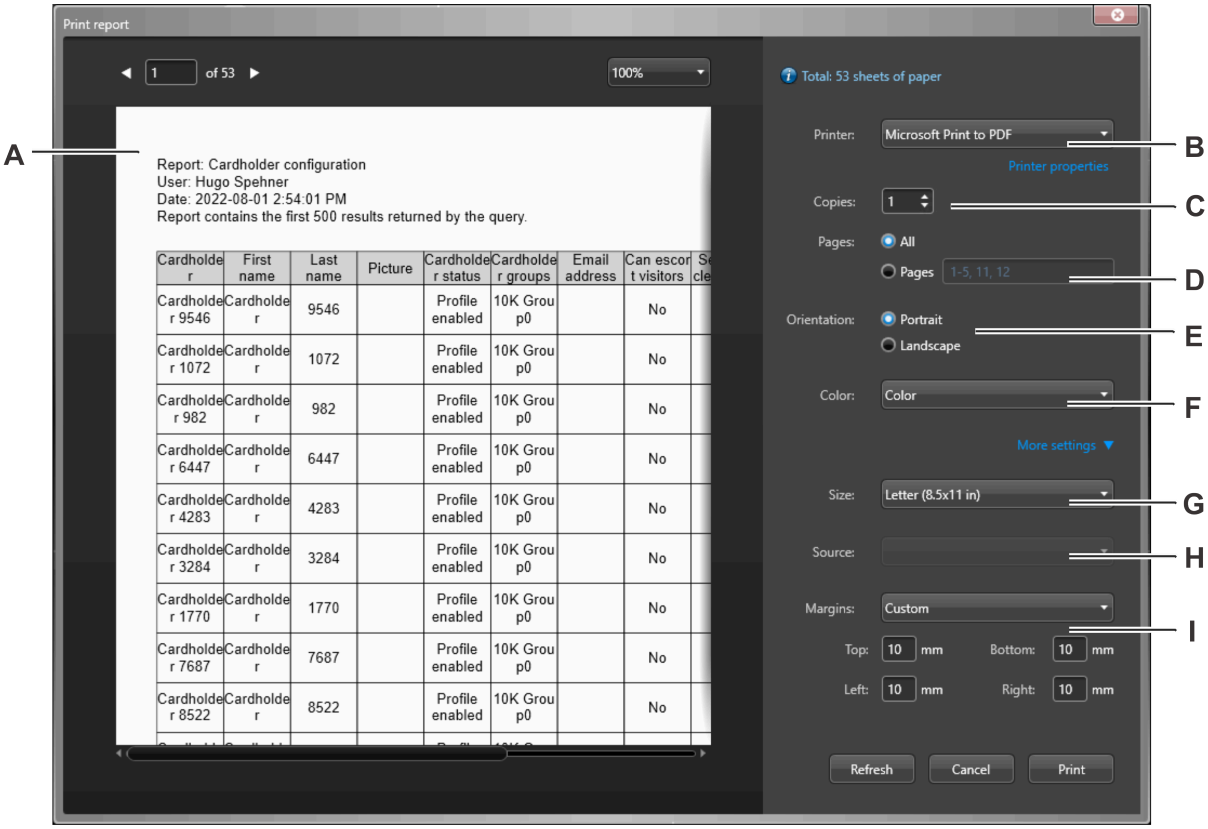
To print a visual report (Print graph):

1 At the top of the report pane, click **Print report** (🖨) then click **Print graph**.

2 In the *Print* window, select a printer and click **Print**.

Print report dialog

Before you print the report, you can make adjustments to the document's format, margins, and orientation, and preview the changes in this *Print report* dialog.



Report: Cardholder configuration
User: Hugo Spehner
Date: 2022-08-01 2:54:01 PM
Report contains the first 500 results returned by the query.

Cardholder	First name	Last name	Picture	Cardholder status	Cardholder groups	Email address	Can escort visitors	Se cle
Cardholder 9546	Cardholder	9546		Profile enabled	10K Group0		No	
Cardholder 1072	Cardholder	1072		Profile enabled	10K Group0		No	
Cardholder 982	Cardholder	982		Profile enabled	10K Group0		No	
Cardholder 6447	Cardholder	6447		Profile enabled	10K Group0		No	
Cardholder 4283	Cardholder	4283		Profile enabled	10K Group0		No	
Cardholder 3284	Cardholder	3284		Profile enabled	10K Group0		No	
Cardholder 1770	Cardholder	1770		Profile enabled	10K Group0		No	
Cardholder 7687	Cardholder	7687		Profile enabled	10K Group0		No	
Cardholder 8522	Cardholder	8522		Profile enabled	10K Group0		No	

Printer: Microsoft Print to PDF

Copies: 1

Pages: ● All ○ Pages 1-5, 11, 12

Orientation: ● Portrait ○ Landscape

Color: Color

Size: Letter (8.5x11 in)

Source:

Margins: Custom

Top: 10 mm Bottom: 10 mm

Left: 10 mm Right: 10 mm

A	**Preview**	Preview your report before printing. Changes made in this dialog automatically reload the preview for reports that are 30 pages or less. For larger reports, click **Refresh** to view your changes.
B	**Printer**	Select which printer to use to print the report.
C	**Copies**	Select the number of copies of the report to print. If you do not see the option, then the printer you have selected only prints one copy at a time.
D	**Pages**	Choose to print all pages of the report or a subset of pages.
E	**Orientation**	Display your report in portrait or landscape mode.
F	**Color**	Choose the color mode for the report. The options available depend on what the selected printer supports.
G	**Size**	Select a paper size for the report.
H	**Source**	Choose the paper source for the report from the input trays on the printer.
I	**Margins**	Set the margins for the report using preset values, or create custom margins 1-5 cm or 0.4-2 inches wide. The unit of measurement used depends on your Windows Regional setting.

Customizing time zone settings

If your Security Center system includes devices operating in different time zones, you must select whether the report queries are based on a fixed time zone, or on each device's local time zone.

What you should know

The time zone settings affect how the time range filters in your reports work. If you select a fixed time zone, the results that come from a device (such as an *access control unit* or a *video unit*) in another time zone are adjusted for time differences.

The time zone settings are saved as part of your user profile and apply to Security Desk and Config Tool.

To customize time zone settings:

1. From the homepage, click **Options** > **Date and time**.
2. To add time zone abbreviations to all time stamps in Security Center, select the **Display time zone abbreviations** option.
3. Select how time fields are displayed and interpreted in Security Center:
   - To display and interpret time according to each device's local time zone, select the **each device's time zone** option.

     This option allows each device to follow a different time zone. Select this option to display and interpret the time according to each device's local time zone.
   - To display and interpret time according to a fixed time zone, select **the following time zone** option, and choose a time zone from the drop-down list.
4. Click **Save**.

Example

If you create a report with a time range between 9 am and 10 am Eastern time, and devices located in Vancouver (Pacific time) are included in the search, one of the following happens based on your time zone settings:

- Time zone based on each device's local time zone: The report results are from events that occurred between 9 am and 10 am Pacific time.
- Fixed time zone (set to Eastern time): The report results are from events that occurred between 6 am and 7 am in the Pacific time zone, because of the three-hour time difference between Montreal and Vancouver.

Generating visual reports

You can view the reports as dynamic charts or graphs. This visual report data can be analyzed to help identify activity patterns and enhance your understanding.

Before you begin

- You must have the *Charts* license to generate visual reports.
- Only users with the *View charts* privilege can access the report charts.

What you should know

Here are some *visual reporting* use case examples:

- Omnicast™ Camera events task: View camera reports as charts to understand activity on multiple cameras, during a specified period.
- KiwiVision™ Security video analytics: Run visual reports to get a global view of your security environment.
- Synergis™ Door activities: View events as charts and graphs to gain insights about your access control system.
- AutoVu™ reads task: Use visual reports to help you better understand the ALPR reports for vehicle traffic in your environment.

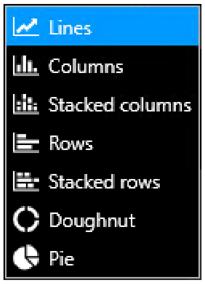
NOTE: The Charts function is not supported for the following reports: Door Troubleshooter, Video File Explorer, and Motion Search.

To generate a visual report:

1 Generate a report that supports the charts function.

2 Click **Charts** (📊).

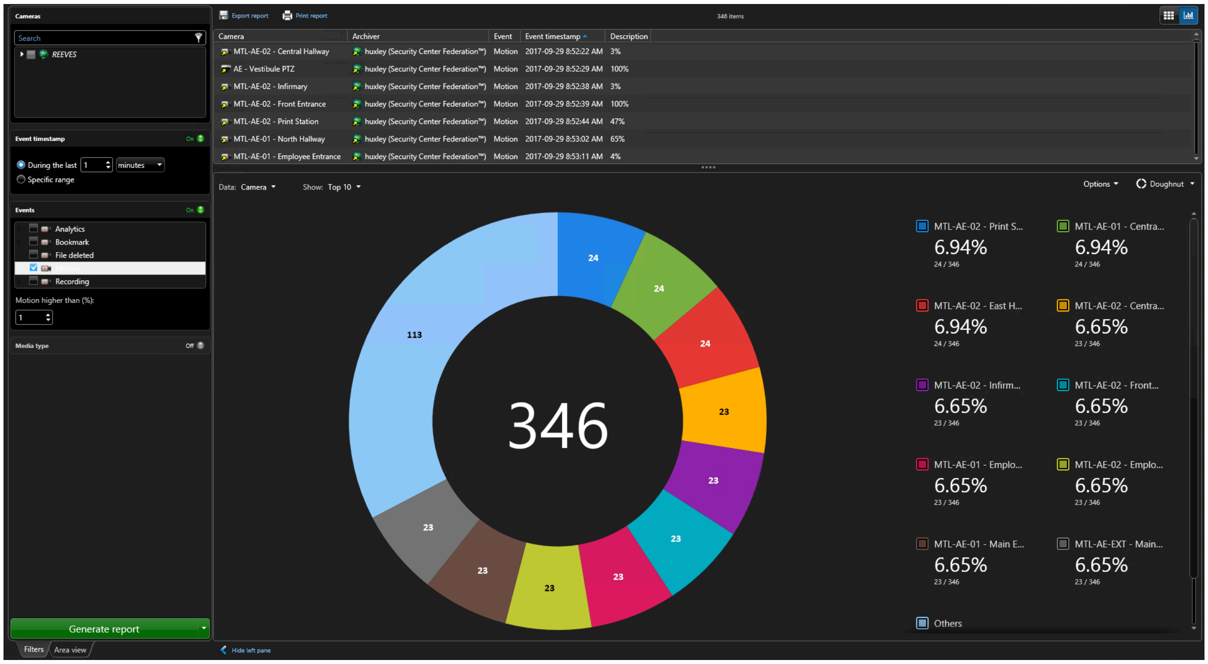
3 In the *Charts* pane, select a chart type from the drop-down menu.



4 Select the data that you want displayed in the visual report using the drop-down menus in the *Charts* pane: **Split by**, **Show** (**Top 10**, **Top 5**, or **Top 3**), **X-Axis**, **Y-Axis**, or **Data**.

NOTE: The choices available in the drop-down menus vary depending on the chart type, and the data in the report pane.

Example: The following **Doughnut** chart shows the Top 10 camera events.



Export report Print report 346 items

Camera	Archiver	Event	Event timestamp	Description
MTL-AE-02 - Central Hallway	huxley (Security Center Federation™)	Motion	2017-09-29 8:52:22 AM	3%
AE - Vestibule PTZ	huxley (Security Center Federation™)	Motion	2017-09-29 8:52:29 AM	100%
MTL-AE-02 - Infirmary	huxley (Security Center Federation™)	Motion	2017-09-29 8:52:38 AM	3%
MTL-AE-02 - Front Entrance	huxley (Security Center Federation™)	Motion	2017-09-29 8:52:39 AM	100%
MTL-AE-02 - Print Station	huxley (Security Center Federation™)	Motion	2017-09-29 8:52:44 AM	47%
MTL-AE-01 - North Hallway	huxley (Security Center Federation™)	Motion	2017-09-29 8:53:02 AM	65%
MTL-AE-01 - Employee Entrance	huxley (Security Center Federation™)	Motion	2017-09-29 8:53:11 AM	4%

Event timestamp: On; ● During the last 1 minutes; ○ Specific range

Events: On; ☐ Analytics; ☐ Bookmark; ☐ File deleted; ☑ Motion; ☐ Recording

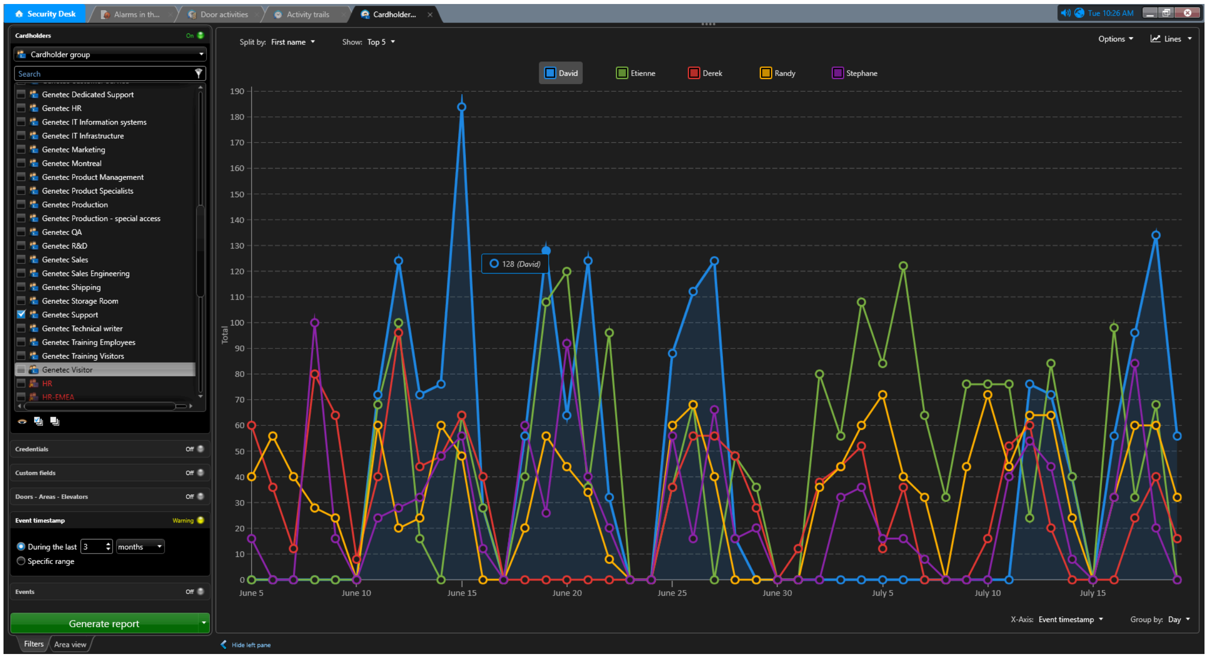
Motion higher than (%): 1

Media type: Off

Data: Camera Show: Top 10

Cameras
Search
REEVES
Options
Doughnut
24
24
24
23
23
23
23
23
23
113
346
MTL-AE-02 - Print S... 6.94% 24 / 346
MTL-AE-01 - Centra... 6.94% 24 / 346
MTL-AE-02 - East H... 6.94% 24 / 346
MTL-AE-02 - Centra... 6.65% 23 / 346
MTL-AE-02 - Infirm... 6.65% 23 / 346
MTL-AE-02 - Front... 6.65% 23 / 346
MTL-AE-01 - Emplo... 6.65% 23 / 346
MTL-AE-01 - Emplo... 6.65% 23 / 346
MTL-AE-01 - Main E... 6.65% 23 / 346
MTL-AE-EXT - Main... 6.65% 23 / 346
Others
Generate report
Filters
Area view
Hide left pane

Example: The following **Lines** chart shows the Top 5 cardholder events split by **First Name** and **Event timestamp** grouped by **Day** over a specified period.



Split by: First name Show: Top 5

X-Axis: Event timestamp Group by: Day

Event timestamp: Warning; ● During the last 3 months; ○ Specific range

5 Show or hide information in the visual report:

- Select (🟩) or clear (■) a chart legend item.
- In the **Options** drop-down menu, select or clear the **Show grid** and **Show values** options to show or hide the grid, and the number of results represented by each data point in the visual report.
- Hover over elements in the graph or chart to display additional information. This also highlights the related item in the chart legend.

6 Print or export the report as data (Excel, CSV, or PDF) or as a graph (PNG or JPEG).

The available formats depend on the query results.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

Related Topics

Generating reports on page 57
About visual reports on page 52
Exporting generated reports on page 58
Printing generated reports on page 59

Generating and saving reports

Instead of waiting for a report to generate and then exporting the results, you can generate a report and save it to a file location directly.

What you should know

- There is no limit to the number of results when you generate and save a report.
- If your report does not have a **Generate and save report** button, you can generate and save the report using a manual action. For more information, see "Using a manual action to generate and export reports" in the *Security Center User Guide*.

To generate and save a report:

1. Open an existing reporting task, or create a new one.
2. In the *Filters* tab, use the query filters to create a customized search.

   NOTE: Some of the filters have a **Select all** button. This button does not appear if there are more than 500 entities to select from. For example, if you have a list of 1500 cardholders. Queries with over 500 entities take longer to generate.
3. Right-click a column heading in the report pane, and click **Select columns** (▤).
4. Select which columns to include in the saved report, and click **Save**.
5. (Optional) To configure a custom sort order for the results using multiple columns as the sorting criteria, right-click a column heading in the report pane and select **Sort by**.
6. Click the drop-down arrow next to **Generate report** and click **Generate and save report**.

   NOTE: If you do not have the *Single user print/export* privilege, the *Authorization* window opens. From here, a second user who does have that privilege must enter their credentials to authorize the export.
7. In the dialog box, set the following options:
   - **File format:** Select the file format. Only CSV and Excel are supported.
   - **Destination file:** Select the file name.
   - **Attached files folder:** Specify where the attached files, such as cardholder pictures or license plate images, are saved. Only CSV is supported.
8. Click **Export**.

The report is saved in the location that you specified.

Customizing the report pane

Once you have generated your report, you can customize how the results are displayed in the report pane.

To customize the report pane:

1 Generate your report.

2 Choose which columns to show, as follows:

   a) In the report pane, right-click a column heading, and then click **Select columns** (▦).

   b) Select the columns you want to show, and clear the columns you want to hide.

   c) To change the column order of appearance, use the ▲ and ▼ arrows.

   d) Click **OK**.

3 To adjust the width of a column, click between two column headings and drag the separator to the right or left.

4 To change the column order, click and hold a column heading in the report pane, and dragging it to the desired position.

5 Sort the report results by one of the following methods:

   - **Sort by one column**: Click the column heading. Click the column heading a second time to reverse the order.
   - **Sort by multiple columns**: Right-click a column heading in the report pane and select **Sort by**. Configure a custom sort order for the results using multiple columns as the sorting criteria.

   NOTE: All columns containing timestamps are sorted according to their UTC time value. If you choose to display the times in Security Center according to each device's local time zone rather than a fixed time zone, the times might appear out of order if the report contains devices from different time zones.

6 To increase the size the report pane, drag the separator bar between the report pane and the canvas to the bottom of the application window.

7 Save your task layout with the changes you made to the report pane as follows:

   - To save the task as a *private* or *public* task, right-click the task tab, and then click **Save as**.
   - To save the workspace for the next time you open the application, right-click in the taskbar, and then click **Save workspace**.

Related Topics

Customizing time zone settings on page 61

Customizing report behavior

You can select how many report results to receive, and when you want to receive error messages about reports, from the *Options* dialog box.

What you should know

When the query reaches the specified limit, it automatically stops with a warning message. The maximum value you can set is 50,000. The report settings are saved as part of your user profile and apply to Security Desk and Config Tool.

To customize report behavior:

1. From the homepage, click **Options** > **Performance**.
2. In the *Reports* section, set the **Maximum number of results** option value.

   This option determines the maximum number of results that can be returned by a query using a reporting task. This limit helps ensure stable performance when too many results are returned if your query is too broad.
3. Click the **User interaction** tab.
4. (Optional) Select the **Display warning if query may take a long time to execute** option.
5. Click **Save**.

Related Topics

Backing up and restoring your user options on page 40

About the Report Manager role

The Report Manager role automates report emailing and printing based on schedules.

Only one instance of this role is permitted per system.

This role is created by default at system installation and hosted on your *main server*.

Setting maximum report results for automated reports

You can select the maximum number of results that can be generated using the *Email a report* or *Export report* actions, to prevent report that has too many results from freezing your computer.

What you should know

The maximum number of results only applies if you are saving the report in PDF or Excel format. It does not apply to CSV format.

The *Email a report* or *Export report* actions can be triggered using event-to-actions, or triggered as a one-time action or hot action from Security Desk.

To set the maximum number of report results:

1. From the Config Tool homepage, open the *System* task and click the **Roles** view.
2. Select the Report Manager role, and click the **Properties** tab.
3. Set a value in the **Maximum number of results for batch reports** option, and click **Apply**.

4

Keyboard shortcuts

This section includes the following topics:

Default keyboard shortcuts

This table lists the default keyboard shortcuts that you can use to control task, tiles, and entities on your local workstation. This list is categorized alphabetically by command category.

NOTE: You can change the keyboard shortcuts from the *Options* dialog box.

Command	Description	Shortcut
General commands		
Apply changes	Apply the changes made to your current configuration tab.	Ctrl+S
Exit application	Close the application.	Alt+F4
Full screen	Toggle between displaying the application in windows and full screen mode.	F11
Go to next page	Switch to the next task tab.	Ctrl+Tab
Go to previous page	Switch to the previous task tab.	Ctrl+Shift+Tab
Help	Open the online help.	F1
Homepage	Go to the homepage.	Ctrl+Grave accent (`)
Options	Open the *Options* dialog box.	Ctrl+O
Select columns	Select which columns to show or hide in the report pane.	Ctrl+Shift+C
Tile context menu	Open the tile context menu for the selected tile in the canvas. **NOTE:** This keyboard shortcut cannot be modified from the *Options* dialog box.	Shift+F10 or Context menu key Press Tab to cycle through the menu options, and then press `Enter`.
Camera commands		
Add a bookmark	Add a bookmark to video in the selected tile (for live video only).	B
Add bookmark (all)	Add bookmarks to video in all selected tiles (for live video only).	Ctrl+Shift+B
Copy statistics of the currently selected video tile	Copy the statistics of the selected tile.	Ctrl+Shift+X
Show diagnostic timeline	Show the timeline of the video stream diagnosis.	Ctrl+Shift+T
Show video stream diagnosis	Show or hide the video stream diagnosis, where you can troubleshoot your video stream issues.	Ctrl+Shift+D

Command	Description	Shortcut
Show video stream statistics on the tile	Show or hide the statistics summary of the video in the selected tile.	Ctrl+Shift+A
Show video stream status	Show or hide the status summary of the video stream connectins and redirections in the selected tile.	Ctrl+Shift+R
PTZ commands		
Go to preset	Jump to a PTZ preset you select.	<PTZ preset>+Shift +Insert
Pan left	Pan the PTZ camera image to the left.	Left arrow
Pan right	Pan the PTZ camera image to the right.	Right arrow
Tilt down	Tilt the PTZ camera image down.	Down arrow
Tilt up	Tilt the PTZ camera image up.	Up arrow
Zoom in	Zoom in the PTZ camera image.	Hold the Plus sign (+)
Zoom out	Zoom out the PTZ camera image.	Hold the En dash (-) key
Task commands		
Rename task	Rename the selected task.	F2
Save as	Save a task under a different name and scope (private or public).	Ctrl+T
Save workspace	Save the task list so that it is automatically restored the next time you log on to the system with the same user name.	Ctrl+Shift+S
Saved tasks	Open the *public tasks* page from the homepage.	Ctrl+N

Related Topics

Customizing keyboard shortcuts on page 73

Customizing keyboard shortcuts

You can assign, modify, import, or export the keyboard shortcuts mapped to frequently used commands in Security Center.

What you should know

A keyboard shortcut can only be assigned to a single command. If you assign an existing keyboard shortcut to a command, that shortcut is removed from the previously assigned command.

The keyboard shortcut configuration is saved as part of your user profile and applies to Security Desk and Config Tool. If your company uses a standard set of shortcuts, you can export the keyboard shortcut configuration to an XML file and send it to another workstation, or import one to your workstation.

To customize your keyboard shortcuts:

1. From the homepage, click **Options** > **Keyboard shortcuts**.
2. (Optional) Import a keyboard shortcut configuration as follows:
   a) Click **Import**.
   b) In the dialog box that opens, select a file and click **Open**.
3. In the *Command* column, select the command you want to assign a keyboard shortcut to.
4. Click **Add an item** (➕) and press the desired key combination.

   If the shortcut is already assigned to another command, a message is shown.

   - Click **Cancel** to choose another shortcut.
   - Click **Assign** to assign the shortcut to the selected command.
5. Click **Save**.
6. If you need to send your short configuration to another user, export the configuration as follows:
   a) From the homepage, click **Options** > **Keyboard shortcuts**.
   b) Click **Export**.
   c) In the dialog box that opens, select a filename and click **Save**.
7. To restore the default keyboard shortcuts:
   a) From the homepage, click **Options** > **Keyboard shortcuts**.
   b) Click **Restore default** > **Save**.

Related Topics

Default keyboard shortcuts on page 71

Part II

Common Security Center administration

This part includes the following chapters:

5

Entities

This section includes the following topics:

About entities

Entities are the basic building blocks of Security Center. Everything that requires configuration is represented by an entity. An entity can represent a physical device, such as a camera or a door, or an abstract concept, such as an alarm, a schedule, a user, a role, a plugin, or an add-on.

Entities created automatically in Security Center

Although most *entities* are created manually in Security Center, some entities can also be discovered or created automatically.

The entities that are *discovered* in Security Center are those that represent hardware devices, such as video units or access control units. Usually, Security Center needs a live connection to the hardware device before the entity can be created.

The following table lists the entities that are automatically created in Security Center:

Entity type	Automatic creation	Manual creation
Servers	Always.	Not supported.
Networks	Adding a new server automatically creates a new network.	Supported, but generally not required.
Access control units	Only for units that support *automatic discovery*.	Supported, but requires a live connection to the unit.
Video units	Only for units that support *automatic discovery*.	Supported, but requires a live connection to the unit.
Cameras	Always. Camera (or video encoder) entities are created when the encoding video units are added to your system.	Not supported.
Analog monitors	Always. Analog monitor (or video decoder) entities are created when the decoding video units are added to your system.	Not supported.
ALPR units	• Fixed ALPR units are discovered by the ALPR Manager roles. • Mobile ALPR units (mounted on patrol vehicles) are added when the Genetec Patroller™ entities are added.	Supported for fixed ALPR units, but generally not required.
Patrollers	Always.	Not supported.
Intrusion detection units	Never.	Supported, but requires a live connection to the intrusion panel.
Intrusion detection areas	Created by the Intrusion Manager role when the intrusion panel is enrolled.	Supported only if the Intrusion Manager cannot read the area configurations from the unit.

Related Topics

Automatic enrollment of access control units

Discovering units on your network on page 226

Changing entities' icons

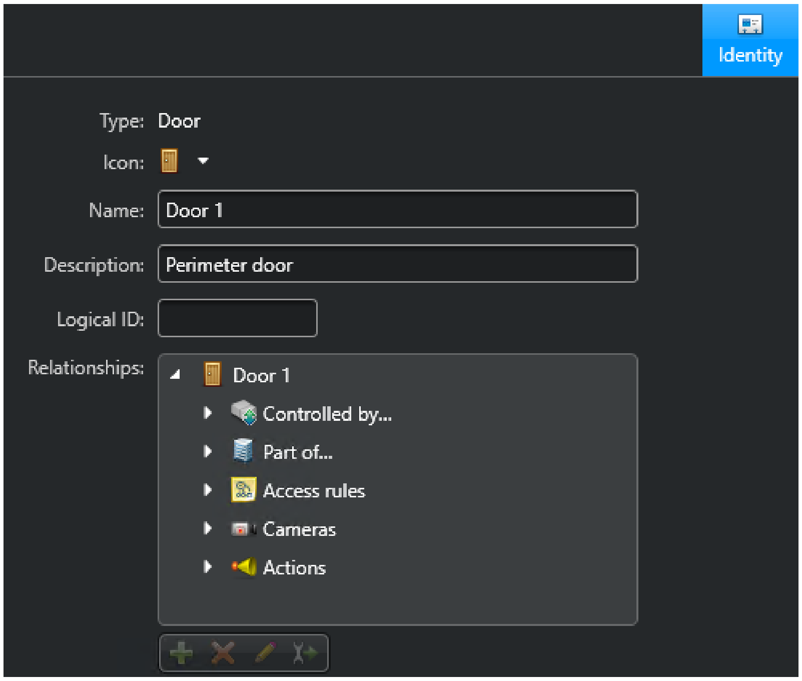
Entity icons graphically represent entity functions, acting as a quick visual hint when you are interacting with the *entity tree*.

What you should know

You can change an entity's icon to match the entity's specific purpose (for example, a door entity that represents a turnstile or a parking gate).

To change an entity's icon:

1. From the Config Tool home page, open the *Area view* task.
2. From the *entity browser*, select the entity and click the **Identity** tab.



Type: Door

Icon:

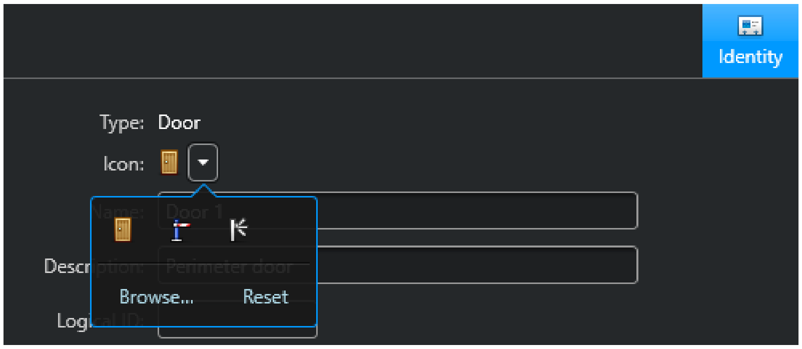
Name: Door 1

Description: Perimeter door

Logical ID:

Relationships:
- Door 1
  - Controlled by...
  - Part of...
  - Access rules
  - Cameras
  - Actions

3. From the **Icon** list, select a new icon.



Type: Door

Icon:

NOTE: You can select the default icon that matches the entity's real-world function, or do one of the following:

- Click **Browse...** to navigate to and select your own preferred custom icon.
- Click **Reset** to restore the default icon.

4. Click **Apply**.

Setting geographical locations of entities

To calculate the rising and setting of the sun for video units, or to plot a map for ALPR units, you can set the latitude and longitude of that entity.

What you should know

The geographical location (latitude, longitude) of an entity has two different uses:

- The geographical location of video units is used to automatically calculate the time when the sun rises and sets on a given date. This is helpful if you want the system to only record video during the daytime (for cameras that are placed outside), or adjust the brightness of a camera based on the time of day.
- The geographical location of fixed *ALPR units* without a GPS receiver is used to plot the ALPR events (*reads* and *hits*) associated with the ALPR unit on the map in Security Desk.

To set the geographical location of an entity:

1. In the **Location** tab of an entity, click **View on map**.

   A map window appears.
2. Navigate to the location of your entity on the map.

   You can click and drag to zoom in, zoom out, and pan.
3. Click **Select** in the map window.

   The cursor changes to a cross.
4. Click on the desired location on the map.

   A pushpin appears on the map.
5. Click **OK**.

The latitude and longitude fields display the coordinates of the location you clicked on the map.

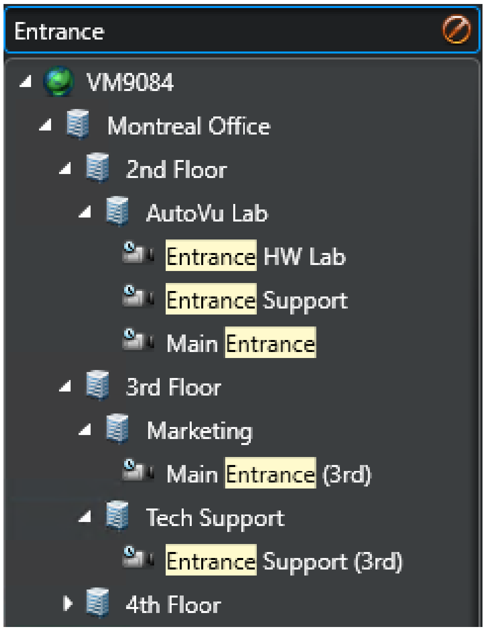
Searching for entities

If you cannot find the entity you need in a task, you can search for the entity by name.

To search for an entity:

1 In the *Search* box in the selector, type the entity name you are searching for.

2 Click **Search** (🔍).



Entrance ⊘

- VM9084
  - Montreal Office
    - 2nd Floor
      - AutoVu Lab
        - Entrance HW Lab
        - Entrance Support
        - Main Entrance
    - 3rd Floor
      - Marketing
        - Main Entrance (3rd)
      - Tech Support
        - Entrance Support (3rd)
    - 4th Floor

Only entities with names containing the text you entered are displayed.

3 Click **Clear filter** (⊘) to stop using the search filter.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

Searching for entities using the search tool

You can apply a set of filters to find the entities you need using the *Search* tool.

What you should know

The *Search* tool is available for many tasks. The available filters depend on the task you are using. For example, you can filter entities by name, description, entity type, partitions, and so on.

To search for an entity using the Search tool:

1 In the *Search* box in the selector, click **Apply a custom filter** (▼).

2 In the *Search* window, use the filters to specify your search criteria.

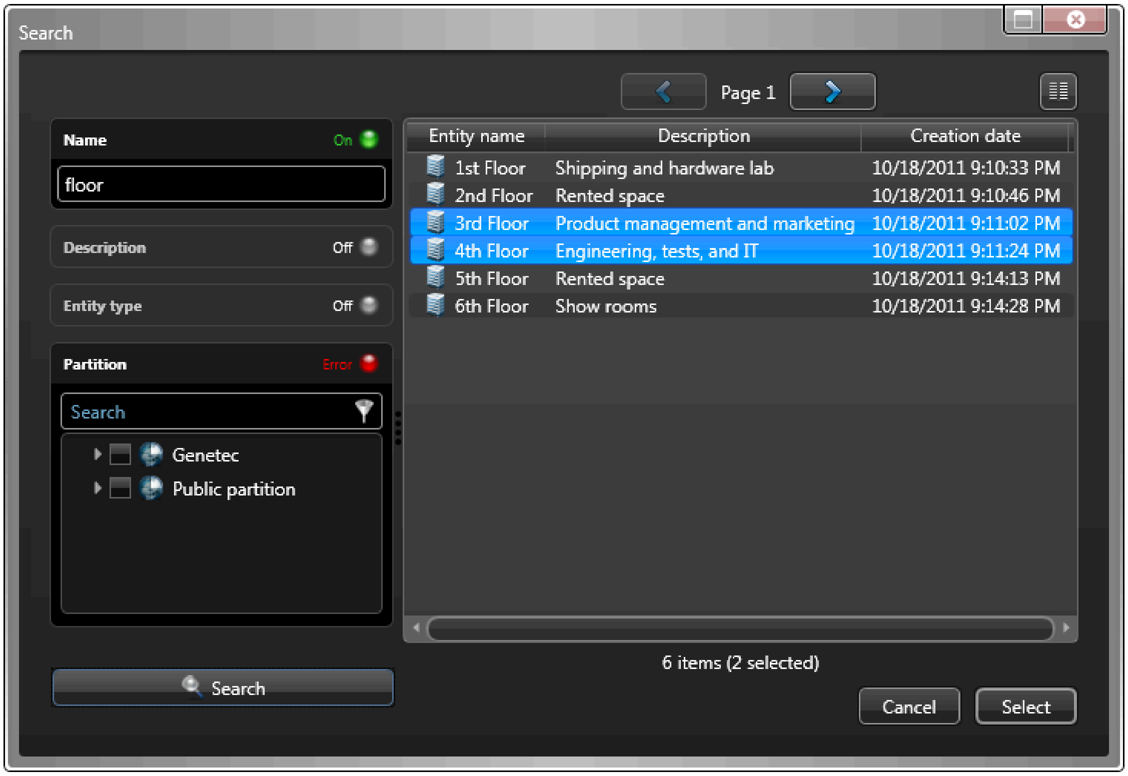
- To turn on a filter, click the filter heading. Active filters are shown with a green LED (●).
- To turn off a filter (●), click the filter heading.

NOTE: Invalid filters are shown in red. Hover your mouse cursor over the heading to see why the filter is invalid.

3 Click **Search** (🔍).
The search results appear on the right. The total number of results is displayed at the bottom of the list.

4 Click **Select columns** (▤) to choose which columns to display in the result list.

5 Select the entities you want.
TIP: Hold the Ctrl key for multiple selections. Click ‹ and › to scroll through multiple pages of results.



Name: floor

Partition: □ Genetec, □ Public partition

Entity name	Description	Creation date
1st Floor	Shipping and hardware lab	10/18/2011 9:10:33 PM
2nd Floor	Rented space	10/18/2011 9:10:46 PM
3rd Floor	Product management and marketing	10/18/2011 9:11:02 PM
4th Floor	Engineering, tests, and IT	10/18/2011 9:11:24 PM
5th Floor	Rented space	10/18/2011 9:14:13 PM
6th Floor	Show rooms	10/18/2011 9:14:28 PM

6 items (2 selected)

6 Click **Select**.
Only the entities you selected appear in the selector.

7 Click **Clear filter** (⊘) to stop using the search filter.

Copying configuration settings from one entity to another

When you have many similar entities to configure, you can save time by copying the settings of one entity to others of the same type using the Copy configuration tool.

Before you begin

If you are copying camera settings, make sure the source and destination cameras are of the same brand and model so their settings are compatible.

The Copy configuration tool does not work on federated entities.

To copy the configuration settings of one entity to another entity:

1. Open the **Copy configuration tool** one of the following ways:
   - From the Config Tool home page, click **Tools** > **Copy configuration tool**.
   - From the Config Tool, right-click an entity in any entity tree, and then click **Copy** > **Copy configuration tool**.
2. Select an entity type, and click **Next**.
3. In the *Source* page, select which entity you want to copy the settings from, and click **Next**.
4. In the *Options* page, select the types of settings you want to copy, and click **Next**.

   To know which options are available for each entity type, see the following list.
5. In the *Destinations* page, select the entities you want to copy the settings to, and click **Next**.
6. When the copying process is completed, click **Close.**

After you finish

If you copied camera settings, test the settings that are dependent on camera location (for example, motion detection or color) on the camera you copied the configuration to. You might have to adjust the settings, depending on whether the camera is inside or outside, in a busy or quiet location, and so on.

Related Topics

Testing motion detection settings on page 629

Adjusting camera color settings on page 631

Upgrading access control unit firmware and platform, and interface module firmware on page 943

Replacing SharpV units on page 1046

Settings copied for each entity type using the Copy configuration tool

You can determine which categories of settings are copied when using the Copy configuration tool. The available categories are different for each entity.

The following table lists the categories of settings that are available for each entity type when using the Copy configuration tool:

Entity type	Setting categories available
Access Control unit	• Actions • Properties (HID only) — All settings in the **Properties** tab, except the ones covered under the *Security* category. • Security (HID only) — Includes: **Secure mode** and **Admin password**. • Synchronization • Time Zone
Access rule	• Attached entities • Members • Properties
Alarm	• Actions • Attached entities • Properties • Recipients
ALPR Unit	• Hotlists
Area	• Advanced • Map
Camera	• Actions (not for federated cameras) • Boost quality • Color • Encryption (not for federated cameras) • Hardware specific settings • Motion detection • Network • Privacy protection (not for federated cameras) • PTZ (not for federated cameras) • Recording • Stream usage • Video quality • Visual tracking (not for federated cameras)
Cardholder	• Access rules • Actions • Options • Parent cardholder groups • State
Cardholder group	• Access rules • Members • Parent cardholder groups • Properties

Entity type	Setting categories available
Credential	• Actions • Badge template • State
Door	• Access rules • Actions • Cameras • Properties • Unlock schedules
Elevator	• Access rules • Actions • Advanced • Cameras • Unlock schedules
Hotlist	• Advanced • Attributes • Path • Properties
Parking rule	• Properties
Parking zone	• Enforcement • ALPR cameras • Parking rules • Properties
Patroller	• Actions • Hotlists • Permits • Properties
Permit	• Advanced • Attributes • Parking lots • Path • Properties
Permit restriction	• Properties • Zones

Entity type	Setting categories available
User	• Access rights • Actions • Advanced • Alarms • Privileges • Properties • Security Desk settings
User group	• Access rights • Advanced • Alarms • Members • Privileges • Properties • Security Desk settings
Video unit	• Actions • Audio • Hardware specific settings • Motion detection • Network • Security • Time Zone
Zone	• Actions

NOTE: Custom fields can also be copied if they are defined for the selected entity type.

Assigning logical IDs to entities

You can assign a logical ID (unique number) to entities, public tasks, and workstations in your system so that you can control them using keyboard shortcuts.

What you should know

If you want to use keyboard shortcuts to switch to different public tasks, control other workstations, or display entities in the Security Desk canvas, you must assign unique numbers (logical IDs) to entities. The logical IDs can then be used in a keyboard shortcut. For more information about using keyboard shortcuts in Security Desk, see the *Security Center User Guide*.

There are a few entities that are often used together in a keyboard shortcut. These entities are grouped, and cannot have the same logical ID. For example, *cameras* and *public tasks* are in the same group, because they are often used together in a keyboard shortcut to open a saved task and display a camera.

TIP: You can also change the logical ID from the *Identity* tab of each entity's configuration page.

To assign a logical ID to an entity:

1. Open the *System* task, click **General settings** view, and go to the *Logical ID* page.
2. From the **Show logical ID for** list, select the group that lists the entity, public task, or workstation you want to use.

   If the item you want is not listed in one of the groups, select **All types**.
3. Next to the item you want to assign the logical ID to, type a number in the **ID** column.
4. Click **Apply**.

   If the logical ID is already assigned, you receive an error message. Select a different ID and try again.

Modifying logical IDs

If there are duplicate logical IDs, or you want to change an ID to a number that is easier to remember when using your keyboard shortcuts, you can modify the logical ID of an entity.

To modify a logical ID:

1. Open the *System* task, click **General settings** view, and go to the *Logical ID* page.
2. From the **Show logical ID for** list, select the group to configure.
3. If you have a large system, select the **Hide unassigned logical IDs** option to only show entities, public tasks, and workstations that have a logical ID.
4. If there are still multiple pages, use the ❮ and ❯ buttons to scroll through the pages.
5. Next to the entity, public task, or workstation you want to modify, type a new logical ID in the **ID** column.
6. Click **Apply**.

Customizing how entities are displayed in the canvas

You can show the logical ID (unique ID number) of entities in the area view to help you identify them. You can also display the name of the *Active Directory* the entity is imported from.

What you should know

These settings are saved as part of your user profile and are applied to Security Desk and Config Tool.

To customize how entities are displayed:

1. From the homepage, click **Options** > **User interaction**.
2. To display the logical ID in brackets after the entity name, select the **Show logical ID** option.
3. To display the username and domain name of the Active Directory, select the **Show Active Directory domain name where it is applicable** option.
4. Click **Save**.

Related Topics

Backing up and restoring your user options on page 40

Deleting entities

You can delete entities that you have manually created, and those that were discovered automatically by the system.

Before you begin

If the entity was automatically discovered, it must be offline or inactive (shown in red) before you can delete it.

What you should know

- If you delete a parent entity that has entities underneath it in the entity tree, those entities are also deleted.
- By default, users who are allowed to delete cameras can simultaneously delete any associated video archives. If you do not want archives to be deleted when users delete cameras, deny the user or user group the *Delete cameras and associated video archives* privilege.

  NOTE: This does not apply when removing a camera from an Auxiliary or Remote Site Archiver. The user will have the option to delete the video archives from those roles even without the privilege.

To delete an entity:

1. In the entity view of any task, select the entity.
2. At the bottom of the window, click **Delete** (✖).
3. In the confirmation dialog box that appears, click **Delete**.

   If more than one copy of the entity exists, the other copies stay until they are deleted.

Entity states

Entities can appear in several different states in the area view, which are represented by different colors.

The following table lists the three entity states:

State	Color	Description
Online	White	The server can connect to the entity.
Offline	Red	The server cannot connect to the entity.
Warning	Yellow	The server can connect to the entity, but there are problems.

Entity warnings usually appear because of invalid configurations. For example, when it comes to cameras the following two conditions can cause the camera to fall into a yellow warning state:

- Multiple, conflicting recording schedules have been applied to the same camera.
- A *Transmission lost* event has occurred. This means that the Archiver is still connected to the camera, but it has not received any video packets for more than 5 seconds.

To troubleshoot offline and warning states of cameras, you do one of the following:

- Change the conflicting schedules.
- Troubleshoot the Archiver role.

Related Topics

Troubleshooting: entities on page 90
About schedules on page 202

Troubleshooting: entities

You can troubleshoot entities and roles using the *diagnostic* tool.

What you should know

An entity or role that is not properly configured is displayed in yellow. An entity that is offline is displayed in red. The *diagnostic* tool can help you troubleshoot the problem with the entity.

To troubleshoot an entity:

1. Open the *System status* task.
2. From the **Monitor** list, select the entity type you want to diagnose.
3. If required, select an area in the *Selector*.
4. To include entities within nested areas, select the **Search member entities** option.

   The related entities are listed in the report pane.
5. Select a trouble entity, and click **Diagnose** (✚).

   A troubleshooting window opens, showing the results from the diagnostic test performed on the selected entity.
6. To save the results of the test, click **Save** > **Close**.

Related Topics

Entity states on page 89

About custom fields

A custom field is a user-defined property that is associated with an entity type and is used to store additional information that is useful to your organization.

Custom fields can include any information that you define. They can use data types that are available by default in Security Center, or you can create your own data types. Once custom fields are added, they are available in all database reports and queries related to the entity they are defined for. If a custom field contains private information, you can restrict its access to certain groups of users. You can also choose to encrypt the custom field values stored the database.

For example, you can add *Gender*, *Home phone number*, and *Cellphone number* as custom fields for cardholder entities, and only allow the *Human Resource* user group to access that information. To prevent someone with access to the database from viewing this personal information, you can encrypt these custom fields in the database.

Standard data types

Security Center includes the following default data types for custom fields:

- **Text:** Alphanumeric text.
- **Numeric:** Integers in the range -2147483648 to 2147483647.
- **Decimal:** Real numbers from -1E28 to 1E28.
- **Date:** Gregorian calendar date and time.
- **Boolean:** Boolean data, represented by a check box.
- **Image:** Image file. The supported formats are: .bmp, .jpg, .gif, and .png.
- **Entity:** Security Center entity.

Limitations of custom fields

- Custom fields are always local to the system where they are defined.
  - In a *Federation*™ scenario, custom fields are not imported from the federated system. However, you can associate custom fields as local attributes to *federated entities*.
  - In an *Active Directory (AD)* integration scenario, custom fields can be imported from object attributes to display their values in your local system, but not to update the AD.
- Encrypted custom fields are subject to the following limitations:
  - You cannot enforce the *unique value* option if the custom field is encrypted.
  - You cannot use an encrypted custom field as a query filter for reports.

    However, if the client application (Security Desk or Config Tool) is at a version older than 5.10.3.0, encrypted custom fields are displayed as query filters, but they do not work.
  - When you modify the value of an encrypted custom field, the change is recorded in the audit trail, but the old and new values are not shown in the log entry.

Related Topics

About federated entities on page 270

Linking AD attributes to Security Center fields on page 483

Creating custom data types for custom fields

To use something other than the standard data types when creating custom fields, you can create your own custom data types.

What you should know

Custom data types define a list of values based on a standard data type. Custom data types appear in a drop-down list in the *Custom fields* tab of the entity's configuration page.

To create a custom data type for a custom field:

1. Open the *System* task and click the **General settings** view.
2. On the *Custom fields* page, click the **Custom data types** tab.
3. Click ✚ at the bottom of the custom data type list.
4. On the *Edit custom data type* page, enter the **Name**, **Description**, and **Type** for your custom data type, and click **Next**.
5. On the *Data entry* page, enter a value in the **Value** field and click ✚.

   The entered value is added to the enumerated list.
6. Define other possible values for this data type.
7. When you are finished, click **Next**, **Next**, and **Close**.

Modifying custom data types

You can modify custom data types (rename, add or delete values, and so on) before or after the custom data type is being used in a custom field.

What you should know

The following limitations apply when modifying custom data types:

- You cannot delete a value if it is being used as the default value for a custom field.
- You cannot change the standard data type on which the custom data type is based.

To modify a custom data type:

1. Open the *System* task and click the **General settings** view.
2. Go to the *Custom fields* page and click the **Custom data types** tab.
3. Select the data type, click **Edit the item** (✏), and follow the wizard.

Creating custom fields

To add more information to the properties of entities in your system, you can create custom fields.

Before you begin

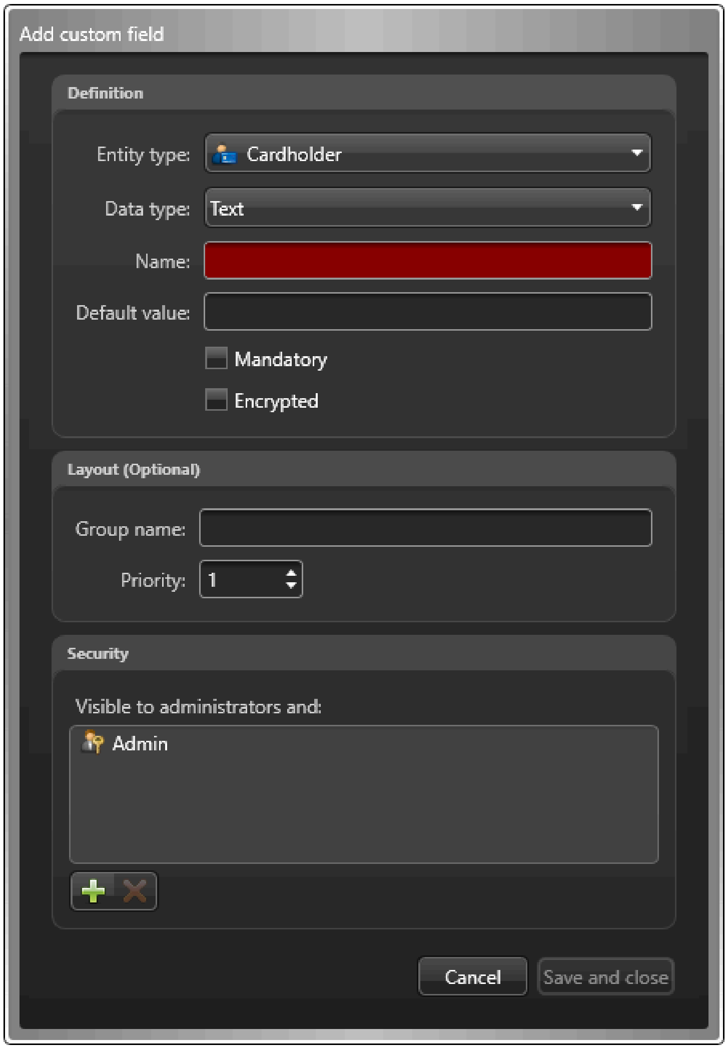
If you want to create a custom field using your own custom data type, the data type must already be created.

To create a custom field:

1 Open the *System* task and click the **General settings** view.

2 Click the **Custom fields** tab, and click **Add an item** (+) at the bottom of the custom field list.

3 In the *Add custom field* dialog box, select the **Entity type** that applies to this custom field.



Add custom field

Definition

Entity type: Cardholder

Data type: Text

Name:

Default value:

□ Mandatory

□ Encrypted

Layout (Optional)

Group name:

Priority: 1

Security

Visible to administrators and:

Admin

4 From the **Data type** list, select a standard or custom data type for the custom field.

5 In the **Name** field, enter the name for the custom field.

6 (Optional) In **Default value** field, enter or select the default value for this field.
This value is displayed by default when an entity that uses this custom field is created.

7. Depending on the selected data type, the following additional options are available:
   - **Mandatory:** Select this option if the custom field cannot be empty.
   - **Value must be unique:** Select this option if the value of the custom field must be unique.

     NOTE: The *unique value* option can only be enforced after the field is created. To enforce this option, you must first make sure that all entities in your system have a distinct value for this custom field, then edit this custom field to apply the unique value option to it. Selecting this option automatically selects the **Mandatory** option.
   - **Encrypted:** Select this option if you want this field to be encrypted in the database (encryption at rest).

     NOTE: You must make that decision at creation time. You cannot change this option after the field is created. For other limitations regarding custom field encryption, see About custom fields on page 91.
8. Under the *Layout* section, type the **Group name**, and select the **Priority** from the drop-down list.

   These two attributes are used when displaying the unit's web page, field in the *Custom fields* page of associated entity. The group name is used as the group heading, and the priority dictates the display order of the field within the group.
9. In the *Security* section, click ➕ to add users and user groups that are able to see this custom field.

   By default, only administrators can see a custom field.
10. Click **Save and close** > **Apply**.

The new custom field is now available on the *Custom fields* page of the selected entity type, and can be used to search for those entity types in the *Search* tool.

Related Topics

About custom fields on page 91

6

Servers and roles

This section includes the following topics:

About servers

In Security Center, a server entity represents a computer on which the Genetec™ Server service is installed.

IMPORTANT: Server names must be 15 characters or fewer. Security Center truncates all server names longer than 15 characters, causing errors when the system tries to access those servers.

Server entities are automatically created when the Security Center Server software is installed on a computer, and that computer is connected to the *main server* of your system.

Main server

The main server is the computer that hosts the *Directory* role. All other servers (expansion servers) on the system must connect to the main server in order to be part of the same system.

You can have only one main server on a Security Center system.

Expansion servers

An expansion server is a computer that you add to your system to increase its overall computing power. An expansion server must connect to the main server, and can host any role in Security Center, except the Directory role.

You can increase the computing power of your system at any time by adding more expansion servers to your pool of resources.

Genetec™ Server service

The Genetec™ Server service is a Windows service that is automatically installed when you install Security Center Server on a computer.

Security Center Server and the *Genetec™ Server* service must be installed on every computer that you want to include in the pool of servers available for Security Center. After the *Genetec™ Server* service is installed, you can change its password and other settings using the *Server Admin* web application.

Related Topics

Adding expansion servers on page 107

Opening Server Admin using a web browser

Using a web browser, you can open Server Admin on any server in your system and then change the settings of any server in your system.

Before you begin

To log on to a server in your system using Server Admin, you must know the server's DNS name or IP address, the web server port, and the server password. The server password is specified during Security Center Server installation, and is the same for all servers in your system.

What you should know

Regardless of which expansion server you try to connect to, Server Admin always redirects you to the main server, if the following conditions are met:

- The expansion server is connected to the main server.
- The expansion server and the main server are running the same version (X.Y) of Security Center.

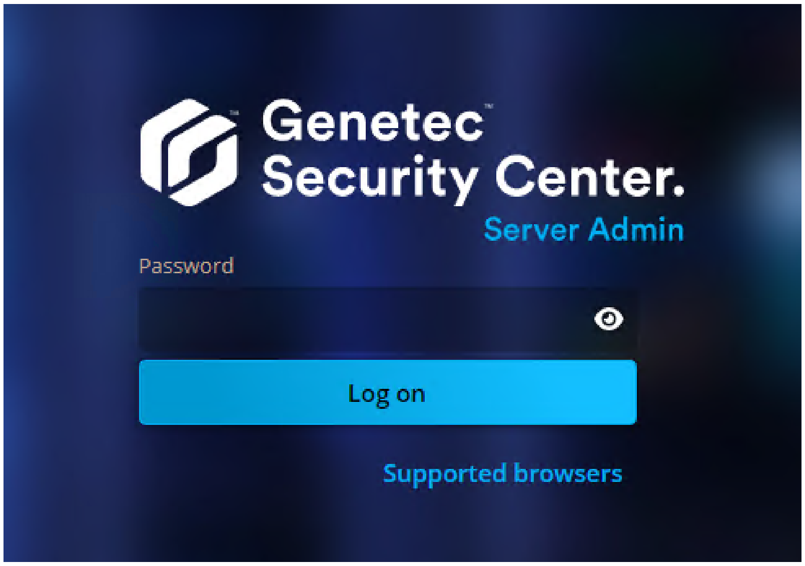
To open Server Admin using a web browser:

1 Do one of the following:

- If connecting to Server Admin from the local host, double-click **Genetec™ Server Admin** (⚙) in the *Genetec Security Center* folder in the Windows Start menu.
- If you are not on the main server, type `https://computer:port/Genetec` in your web browser, where `computer` is the hostname or the IP address of your server and `port` is the web server port specified during the Security Center expansion server installation.

NOTE: If you are connecting to a remote server, Server Admin always uses a secure connection (HTTPS). If your server is using a self-signed certificate, the browser warns you that your connection is unsafe. If you get the warning message, ignore it and proceed with the unsafe connection.

2 Enter the server password that you set during the server installation, and click **Log on**.



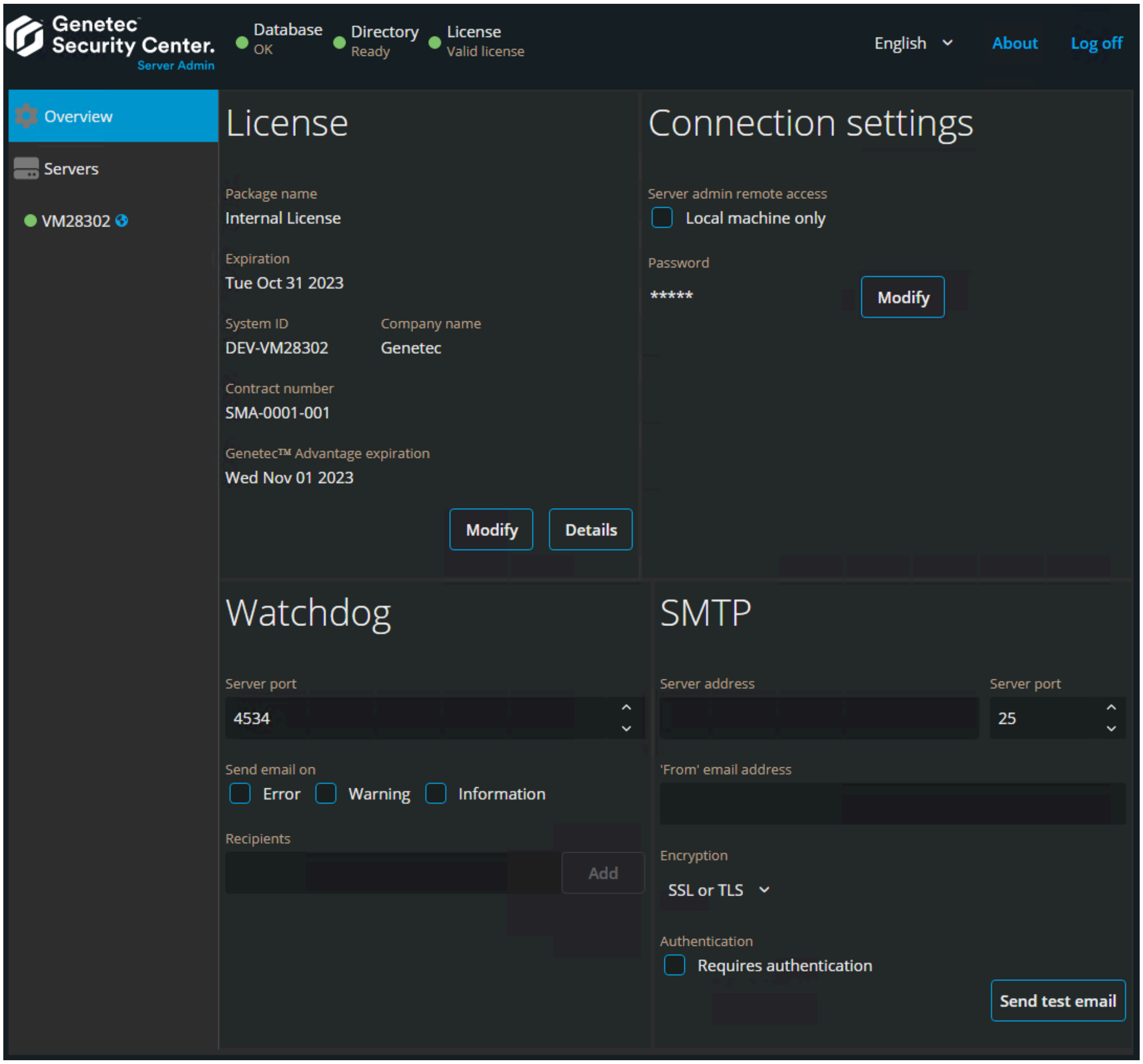
The Server Admin *Overview* page opens.

Related Topics

Server Admin - Overview page on page 99
What is Transport Layer Security protocol? on page 461

Server Admin - Overview page

The Server Admin - *Overview* page shows your Security Center license information, and the common settings (Watchdog, Connection, SMTP) that apply to all servers in your system.



Database: OK
Directory: Ready
License: Valid license

License
Package name: Internal License
Expiration: Tue Oct 31 2023
System ID: DEV-VM28302
Company name: Genetec
Contract number: SMA-0001-001
Genetec™ Advantage expiration: Wed Nov 01 2023

Connection settings
Server admin remote access: □ Local machine only
Password: *****

Watchdog
Server port: 4534
Send email on: □ Error □ Warning □ Information
Recipients:

SMTP
Server address:
Server port: 25
'From' email address:
Encryption: SSL or TLS
Authentication: □ Requires authentication

Dashboard (top left)

The dashboard indicates the status (🟢=ready, 🟠=getting ready, 🔴=not ready) of your system at all times, for the following components:

- **Database:** Directory database. Click to go to the Directory database configuration section.
- **Directory:** Directory role. Click to start, stop, or restart the Directory role.
- **License:** Security Center license. Click to activate the license or display the license details.

Servers (left pane)

List of all servers found on your system (only if you are connected to the main server). Click a server from the list to display its configuration page.

The status and function of each server is indicated as follows:

- 🌐**:** Primary Directory server (main server).
- 🌐**:** Secondary Directory server.
- **No icon:** Expansion server.
- 🟢**:** The server is up.
- 🔴**:** The server is down.
- 🟠**:** The server has problems.

License

Security Center license status and information.

- **Package name:** Software package name.
- **Expiration:** Date when your license expires.
- **System ID:** Your System ID number.
- **Company name:** Name of your company.
- **Contract number:** Number of your Genetec™ Advantage contract. If you did not purchase Genetec Advantage, this field will not be set.
- **Genetec™ Advantage expiration:** Expiry date of your Genetec Advantage contract.
- **Modify:** Click to activate or modify your Security Center license.
- **Details:** Click to view the details of your Security Center license.

Watchdog

Use this section to configure the *Genetec™ Watchdog* service. The role of the Watchdog is to ensure that the Genetec™ Server service is always running.

- **Server port:** Communication port between the Watchdog and the server.
- **Send email on:** Send email notifications from the Watchdog to a list of recipients for *Error*, *Warning*, and *Information* events.

  NOTE: No email is sent if the event is the direct cause of a manual user action, such as deactivating a role from Config Tool or stopping the Genetec™ Server service from Windows Services.
- **Recipients:** Security Center users who receive the Watchdog emails.

Connection settings

Use this section to configure the connection settings to Server Admin.

- **Local machine only:** Enable this option to restrict the Server Admin connections to the local machine.
- **Password:** Log on password for Server Admin.

SMTP

Use this section to configure the SMTP server responsible for handling email messages in Security Center.

- **Server address:** DNS name or IP address of your SMTP mail server.
- **Server port:** The server port is usually 25, though your mail server might use a different port.
- **“From” email address:** Email address shown as the sender of the email when the system needs to email a health notification through the Genetec™ Watchdog service, or email a message or report through an event-to-action.

  NOTE: This email address does not need to be real; it is only used to identify your system as the sender.
- **Use SSL connection:** Enable secure communication with the mail server.

- **Requires authentication:** Enable this option if your mail server requires authentication. If so, you need to enter a username and password.
- **Send test email:** To validate your SMTP configuration, enter a valid email address to send a test email to.

  NOTE: The test email is configured to be sent to the **"From" email address** by default.

Related Topics

Server Admin - Main server page on page 102

Server Admin - Expansion server page on page 105

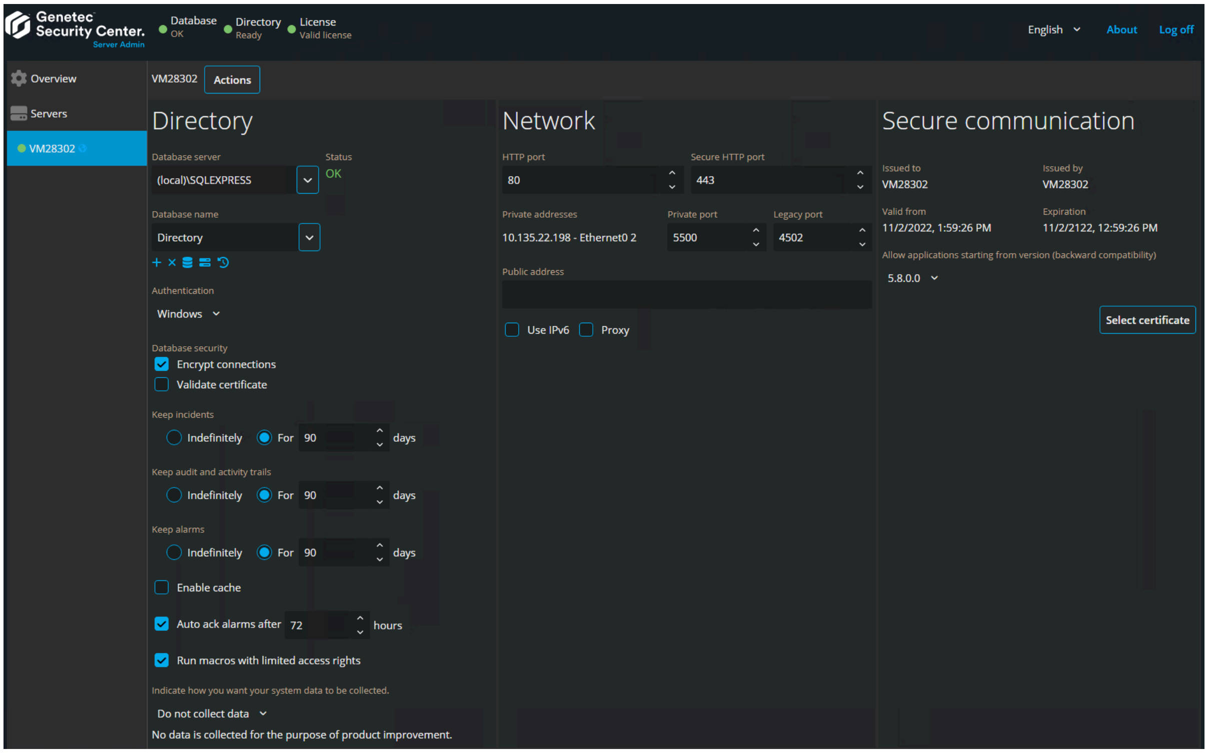
Activating Security Center license using the web on page 113

Activating Security Center license manually on page 116

Server - Properties tab on page 1291

Server Admin - Main server page

The Server Admin - *Main server* page lets you configure your Directory database and the settings pertaining to your main server.



Genetec Security Center. Server Admin | Database OK | Directory Ready | License Valid license | English | About | Log off

Overview | Servers | ● VM28302

VM28302 | Actions

Directory

Database server: (local)\SQLEXPRESS | Status: OK

Database name: Directory

Authentication: Windows

Database security

☑ Encrypt connections

□ Validate certificate

Keep incidents: ○ Indefinitely ● For 90 days

Keep audit and activity trails: ○ Indefinitely ● For 90 days

Keep alarms: ○ Indefinitely ● For 90 days

□ Enable cache

☑ Auto ack alarms after 72 hours

☑ Run macros with limited access rights

Indicate how you want your system data to be collected.

Do not collect data

No data is collected for the purpose of product improvement.

Network

HTTP port: 80 | Secure HTTP port: 443

Private addresses: 10.135.22.198 - Ethernet0 2 | Private port: 5500 | Legacy port: 4502

Public address:

□ Use IPv6 □ Proxy

Secure communication

Issued to: VM28302 | Issued by: VM28302

Valid from: 11/2/2022, 1:59:26 PM | Expiration: 11/2/2122, 12:59:26 PM

Allow applications starting from version (backward compatibility): 5.8.0.0

Select certificate

Actions

Click the **Actions** list beside the server name to see what actions can be applied to the main server.

The available actions are:

- **Directory:**
  - **Start/Stop:** Start or stop the Directory.
  - **Restart:** Restart the Directory.
  - **Deactivate:** Convert the main server to an expansion server.
- **Genetec™ Server:**
  - **Console:** Open the *Debug Console* page (reserved for Genetec™ Technical Support Engineers).
  - **Restart:** Restart the Genetec™ Server service. This action renders the server temporarily unavailable.

Directory

The *Directory* section shows the status and settings of the Directory database. The Directory database contains all system and entity configurations, the incident reports, and the alarm history.

NOTE: If you accessed Server Admin from Config Tool instead of through a web browser, you do not see the database commands (upgrading or restoring the database) because you are still connected to the Directory. You cannot modify the Directory database while you are still connected to it.

- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.

- **Database name:** Name of the database instance (default = Directory).
- **Actions:** Maintenance functions you can perform on the Directory database:
  - **Create database (✚):** Create a new database.
  - **Delete database (✖):** Delete the database.
  - **Database properties ( ):** Opens a dialog box showing the database information, and the automatic Backup and Email notification settings.
  - **Show progress ( ):** Opens a dialog box showing the past and current actions being performed on the database.
  - **Update database ( ):** Upgrade the database schema to the current version.
  - **Resolve conflicts ( ):** Resolve conflicts for imported entities.
  - **Backup/Restore ( ):** Opens a dialog box allowing you to back up or restore the Directory database.
- **Authentication:** Specifies which SQL Server authentication is to be used:
  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.
- **Keep incidents:** Specifies how long the incident reports are kept in the Directory database.
- **Keep audit and activity trails:** Specifies how long the entity configuration history and the activity history are kept in the Directory database.
- **Keep alarms:** Specifies how long the alarm history is kept in the Directory database.
- **Auto ack alarms after:** Lets the system automatically acknowledge all active alarms that do not get acknowledged before the specified time (default = 72 hours). When turned on, this option supersedes the **Automatic acknowledgment** option configured for each individual alarm. When the automatic acknowledgment of alarms is turned on at both the system and individual alarm level, it is the shortest delay that applies.
- **Run macros with limited access rights:** Runs macros in a subprocess with limited access to the Directory host OS to protect the system from malicious macro execution.
- **Indicate how you want your system data to be collected:** You can change your data collection preference selected at system installation. The options are:
  - **Do not collect data:** No data is collected for product improvement.
  - **Collect data anonymously:** System data are collected and shared with Genetec Inc., but all data that identify your company are first removed.
  - **Collect and link data to your system ID:** System data are linked to your system ID and shared with Genetec Inc. to facilitate proactive support and improve communication.

Network

Use this section to configure the network card and the TCP listening port used by the Genetec™ Server service.

- **HTTP port:** Port used by the Genetec™ Server service to listen to commands received from other Security Center servers on the public address.
- **Secure HTTP port:** Port used by Genetec™ Server service for secured HTTP connections.

- **Private address:** List of private addresses corresponding to the network interface cards (NIC) installed on this server. Only select the ones that are used for the communication between Security Center applications.
- **Private port:** Port used by the main server to listen to incoming connection requests, and by all servers for communication between themselves, on the private IP address. (default = 5500).

  NOTE: If you change this port on the main server, then all users must specify the new port number. This is found after the **Directory** name in the *Logon* dialog box, separated by a colon (:). This applies to all expansion servers. Specify the new port number after the **Security Center Directory** name in Server Admin, in the *Main server connection* section.
- **Legacy port:** Port used by the Genetec™ Server service to listen to commands received from servers running an older version of Security Center (default = 4502).
- **Public address:** Public address of the server.
  - **Use IPv6:** Use IPv6 for video streaming and communication between servers (only if your network supports it).
  - **Proxy:** Select this option if the server is used as the proxy server for a private network protected by a firewall.

Secure communication

Use this section to view the current *identity certificate* used by the server to communicate with other Security Center servers.

- **Issued to:** Subject of the current certificate. A *self-signed certificate* created at software installation appears in the form *GenetecServer-{MachineName}*.
- **Issued by:** Name of the *certificate authority (CA)* that issued the certificate. The issuer and the subject are the same for self-signed certificates.
- **Valid from/Expiration:** Validity period of the current certificate.
- **Select certificate (button):** Dialog box listing all certificates installed on this machine. You can use this dialog box to change the certificate used for this server.

  Some common certificate signature algorithms that we support are:

  - Elliptic Curve Digital Signature Algorithm (ECDSA)
  - Digital Signature Algorithm (DSA)
  - Rivest–Shamir–Adleman (RSA)

  NOTE: After changing the certificate, manually reconnect your ALPR units to the ALPR Manager role. For more information, see Adding a SharpV camera to the ALPR Manager on page 1029.
- **Allow application starting from version (backward compatibility):** To increase system security, limit backward compatibility to your current version (5.11). Select an older version if you have expansion servers running older versions in your system.

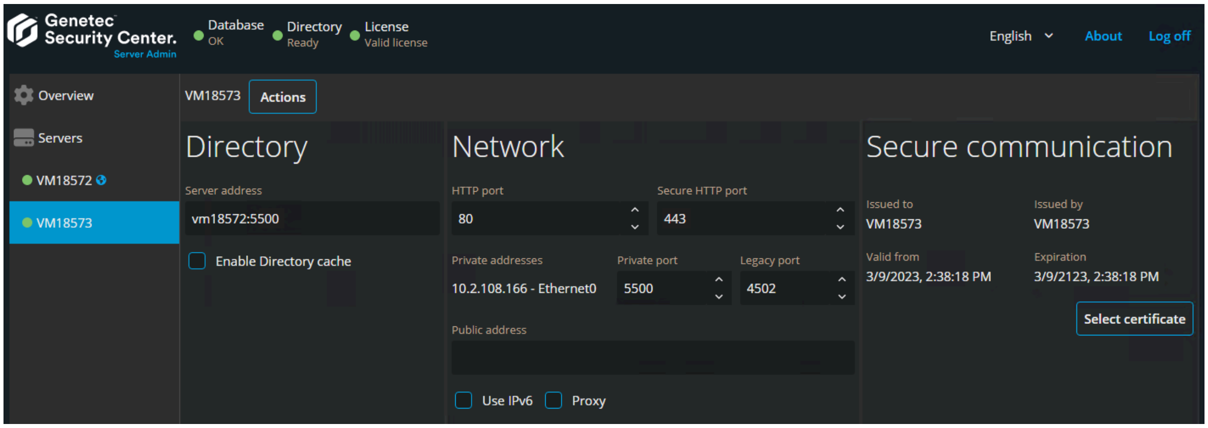
Related Topics

Server Admin - Overview page on page 99

Server - Properties tab on page 1291

Server Admin - Expansion server page

The Server Admin - *Expansion server* page shows all settings pertaining to the selected expansion server.



Directory

Server address: vm18572:5500

□ Enable Directory cache

Network

HTTP port: 80

Secure HTTP port: 443

Private addresses: 10.2.108.166 - Ethernet0

Private port: 5500

Legacy port: 4502

Public address:

□ Use IPv6 □ Proxy

Secure communication

Issued to: VM18573

Issued by: VM18573

Valid from: 3/9/2023, 2:38:18 PM

Expiration: 3/9/2123, 2:38:18 PM

Actions

Click the **Actions** list beside the server name to see what actions can be applied to the expansion server.

The available actions are:

- **Directory:**
  - **Activate:** Convert the expansion server to a main server.
- **Genetec™ Server:**
  - **Console:** Open the *Debug Console* page (reserved for Genetec™ Technical Support Engineers).
  - **Restart:** Restart the Genetec™ Server service. This action renders the server temporarily unavailable.

Main server connection

This section identifies the main server that the expansion server must connect to.

- **Server address:** The DNS name or the IP address of the main server.
- **Change password:** Only appears when no connection has been established between the expansion server and the main server. Click to set the password. Once the first contact is made, the expansion server sends its *identity certificate* to the main server, and the password is not needed again.

Network

Use this section to configure the network card and the TCP listening port used by the Genetec™ Server service.

- **HTTP port:** Port used by the Genetec™ Server service to listen to commands received from other Security Center servers on the public address.
- **Secure HTTP port:** Port used by Genetec™ Server service for secured HTTP connections.
- **Private address:** List of private addresses corresponding to the network interface cards (NIC) installed on this server. Only select the ones that are used for the communication between Security Center applications.
- **Private port:** Port used by the main server to listen to incoming connection requests, and by all servers for communication between themselves, on the private IP address. (default = 5500).

  NOTE: If you change this port on the main server, then all users must specify the new port number. This is found after the **Directory** name in the *Logon* dialog box, separated by a colon (:). This applies to all expansion servers. Specify the new port number after the **Security Center Directory** name in Server Admin, in the *Main server connection* section.

- **Legacy port:** Port used by the Genetec™ Server service to listen to commands received from servers running an older version of Security Center (default = 4502).
- **Public address:** Public address of the server.
  - **Use IPv6:** Use IPv6 for video streaming and communication between servers (only if your network supports it).
  - **Proxy:** Select this option if the server is used as the proxy server for a private network protected by a firewall.

Secure communication

Use this section to view the current *identity certificate* used by the server to communicate with other Security Center servers.

- **Issued to:** Subject of the current certificate. A *self-signed certificate* created at software installation appears in the form *GenetecServer-{MachineName}*.
- **Issued by:** Name of the *certificate authority (CA)* that issued the certificate. The issuer and the subject are the same for self-signed certificates.
- **Valid from/Expiration:** Validity period of the current certificate.
- **Select certificate (button):** Dialog box listing all certificates installed on this machine. You can use this dialog box to change the certificate used for this server.

  Some common certificate signature algorithms that we support are:

  - Elliptic Curve Digital Signature Algorithm (ECDSA)
  - Digital Signature Algorithm (DSA)
  - Rivest–Shamir–Adleman (RSA)

  NOTE: After changing the certificate, manually reconnect your ALPR units to the ALPR Manager role. For more information, see Adding a SharpV camera to the ALPR Manager on page 1029.

Related Topics

Server Admin - Overview page on page 99

Server - Properties tab on page 1291

Adding expansion servers

You can add expansion servers to your system at any time to increase the overall computing power of your system.

What you should know

An expansion server is any server machine in a Security Center system that does not host the Directory role. The purpose of the expansion server is to add to the processing power of the system.

Every Security Center system requires its own pool of servers to run the system's functions. You must ensure that enough computing power is available for your system to carry out its required functions.

To add an expansion server:

1. Install Security Center Server on the computer that you want to add to the server pool.

   For more information about installing Security Center Server, see the *Security Center Installation and Upgrade Guide*.
2. Connect that computer to the Security Center's main server.

   The main server is the one that hosts the Directory role. This is done with the Server Admin through a web browser.
3. Open Config Tool on any workstation.
4. From the homepage, open the *Network view* task.

   The server you just added should appear in the network tree. The name of the server entity should match the domain name of the server.
5. Select the new server entity, and click the **Properties** tab.

   If the server is used as the proxy server for a private network protected by a firewall, set its **Public address** and **Port** as configured by your IT department.
6. Click **Apply**.

You can now assign roles to the server.

Related Topics

Security Center architecture overview on page 5

Converting the main server to an expansion server

You can convert your main server to an expansion server, if you want a different machine to take on the role of the main server.

Before you begin

- Prepare another server to take over as the new main server on your system. For more information about installing Security Center on a main server, see the *Security Center Installation and Upgrade Guide*.
- If you need to keep your system configuration, and if the Directory database is currently hosted on your main server, then move the Directory database to a different server (this could be the new main server you prepared).

What you should know

You convert a main server to an expansion server by deactivating the Directory role on your server using Server Admin.

CAUTION: This operation restarts the Genetec™ Server service which temporarily deactivates all roles hosted on your server. You must log on again to Server Admin to connect your old main server (converted to an expansion server) to the new main server you prepared.

To convert the main server to an expansion server:

1. Log on to Server Admin on your computer using a web browser.
2. From the server list, select the main server (🌐).

   The Server Admin - Main server page is displayed.
3. Beside the server name, click **Actions** > **Deactivate**.
4. In the confirmation dialog box that appears, click **Continue**.

   The Genetec™ Server service restarts. You are temporarily logged off from Server Admin.
5. Reset the server identification ID.
   a) Launch Notepad with the **Run as administrator** option.
   b) In Notepad, open *GenetecServer.gconfig* found in the *ConfigurationFiles* folder under the Security Center installation folder (*C:\Program Files (x86)\Genetec Security Center 5.11*).
   c) Find and delete the following phrase <serverIdentification id="<*guid*>" />.
   d) Save your changes and close the file.
6. Open a web browser and enter http://machine/Genetec in the address bar, where machine is the DNS name or the IP address of your server.
7. Log on again to Server Admin.

   The Server Admin - Expansion server page is displayed.
8. Under the *Main server connection* section, enter the name and password of the main server that the expansion server is supposed to connect to, and click **Save**.
9. In the confirmation dialog box that appears, click **Yes**.

   The Genetec™ Server service restarts. You are temporarily logged off from Server Admin.
10. Close your browser page and open a new page.
11. Log on again to Server Admin, and verify that you are connected to the new main server.

Related Topics

Replacing the main server on page 125

Converting an expansion server to the main server

To replace your existing main server or to start a new system, you can convert an expansion server into the main server.

Before you begin

If you are replacing an old main server, and if the Directory database was hosted on your old main server, move the Directory database to the server you want to convert, or to a third computer.

What you should know

You convert an expansion server to a main server by activating the Directory role on your server using Server Admin.

CAUTION: This operation restarts the Genetec™ Server service which temporarily deactivates all roles hosted on your server. You must log on again to Server Admin to activate your software license on your new main server.

To convert an expansion server to the main server:

1. Log on to Server Admin on your computer using a web browser.
2. From the server list, select the expansion server you want to convert.

   The Server Admin - Expansion server page is displayed.
3. Beside the server name, click **Actions** > **Activate**.
4. In the confirmation dialog box that appears, click **Continue**.

   The Genetec™ Server service restarts. You are temporarily logged off from Server Admin.
5. Open a web browser, and enter http://machine/Genetec in the address bar, where machine is the DNS name or the IP address of your server.
6. Log on again to Server Admin.

   The Server Admin - Overview page is displayed.
7. Activate the software license on the new main server.
8. If you are replacing an old main server, configure the database settings on the Server Admin - Main server page so that this server connects to your existing Directory database.

   This operation forces the expansion server (promoted to main server) to take on the identity of the old main server. This means that if there were roles hosted on the expansion server before, they must be moved to the *new* main server, because the ID of the expansion server has changed.
9. From the Config Tool home page, open the *Network view* task.
10. In the network view, if you see an offline copy of the expansion server you just converted (🟥), delete it.

After you finish

- (Optional) Convert the original main server to an expansion server.
- Connect all the expansion servers on your system to the new main server.

Related Topics

Connecting expansion servers to the main server on page 110

Replacing the main server on page 125

Connecting expansion servers to the main server

Whenever you move your main server to a new computer, you must use Server Admin to reconnect all the expansion servers in your Security Center system to the main server.

Before you begin

After successfully installing an expansion server, it automatically connects to the main server. These steps are only necessary if:

- You entered the wrong connection parameters to the main server during the expansion server installation.
- You moved the main server to a different computer.
- You changed the password on the main server.
- You enabled Directory authentication on your expansion server, but your Directory certificate is not signed by a trusted certificate authority.

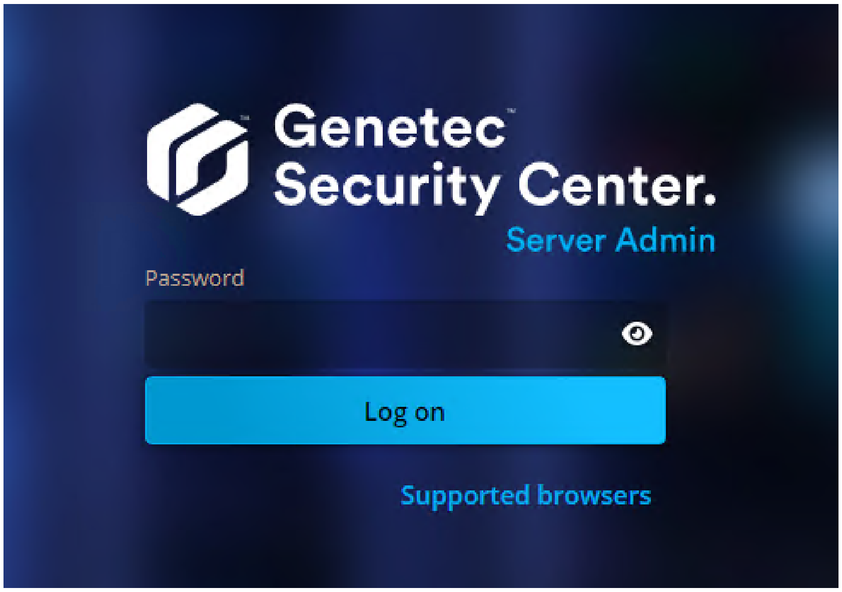
To connect an expansion server to the main server:

1 Open the Server Admin web page on the expansion server by doing one of the following:

- In the address bar of your web browser, type https://computer:port/Genetec, where computer is the hostname or the IP address of your expansion server, and port is the web server port specified during the Security Center Server installation.

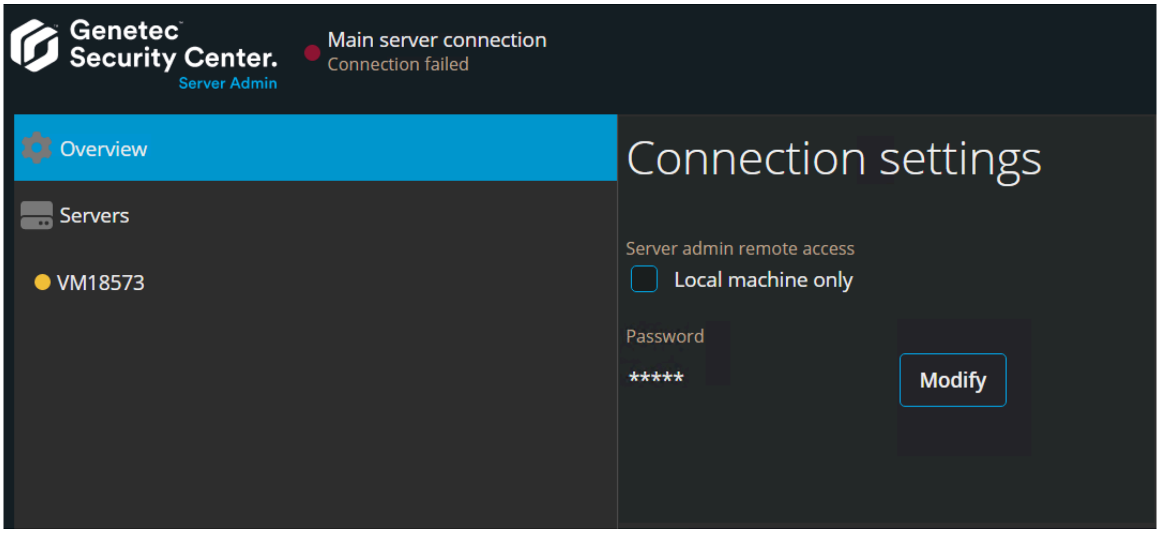
  You can omit the web server port if you are using the default value (443).
- If connecting to Server Admin from the local host, double-click **Genetec™ Server Admin** (⚙) in the *Genetec Security Center* folder in the Windows Start menu.

2 Enter the password and click **Log on**. The initial expansion server password is the main server password that was entered during the expansion server installation. This password is synchronized with the current main server password after the expansion server successfully connects to the main server.



The Server Admin *Overview* page appears.

3 If you are not connected to the main server, click **Main server connection** at the top of the Server Admin window.



4 Enter the **Server address** (main server hostname or IP address) and **Password**, and then click **Save**.

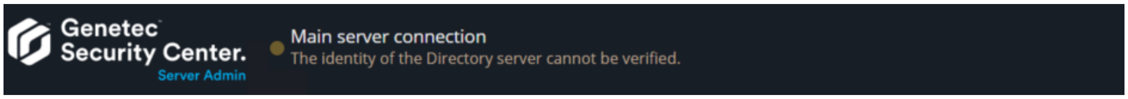
5 When prompted to restart the service, click **Yes**.

While the Genetec™ Server service restarts, you are temporarily logged off from Server Admin.

6 After the Genetec™ Server service restarts, log back on to Server Admin to verify the main server connection.

The main server is connected.

If **Always validate the Directory certificate** is set, you might see a message that the identity of the Directory server cannot be verified.

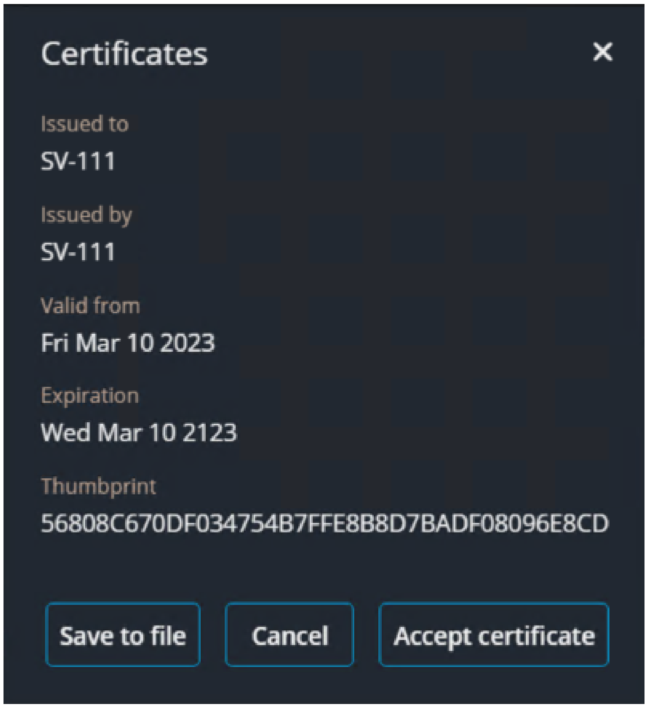


The identity of the Directory server cannot be verified.

7 If the identity of the Directory server cannot be verified, do the following:

a) Click **Main server connection**.

b) In the dialog box, verify that the certificate of your main server is as expected, and click **Accept certificate**.



Certificates

Issued to
SV-111

Issued by
SV-111

Valid from
Fri Mar 10 2023

Expiration
Wed Mar 10 2123

Thumbprint
56808C670DF034754B7FFE8B8D7BADF08096E8CD

IMPORTANT: The accepted certificate is stored in a local allowlist, and you should not be prompted to accept it again. If you are, then you should immediately notify your IT department.

BEST PRACTICE: To avoid having to accept the main server certificate every time someone connects to it from a new machine, only use certificates signed by a certification authority that is trusted by your company's IT.

c) Click **Save**.

d) When prompted to restart the service, click **Yes**.

While the *Genetec™ Server* service restarts, you are temporarily logged off from Server Admin.

The expansion server is now connected to the main server. The two servers can remain connected, even when you change the certificate, on one or both of the servers. For this to work, the two servers must be connected while the change is made.

Related Topics

What is Directory authentication? on page 462

Activating Security Center license using the web

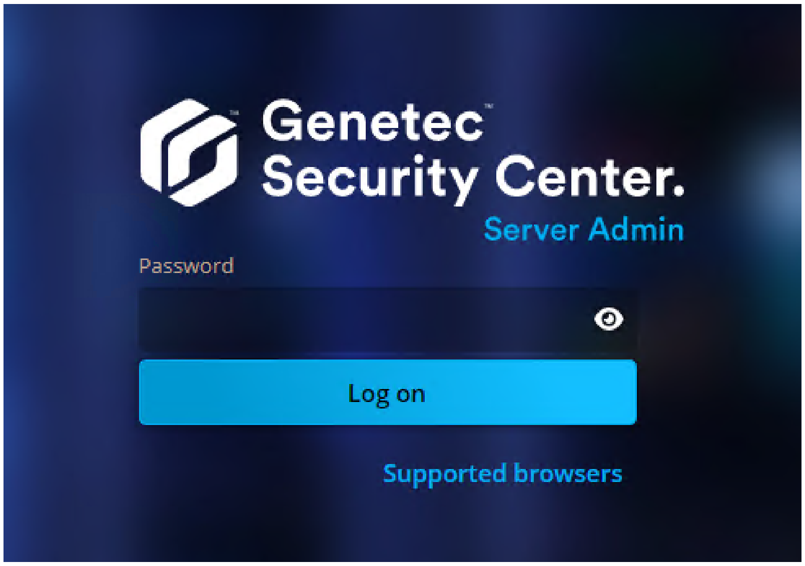
After you install Security Center on the main server or promote an expansion server to a main server, you must activate your Security Center license on the main server. If you have Internet access, you can activate your Security Center license using *web activation* from Server Admin.

To activate your Security Center license using web activation:

1 Open the Server Admin web page by doing one of the following:

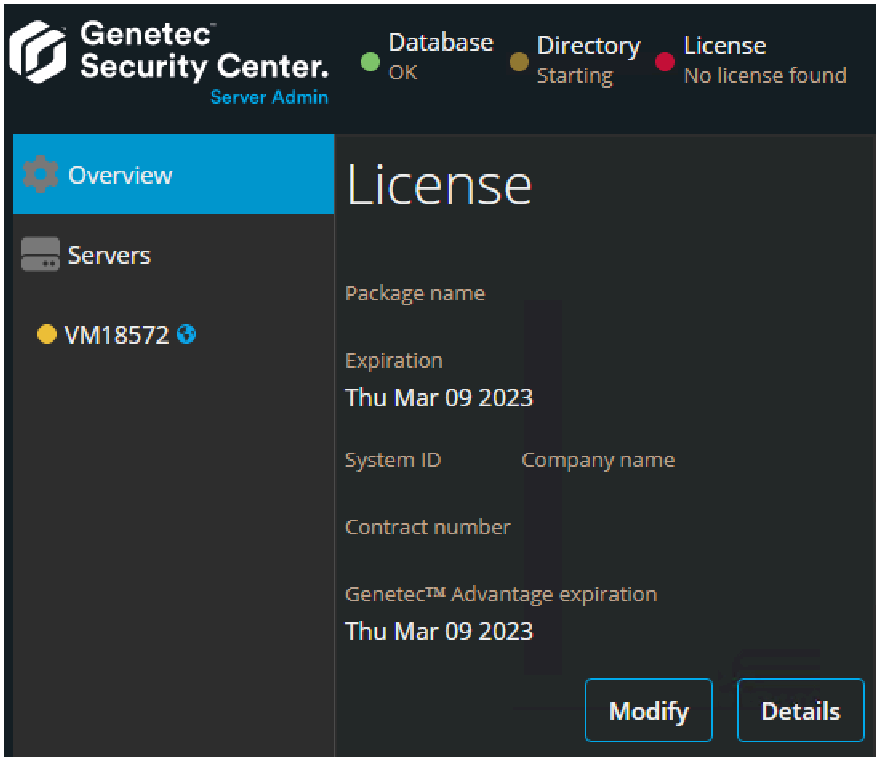
- If connecting to Server Admin from the local host, double-click **Genetec™ Server Admin** (⚙) in the *Genetec Security Center* folder in the Windows Start menu.
- If you are not on the main server, type https://computer:port/Genetec in your web browser, where computer is the hostname or the IP address of your server and port is the web server port specified during the Security Center expansion server installation.

2 Enter the server password that you set during the server installation, and click **Log on**.



The Server Admin *Overview* page opens.

3 In the **License** section, click **Modify**.



License

Package name

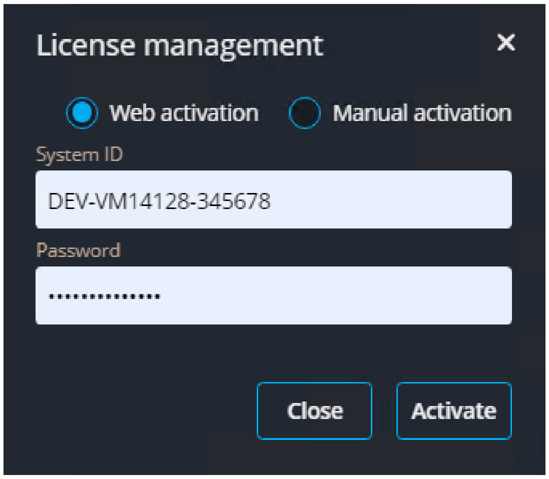
Expiration
Thu Mar 09 2023

System ID
Company name

Contract number

Genetec™ Advantage expiration
Thu Mar 09 2023

4 In the *License management* dialog box, click **Web activation** and enter your **System ID** and **Password**. Your system ID and password are specified in the *Security Center License Information* document. Our Customer Service team sends you this document when you purchase the product.



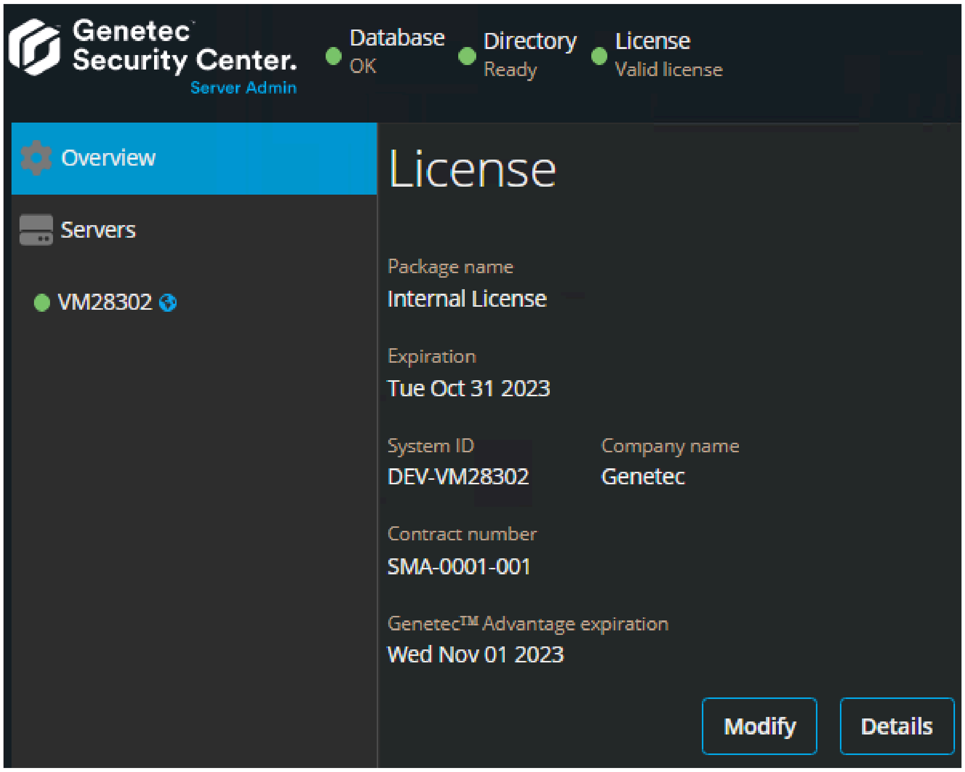
License management

● Web activation ○ Manual activation

System ID
DEV-VM14128-345678

Password
••••••••••••••

5 Click **Activate**.
Your license information appears in the *License* section of the Server Admin *Overview* page.



License

Package name
Internal License

Expiration
Tue Oct 31 2023

System ID
DEV-VM28302

Company name
Genetec

Contract number
SMA-0001-001

Genetec™ Advantage expiration
Wed Nov 01 2023

Activating Security Center license manually

After you install Security Center on the main server or promote an expansion server to a main server, you must activate your Security Center license on the main server.

What you should know

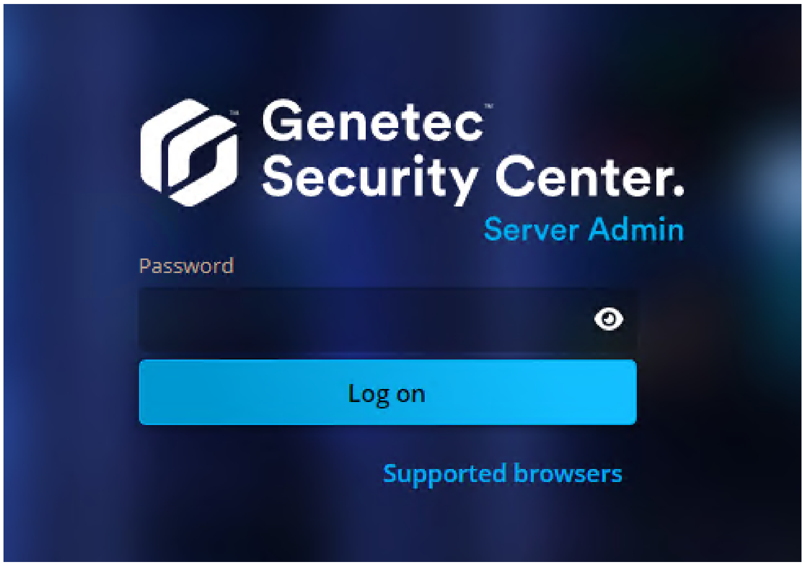
If you do not have Internet access, you can manually activate your Security Center license from Server Admin and the Genetec™ Technical Assistance Portal (GTAP).

To activate your Security Center license manually:

1 Open the Server Admin web page by doing one of the following:

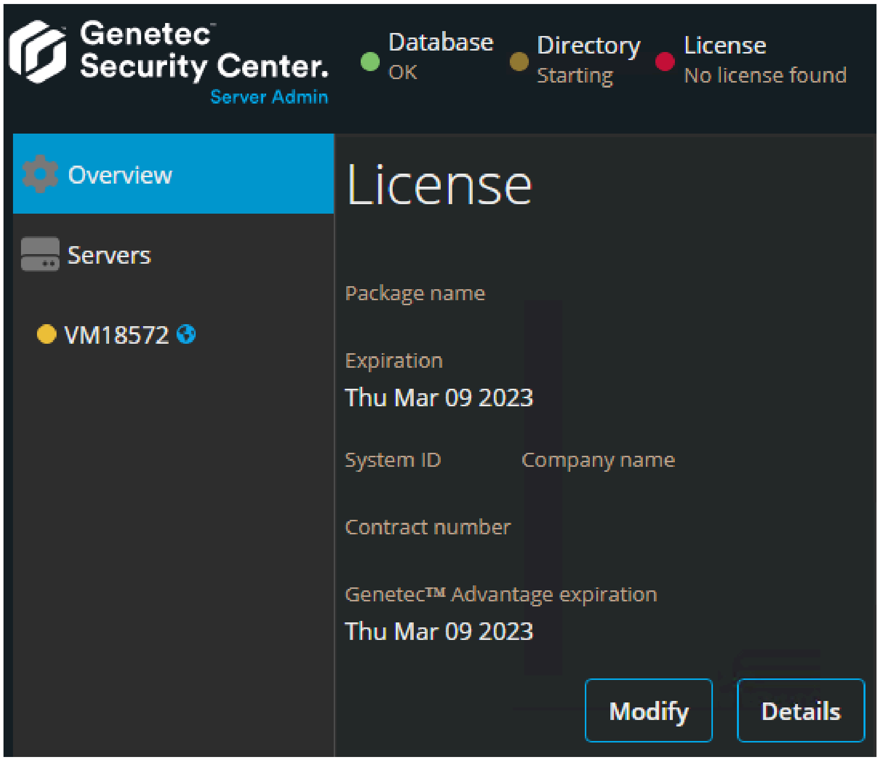
- If connecting to Server Admin from the local host, double-click **Genetec™ Server Admin** (⚙) in the *Genetec Security Center* folder in the Windows Start menu.
- If you are not on the main server, type https://computer:port/Genetec in your web browser, where computer is the hostname or the IP address of your server and port is the web server port specified during the Security Center expansion server installation.

2 Enter the server password that you set during the server installation, and click **Log on**.



The Server Admin *Overview* page opens.

3 In the **License** section, click **Modify**.



Database
OK

Directory
Starting

License
No license found

License

Package name

Expiration
Thu Mar 09 2023

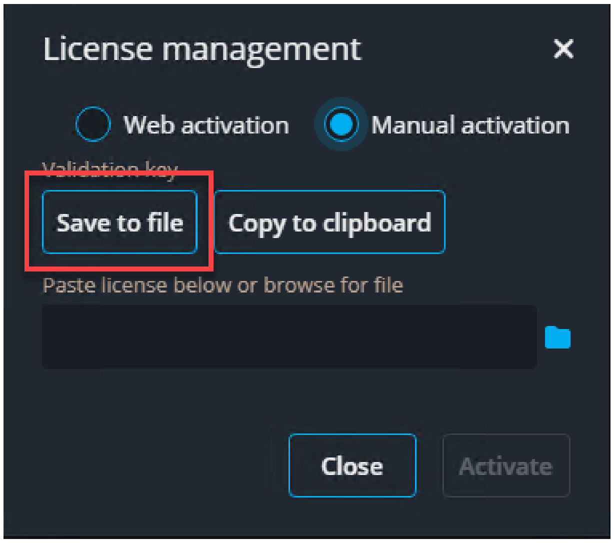
System ID

Company name

Contract number

Genetec™ Advantage expiration
Thu Mar 09 2023

4 In the *License management* dialog box, click **Manual activation**, and then under *Validation key*, click **Save to file**.



License management

○ Web activation ● Manual activation

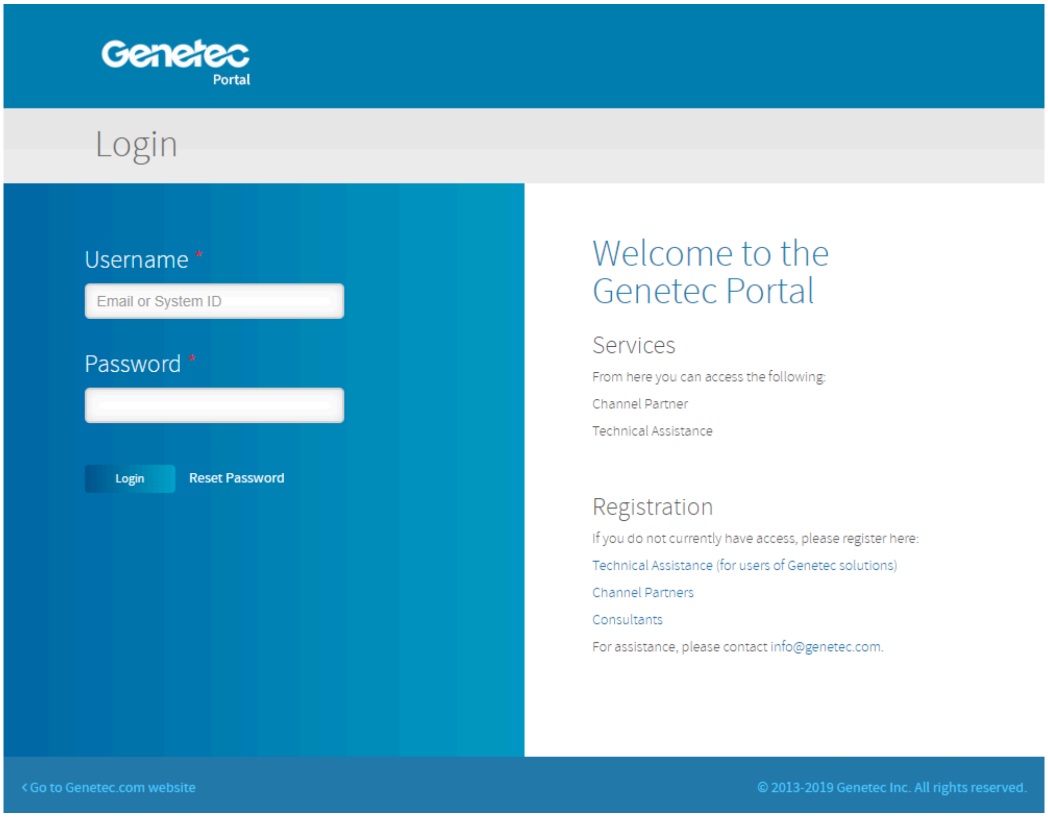
Validation key

Paste license below or browse for file

The validation key is a sequence of numbers (in hexadecimal text format) generated by Security Center that uniquely identifies your server. The validation key is used to generate the license key that unlocks your Security Center software. The license key can only be applied to the server identified by the validation key.

A text file named *validation.vk* is saved to your default *Downloads* folder. Copy the file to a USB key or a location that you can access from a computer that has internet access.

5 From a computer with internet access, open GTAP at: https://portal.genetec.com/support.



Genetec
Portal
Login
Username *
Email or System ID
Password *
Login
Reset Password
Welcome to the
Genetec Portal
Services
From here you can access the following:
Channel Partner
Technical Assistance
Registration
If you do not currently have access, please register here:
Technical Assistance (for users of Genetec solutions)
Channel Partners
Consultants
For assistance, please contact info@genetec.com.
‹ Go to Genetec.com website
© 2013-2019 Genetec Inc. All rights reserved.

6 On the *Login* page, do one of the following:

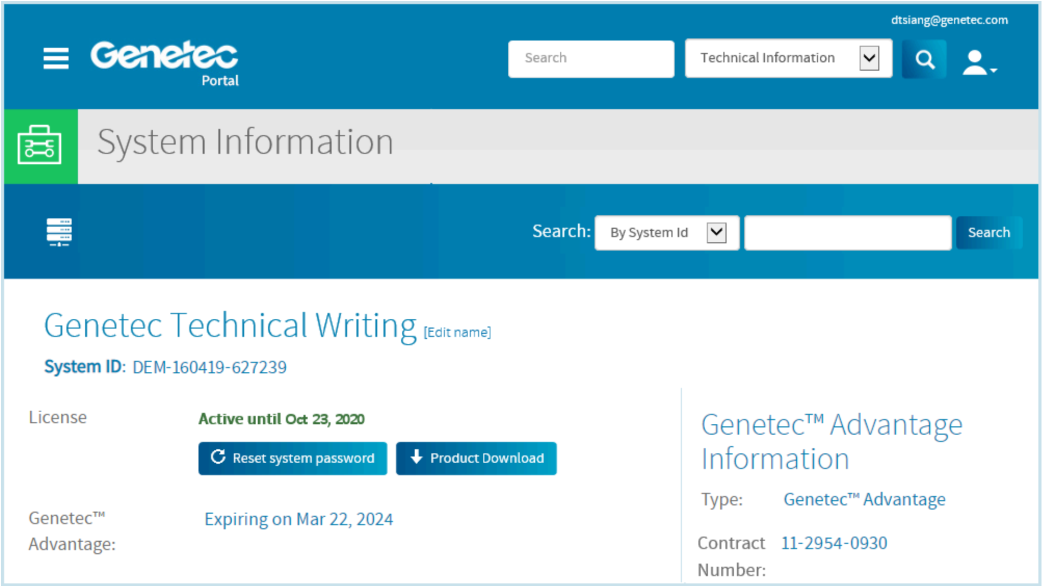
- Enter your system ID and password, and then click **Login**.

  Your system ID and password are specified in the *Security Center License Information* document. Our Customer Service team sends you this document when you purchase the product.
- Enter the email address for your GTAP user account and password, and then click **Login**

7 On the GTAP homepage, open the **Genetec Portal** menu and click **Technical Assistance** > **System Management**.

8 On the *System Management* page, type your system ID and click **Search**.

The *System Information* page opens.



Genetec Technical Writing

System ID: DEM-160419-627239

License: Active until Oct 23, 2020

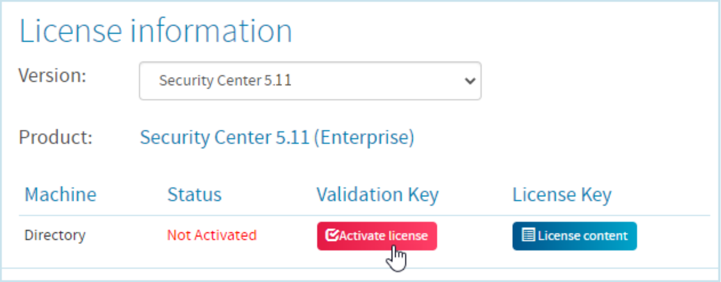
Genetec™ Advantage: Expiring on Mar 22, 2024

Genetec™ Advantage Information

Type: Genetec™ Advantage

Contract Number: 11-2954-0930

9 In the *License information* section, click **Activate license**.



License information

Version: Security Center 5.11

Product: Security Center 5.11 (Enterprise)

Machine	Status	Validation Key	License Key
Directory	Not Activated	Activate license	License content

10 In the dialog box that opens, browse to your validation key (.vk file), and click **Submit**.

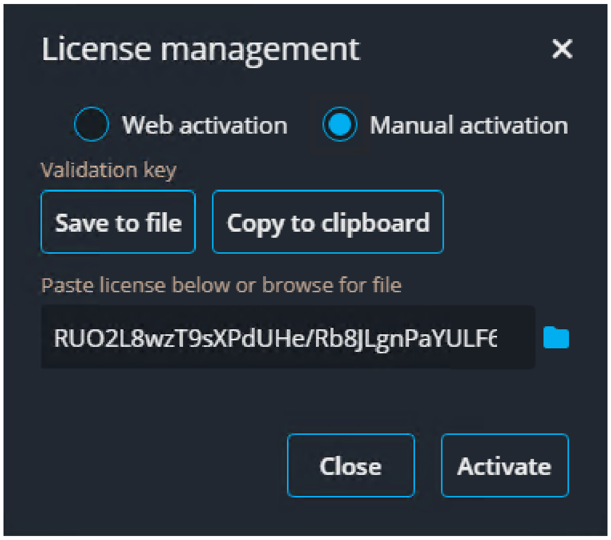
11 When you receive the License activation successful message, click **Download** under *License Key* and save the license key to a file.

The default file name is your system ID, followed by *_Directory_License.lic*.

12 Return to the Server Admin that is connected to your Security Center main server.

13 In the *License management* dialog box, do one of the following:

- Paste your license information from the license key file by copying the content from a text editor.
- Browse for the license key (.lic file), and click **Open**.



○ Web activation ● Manual activation

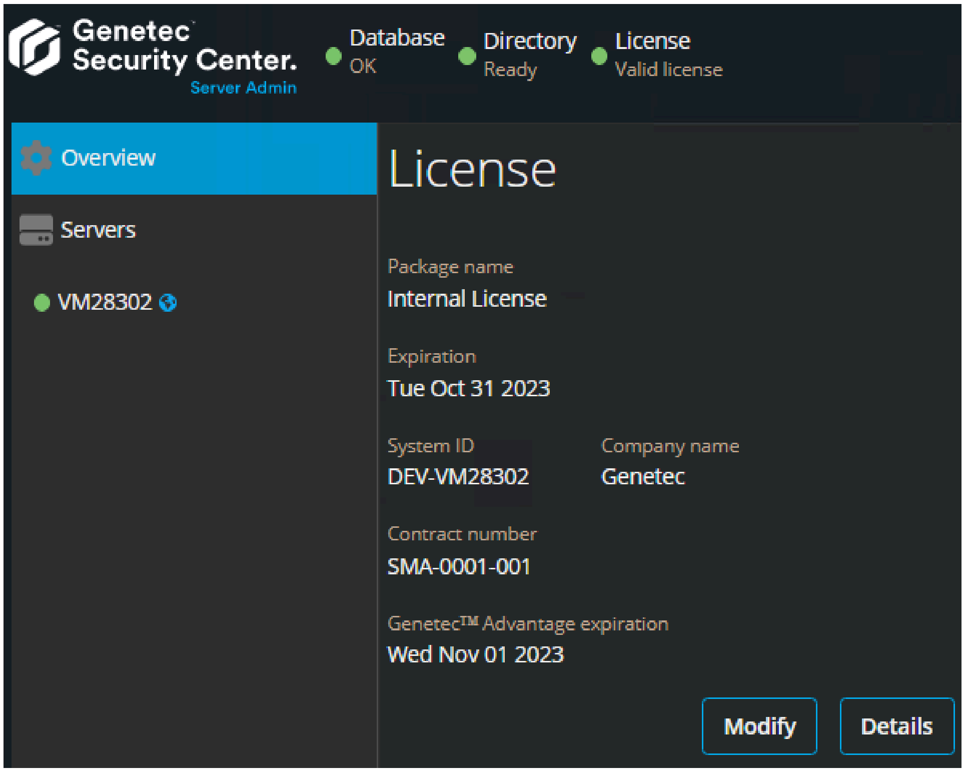
Validation key

Paste license below or browse for file

RUO2L8wzT9sXPdUHe/Rb8JLgnPaYULF€

14 Click **Activate**.

Your license information appears in the *License* section of the Server Admin *Overview* page.



Database OK

Directory Ready

License Valid license

License

Package name
Internal License

Expiration
Tue Oct 31 2023

System ID
DEV-VM28302

Company name
Genetec

Contract number
SMA-0001-001

Genetec™ Advantage expiration
Wed Nov 01 2023

Reapplying Security Center license

Every time your Security Center license is updated (new camera connections added, expiry date extended, and so on), you must reapply it to your main server for the changes to take effect.

What you should know

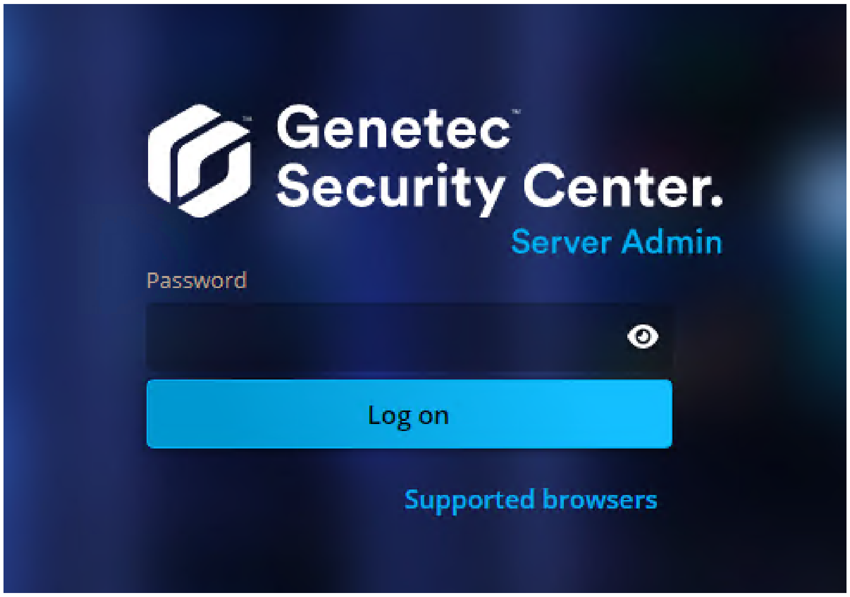
Reapplying your license does not require *reactivating* your license.

- If you replaced your main server with a new machine, activate your license on the new machine instead.
- If you have multiple Directory servers configured for failover, reapply your license from Config Tool instead.

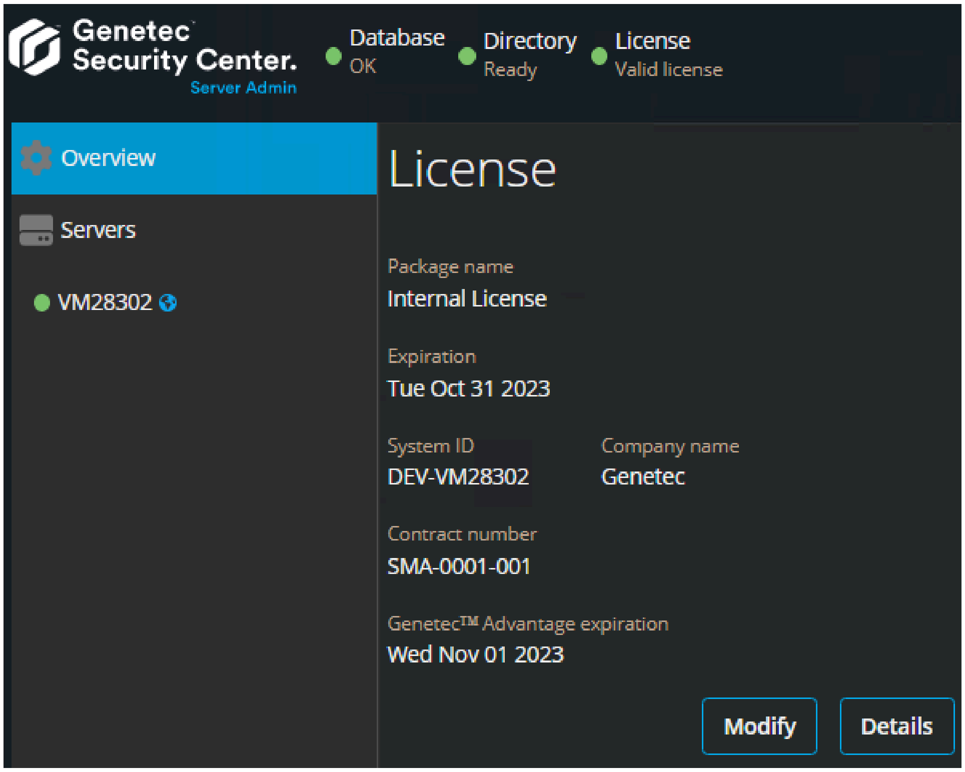
To reapply your Security Center license:

1 Open Server Admin.

2 Enter the server password that you set during the server installation, and click **Log on**.



3 Under the *License* section of the *Overview* page, click **Modify**.



Database
OK

Directory
Ready

License
Valid license

License

Package name
Internal License

Expiration
Tue Oct 31 2023

System ID
DEV-VM28302

Company name
Genetec

Contract number
SMA-0001-001

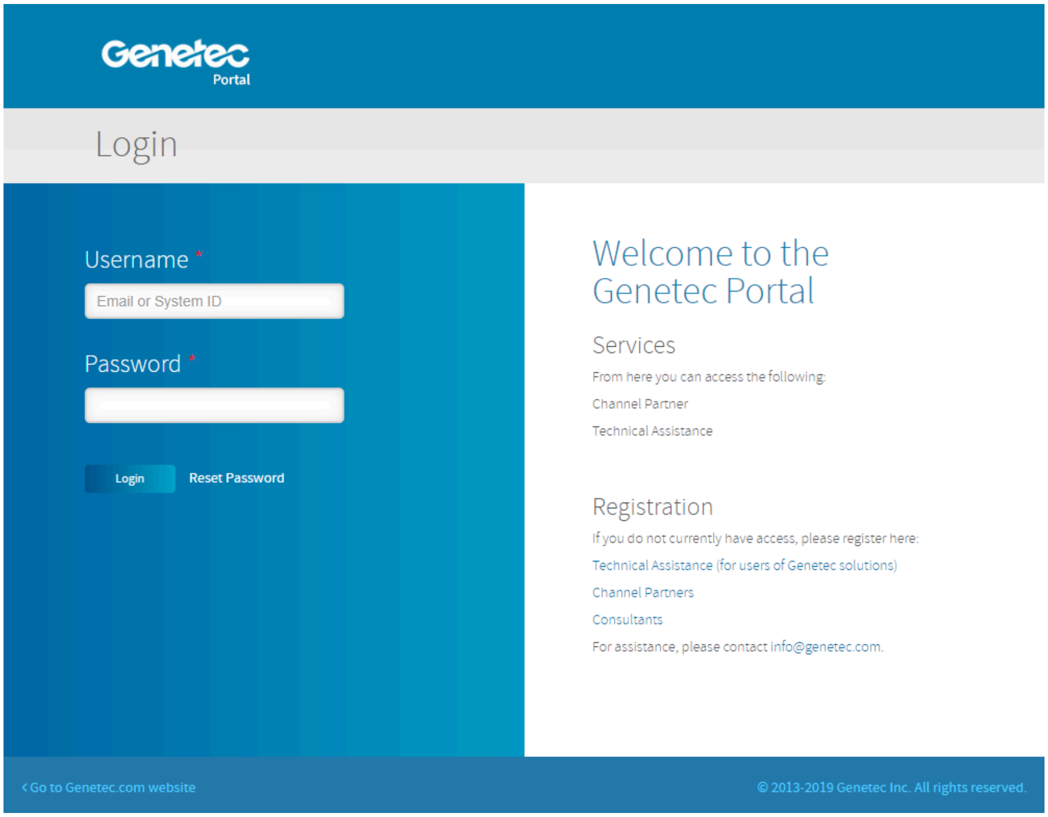
Genetec™ Advantage expiration
Wed Nov 01 2023

4 In the *License management* dialog box, reapply your license in one of the following ways:

- **Web activation:** (Recommended) Reapply your license from the Internet. In the dialog box that opens, enter your *System ID* and *Password* and click **Activate**. The process is complete.

  Your system ID and password are specified in the *Security Center License Information* document. Our Customer Service team sends you this document when you purchase the product.
- **Manual activation:** If your computer does not have Internet access, reapply your Security Center license manually using a license file. Continue with the next step.

5 From a computer with internet access, open GTAP at: https://portal.genetec.com/support.



Genetec Portal

Login

Username *

Email or System ID

Password *

Login Reset Password

Welcome to the Genetec Portal

Services

From here you can access the following:

Channel Partner

Technical Assistance

Registration

If you do not currently have access, please register here:

Technical Assistance (for users of Genetec solutions)

Channel Partners

Consultants

For assistance, please contact info@genetec.com.

‹ Go to Genetec.com website

© 2013-2019 Genetec Inc. All rights reserved.

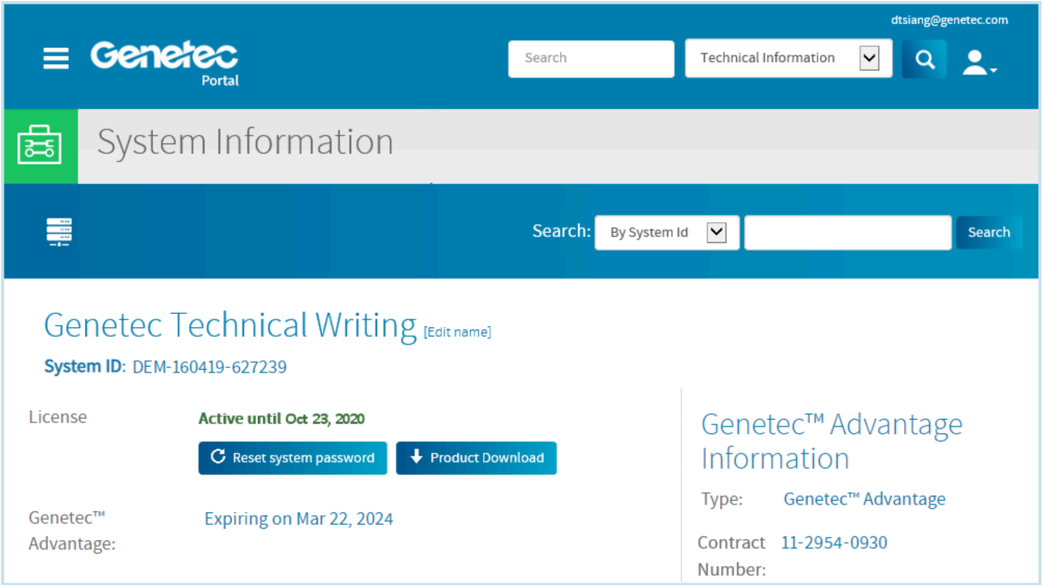
6 On the *Login* page, do one of the following:

- Enter your system ID and password, and then click **Login**.
- Enter your GTAP user account (your email address) and password, and then click **Login**

7 On the GTAP homepage, open the **Genetec Portal** menu and click **Technical Assistance** > **System Management**.

8 On the *System Management* page, type your system ID and click **Search**.

The *System Information* page opens.



dtsiang@genetec.com

Genetec Portal

Search

Technical Information

System Information

Search: By System Id

Search

Genetec Technical Writing [Edit name]

System ID: DEM-160419-627239

License: Active until Oct 23, 2020

Reset system password

Product Download

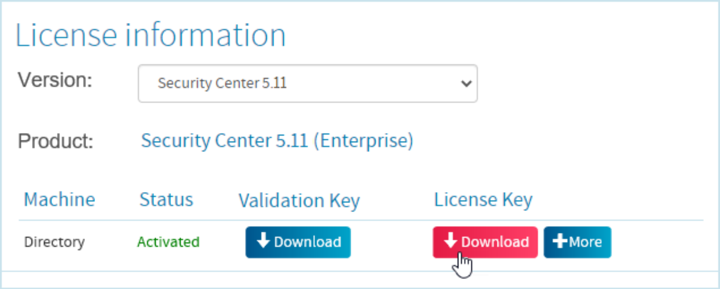
Genetec™ Advantage: Expiring on Mar 22, 2024

Genetec™ Advantage Information

Type: Genetec™ Advantage

Contract Number: 11-2954-0930

9 In the *License information* section, and do one of the following:



License information

Version: Security Center 5.11

Product: Security Center 5.11 (Enterprise)

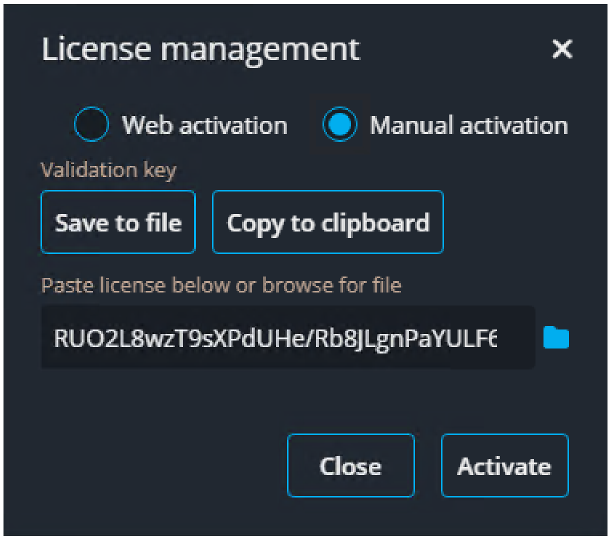
Machine	Status	Validation Key	License Key
Directory	Activated	Download	Download +More

- Below **License Key**, click **Download**, and save the license key to a file.
- To have the license key (.lic file) sent to you through email, click **More** > **Send by email**, enter your email address, and click **OK**.

10 Return to the Server Admin that is connected to your Security Center main server.

11 In the *License management* dialog box, do one of the following:

- Paste your license information from the license key file by copying the content from a text editor.
- Browse for the license key (.lic file), and click **Open**.



License management

○ Web activation ● Manual activation

Validation key

Paste license below or browse for file

RUO2L8wzT9sXPdUHe/Rb8JLgnPaYULF€

12 Click **Activate**.

Replacing the main server

When your main server is no longer adequate, you can replace it with a new server, activate your Security Center license on the new server, and connect all expansion servers to the new server.

Before you begin

If you have multiple Directory servers configured, read Replacing the main server in a Directory failover environment on page 181, instead.

What you should know

This server migration scenario works with the following assumptions:

- You have a single Directory system (no Directory failover configuration).
- The Directory database resides on the main server (no remote database access required).
- The SQL Server running on the new server is at the same version or newer than the SQL Server running on the old server.

  This is to ensure that you can restore your old database on the new machine. You can always restore a database backed up on an older version of SQL Server and restore it on a newer version of SQL Server, but the reverse is not necessarily true.
- Your old main server is still running.
- The old and new main servers are on the same network domain.

NOTE: Replacing the main server requires an interruption of service of up to 3 hours. The larger the system, the more time it takes to backup up and restore the Directory database and to reconnect the expansion servers. As a rule of thumb, you can estimate half an hour for the backup and restore, and one extra hour for every 25 expansion servers you need to reconnect to the new server. Schedule your maintenance window at a time that is the least disruptive to your operations. You can carry out this procedure up to the point where we tell you to wait for the scheduled maintenance window. We advise that you reserve a 4-hour maintenance window to carry out this operation.

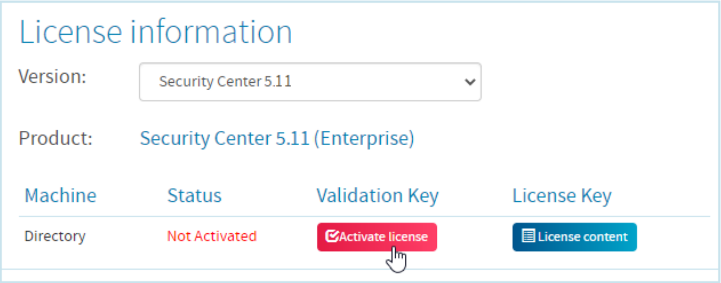
To replace the main server:

1 Install Security Center on the new machine using the *Main server* configuration, but do not activate the license.

  For more information, see the *Security Center Installation and Upgrade Guide*.

2 Contact Genetec™ Customer Services to reset your Security Center license so you can activate it on the new server.

  Verify on GTAP (https://portal.genetec.com/support) that the **Activate license** button for your system is enabled.



License information

Version: Security Center 5.11

Product: Security Center 5.11 (Enterprise)

Machine	Status	Validation Key	License Key
Directory	Not Activated	Activate license	License content

3 Activate your Security Center license on the new server.

  For more information, see the *Security Center Installation and Upgrade Guide*.

  NOTE: The new server is not yet part of your system. It is a system on its own.

4. If you have other roles than the Directory that run on your main server and that need their own database, such as the Health Monitor role, back up their databases.
5. Wait for the scheduled maintenance to start before continuing with the next step.

   Starting from the next step, your system will be down until the end of the process.
6. Back up your Directory database.
   a) Open Server Admin and connect to your old main server.
   b) At the top of the browser window, click **Directory** > **Stop**.

      This ensures that the database is not being accessed while you are backing it up.
   c) Click **Database** > **Properties** ( ), set the **Destination folder** for your database backup, and click **OK**.

      Make sure the backup folder can be accessed from your new server.
   d) Click **Backup/Restore** ( ) > **Backup now**.
   e) Click **Close**.
7. Restore the Directory database (.bak file) onto the new main server.
   a) Open Server Admin and connect to your new main server.
   b) Click **Database** > **Backup/Restore** ( ), select the backup file you want to restore, and click **Restore now**.
   c) Click **Close**.

   NOTE: Some Server Admin settings such as *Secure communication*, *SMTP*, and *Watchdog*, are not carried over to the new server through the database restore. In case you need to retrieve the old settings, you can find them in the *GenetecUtility32_ConfigurationFilesBackup* folder under the database backup folder. For more information, contact Technical support.
8. If you are using trusted certificates, restore the old main server certificate unto the new main server.
   a) Import the certificate with private keys to the new main server.
   b) Open Server Admin on the new main server.
   c) In the *Secure communication* section, click **Select certificate**.
   d) Select the imported certificate and click **Select** > **Save**.
9. Connect all your expansion servers to the new main server.
10. Do one of the following:
    - Convert the old main server to an expansion server.
    - Decommission your old main server.

      We recommend that you do this in two stages. For now, disable the Genetec™ Server service on your old server to prevent the service from starting by accident. When the new server is fully operational, uninstall Security Center from the old server.
11. Open Config Tool and connect it to the new main server, using your old *Admin* credentials.
12. Open the *Network view* task, and confirm that all your expansion servers are online ( ).

    You should also see an offline copy ( ) for each server. Do not delete them yet.
13. Open the *System* task and click the **Roles** view.
14. Recreate the Media Router role database.
    a) Select Media Router from the role list and click **Resources**.
    b) Click **Create a database** (➕).
    c) In the window that opens, click **Overwrite existing database** > **OK**.
15. For the remaining roles in the list that are in warning (yellow) or trouble (red) state, do the following:
    a) Select the role and click **Resources**.
    b) In the **Servers** list, if the old main server is listed, replace it with the new one.
    c) If the role had a database hosted on the old server, create a database on the new server and restore the backup.

16 Open the *Network view* task, and delete the offline copies of your servers (🖥).

Your system is now back online. If you chose to decommission your old main server, uninstall Security Center from it.

After you finish

Notify your users with the DNS name or IP address of your new main server.

Related Topics

Converting an expansion server to the main server on page 109

Converting the main server to an expansion server on page 108

About roles

A role is a software component that performs a specific job within Security Center. To execute a role, you must assign one or more servers to host it. You can assign roles for archiving video, for controlling a group of units, for synchronizing Security Center users with your corporate directory service, and so on.

In Security Center, role entities are defined by the following:

- **Role type:** Determines the specific set of functions that should be performed by the role, such as managing video units and associated video archives.
- **Role settings:** Define the specific set of parameters the role should operate within, such as the retention period for the collected data, or which database the system should use.
- **Servers:** The *servers* that should be hosting (running) this role. You can assign one or more roles to the same server, or assign multiple servers to the same role to provide load balancing and failover.

After a role is configured, you can move it to any server in your Security Center system (for example, one with a faster processor or more disk space) without having to install any additional software on that server. Moving a role to another server might cause a short pause in the role's operations. In addition, some roles can spawn subprocesses (called *agents*) and execute them simultaneously on multiple servers for greater scalability.

Moving roles to other servers

You can move a role to another server without installing any additional software, for example, if the server that the role is installed on is slow or has limited disk space.

Before you begin

Make sure you have another server configured and ready to accept a new role.

What you should know

Moving a role to another server might cause a short pause in the role's operations.

NOTE: This procedure does not apply to Archiver roles. For moving Archiver roles, see Moving the Archiver role to another server on page 569.

To move a role to another server:

1. From the Config Tool homepage, open the *System* task and click the **Roles** view.
2. Select the role you want to modify, and then click the **Resources** tab.
3. If the role requires a database, do one of the following:
   - If the database resides on a third computer, you have nothing to change.
   - If the database is empty, you can create it anywhere you want.
   - If the database contains data and is residing on the current server, move the database to the new server or to a third computer.
4. Under the **Servers** list, click **Add an item** (➕).

   A dialog box shows all available servers on your system.
5. Select the substitute server and click **Add**.
6. Select the current server in the **Servers** list and click **Delete** (✖).
7. Click **Apply**.

Related Topics

Adding expansion servers on page 107

Deactivating and activating roles

For maintenance or troubleshooting purposes, you can deactivate a role without affecting any of its settings and then re-activate it later.

What you should know

If you are experiencing issues with your system, sometimes it is helpful to restart a role. Roles are also deactivated so their properties can be modified. .

You must have the *Modify role properties* privilege to deactivate a role.

To deactivate a role:

1 From the homepage, open the *System status* task.

2 From the **Monitor** list, select **Roles**.

The roles that are part of your system are listed in the report pane.

3 Select a role you want to deactivate, and click **Deactivate role** (🚦) > **Continue**.

The role turns grey (offline) in the report pane.

4 To reactivate the role, select the role, and click **Activate role** (🚦).

About the Directory role

The Directory role identifies a Security Center system. It manages all entity configurations and system-wide settings.

How the Directory role works

Only a single instance of this role is permitted on your system. The server hosting the Directory role is called the *main server*, and must be set up first. All other servers you add in Security Center are called *expansion servers*, and must connect to the main server to be part of the same system.

The main functions of the Directory role are:

- Client application connection authentication
- Software license enforcement
- Central configuration management
- Event management and routing
- Audit trail and activity trail management
- Alarm management and routing
- Incident management
- Scheduled task execution
- Macro execution

Directory role configuration

Because the Directory role is responsible for the authentication of all client connections, it cannot be configured in the Config Tool client application. To configure the Directory role, you must log on to *Server Admin* from a web browser.

Using Server Admin, you can perform the following administrative tasks:

- Start/stop the Directory role
- Manage the Directory database and change the data retention periods
- View and modify your Security Center license
- View and modify the main server's password and communication ports
- Convert the main server into an expansion server

In a multiple Directory server configuration, Directory *failover* and *load balancing* is managed by the *Directory Manager* role.

Related Topics

Directory failover and load balancing on page 166

About Web-based SDK

The Web-based SDK role exposes the Security Center SDK methods and objects as web services to support cross-platform development.

It allows developers on platforms other than Windows (for example, Linux) to write custom programs that can interact with Security Center.

This role mainly exists for clients who need custom development. Genetec™ Professional Services can help you develop the custom solution you need. To find out more, contact your sales representative, or call us at one of our regional offices around the world. To contact us, visit our website at www.genetec.com.

7

Databases and networks

This section includes the following topics:

Databases

A database is a collection of data that is organized so that its contents can easily be accessed, managed, and updated.

How database hosting works in Security Center

By default, a role's database is hosted on the same server that hosts the role. This is shown in the role's **Resources** tab by the value (local)\SQLEXPRESS in the **Database server** field, where "(local)" is the server where the role is running.

If you plan to change the server hosting the role or add secondary servers for failover, the database must be hosted on a different computer.

In addition, the computer hosting the database server does not have to be a Security Center server (meaning a computer where *Genetec Server* service is installed), unless you are configuring Directory database failover using the backup and restore method.

How SQL Server uses memory

If you are using a licensed edition of SQL Server (such as SQL Server Standard, SQL Server Business Intelligence, or SQL Server Enterprise) note that all databases are managed by Microsoft SQL Server in Security Center. By default, SQL Server is configured to use as much memory as is available on the system. This could lead to memory issues if you are hosting SQL Server and many roles on the same server, especially on a virtual machine with little memory resources.

If you run out of memory on one of your servers, you can set a maximum limit to the amount of memory SQL Server is allowed to use.

Related Topics

Moving databases to other computers on page 135

Connecting roles to remote database servers on page 136

Restricting the memory allocated to database servers on page 139

Moving databases to other computers

If you want to change the server hosting a role or add secondary servers for failover, you must host the role's database on a different computer.

Before you begin

- Make sure you have a machine available with SQL Server installed.
- The machine does not need to be a Security Center server.
- The server hosting your role must be able to access the database on the new server. For more information, see Connecting roles to remote database servers on page 136.

What you should know

This procedure is not necessary for the Archiver role. For Archiver roles, it is recommended to host the database locally.

To move a database to another computer:

1. From the Config Tool homepage, open the *System* task and click the **Roles** view.
2. Select the role whose database you want to move, and then click the **Resources** tab.
3. Back up the current database.

   TIP: Since the backup folder is relative to the current server, it might be a good idea to select a network location that can be reached by any server on your system.
4. (Optional) Delete the current database.
5. Create the database on the new machine.
6. Restore the content that you have backed up to the new database.
7. Click **Apply**.

Connecting roles to remote database servers

If a role database is hosted on a different server than the role, you must configure the remote database server (SQL Server) to accept connection requests from the role.

Before you begin

On the server hosting SQL Server, open TCP port 1433 and UPD port 1434 in the Windows Firewall.

To connect a role to a remote database server:

1 For SQL Server 2014 and earlier, allow remote connection on your SQL Server instance.

a) On the server hosting the database, open *Microsoft SQL Server Management Studio* and connect to the database server used by Security Center.

b) In the *Microsoft SQL Server Management Studio* window, right-click the database server name () in the **Object Explorer**, and click **Properties**.

c) In the *Server Properties* window, click **Connections**.

d) Under the *Remote server connections* section, click the **Allow remote connections to this server** option.

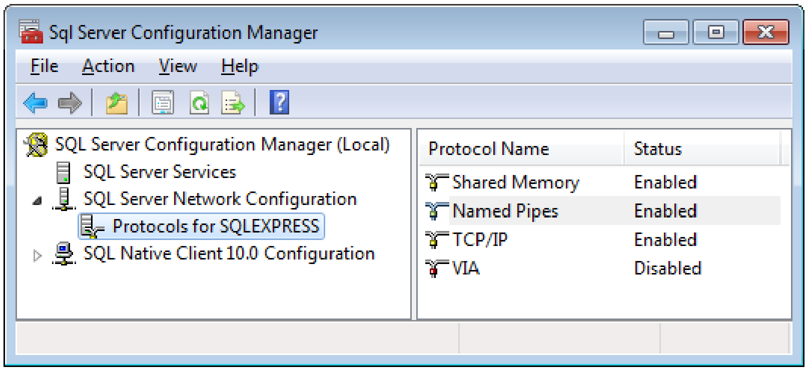
e) Click **OK** and close *Microsoft SQL Server Management Studio*.

2 Enable **Named Pipes** and **TCP/IP** protocols on your SQL Server instance.

a) On the server hosting the database, open *SQL Server Configuration Manager*.

b) Expand the *SQL Server Network Configuration* section, and select the protocols for your database server instance (for example, **Protocols for SQLEXPRESS**).

c) Right-click the **Named Pipes** and **TCP/IP** protocols, and set their status to **Enabled**.


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled
VIA	Disabled

d) Close *SQL Server Configuration Manager*.

3 Make sure your SQL Server instance is visible from other computers on your network.

a) On the server hosting the database, open *Microsoft Management Console Services* (services.msc).

b) Start the service named **SQL Server Browser**.

c) Right-click the SQL Server Browser service, and click **Properties**.

d) In the *General* page, from the **Startup type** list, select **Automatic**.

The SQL Server instance is now available from the **Database server** list of any role's *Resources* page in Config Tool.

4 Restart your SQL Server instance to enable the settings you have changed.

a) On the server hosting the database, open *Microsoft Management Console Services* (services.msc).

b) Right-click the SQL Server instance service, such as SQL Server (SQLEXPRESS), and click **Restart**.

5 On every server that hosts your Security Center roles, change the logon user of the Genetec Server service to a Windows administrator account that also has the permissions to access the SQL Server instance you modified.

   The Windows administrator account is usually a domain account used to connect to all servers.

   a) On the server hosting the role, open *Microsoft Management Console Services* (services.msc).
   b) Right-click the Genetec Server service, and click **Properties**.
   c) In the *Log on* page, select the **This account** option, and type an administrator **Account name** and **Password**.
   d) Click **Apply** > **OK**.
   e) Repeat these steps on every server that is hosting a Security Center role that must connect to the remote database server.

6 From the Config Tool homepage, open the *System* task and click the **Roles** view.

7 Select the role and click the **Resources** view.

8 In the **Database server** field, enter the path to the remote database.

   For example: DB_SERVER.GENETEC.COM\SQLEXPRESS

   NOTE: If required, specify a port as follows: *<hostname>,<port>\<sql_instance>*

Granting SQL Server permissions

For the Security Center Directory role to run, service users who are not Windows administrators (login name SYSADMIN) must be granted the *View server state* SQL Server permission.

What you should know

The minimum SQL Server *server-level role* supported by Security Center is *dbcreator*, and the mimimum SQL Server *database-level role* is *db_owner*. Therefore, you must make sure that members of the *dbcreator* role and members of the *db_owner* role have been granted the *View server state* SQL Server permission.

For more information about SQL Server roles and their capabilities, see your Microsoft documentation.

NOTE: The following procedure is for SQL Server 2019 Express. If you are using a different version of SQL Server, see your Microsoft documentation for information about granting permissions.

To grant SQL Server permissions:

- In SQL Server Management Studio, do one of the following:
  - Execute the following query: `GRANT VIEW SERVER STATE TO [login name]`.
  - Manually modify the user permissions as follows:
    a. Right-click the appropriate SQL Server instance and select **Properties**.
    b. Click the *Permissions* page.
    c. Under **Logins or roles**, select the user or role you want to modify.
    d. In the **Permissions** section, click the **Explicit** tab and select the **Grant** checkbox beside the **View server state** permission.
    e. Click **OK**.

After you finish

For users that are granted the permission locally on the Security Center server, you must add them as users on the SQL Server.

Restricting the memory allocated to database servers

The database server (SQL Server) is configured to use as much memory as it is available on the system. If you are experiencing issues with insufficient memory, you can fix the problem by setting a maximum limit to the amount of memory SQL Server is allowed to use.

To restrict the memory used by SQL Server:

1 On the server hosting the database, open *Microsoft SQL Server Management Studio*.

2 In the *Microsoft SQL Server Management Studio* window, right-click the database server name (🛢) in the **Object Explorer**, click **Properties**.

3 In the *Server Properties* window, click **Memory**.

4 In the field **Maximum server memory (in MB)**, enter the maximum memory SQL Server is allowed to use.

Microsoft recommends the following guidelines:

- RAM = 2 GB, Maximum server memory = 1000 MB
- RAM = 4 GB, Maximum server memory = 2200 MB
- RAM = 6 GB, Maximum server memory = 3800 MB
- RAM = 8 GB, Maximum server memory = 5400 MB
- RAM = 12 GB, Maximum server memory = 8000 MB
- RAM = 16 GB, Maximum server memory = 13500 MB
- RAM = 24 GB, Maximum server memory = 21500 MB

5 Click **OK**, and close *Microsoft SQL Server Management Studio*.

The SQL Server service automatically adjusts its memory footprint.

Creating databases

Under certain circumstances, you might need to create a new database, overwrite the default database assigned to a role, or assign a different database that is prepared by your IT Department if you plan on using a dedicated database server.

Before you begin

If you plan on overwriting the existing database with the new one, you should back up the existing database.

What you should know

All role databases are created from Config Tool, except the Directory database which must be created from the Server Admin - Main Server page. The procedures are very similar, so only creating from Config Tool is described here.

To create a database:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Select a role, and click the **Resources** tab.

3 From the **Database server** list, type or select the name of the database server.

The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server 2019 Express Edition* that was installed by default with *Genetec™ Security Center*. To specify a database server on a different server than the one hosting the role, enter the name of that remote server.

4 From the **Database** list, type or select the name of the database.

The same database server can manage multiple database instances.

5 Click **Apply**.

The database creation starts. A window opens, showing the progress of this action. You can close this window and review the history of all database actions by clicking **Database actions** in the notification tray.

6 Wait until you see **Database status** indicating **Connected**.

BEST PRACTICE: Consider taking regular backups to avoid data loss.

Related Topics

Backing up databases on page 147

Receiving notifications when databases are almost full on page 146

Deleting databases

To free up disk space, you can delete databases you no longer use.

What you should know

All role databases are deleted from Config Tool, except the Directory database which must be deleted from the Server Admin - Main Server page. The procedures are similar, so only deleting from Config Tool is described here.

To delete a database:

1. From the Config Tool homepage, open the *System* task and click the **Roles** view.
2. Select a role, and click the **Resources** tab.
3. From the **Database** list in the **Resources** tab of a role, select the database you want to delete.

   NOTE: This does not need to be your current database.
4. Click **Delete the database** (✖).

   CAUTION: A confirmation dialog box appears. If you continue, the database is permanently deleted.
5. Click **Delete** in the confirmation dialog box.

   The database deletion starts. A window appears, showing the progress of this action. You can close this window, and review the history of all database actions later on by clicking **Database actions** in the notification tray.
6. Create a new database for the role.

After you finish

Connect the role to an existing database or create a new database.

Related Topics

Creating databases on page 140

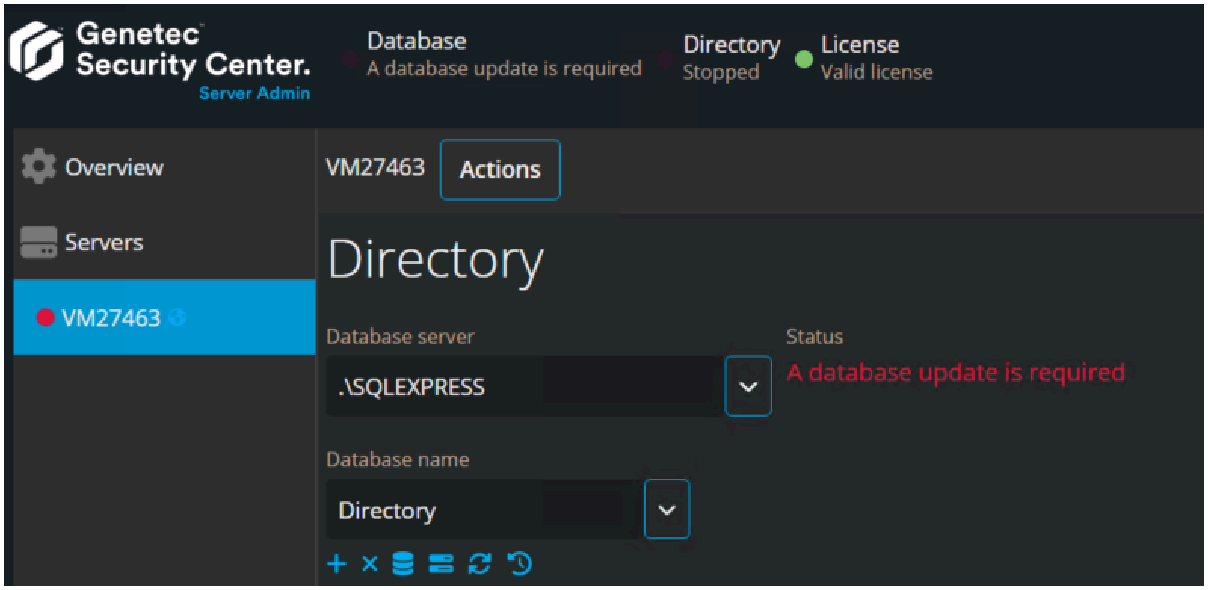
Upgrading the Security Center Directory database

The Security Center 5.11 Installer upgrades the Directory database as part of the main server upgrade. You only need to upgrade the Directory database manually if you restored an older version of the database.

What you should know

After restoring an older version of the Directory database, Server Admin notifies you that a database update is required. For information on restoring databases, see the *Security Center Administrator Guide*.

BEST PRACTICE: Before you upgrade, back up your database in a secure location that is separate from your main server.



Database
A database update is required

Directory
Stopped

License
Valid license

Database server: .\SQLEXPRESS

Status: A database update is required

Database name: Directory

To upgrade the Directory database:

1 Do one of the following:

- Click **Database** with the flashing red LED.
- Click **Database update** (⟳) in the *Directory* section.

The Directory database update starts, and the database server status shows **Upgrading**.

2 While the database is being upgraded, click **Show progress** (☰) to view the progress of the upgrade.

When the upgrade is completed, the **Status** shows **OK**.

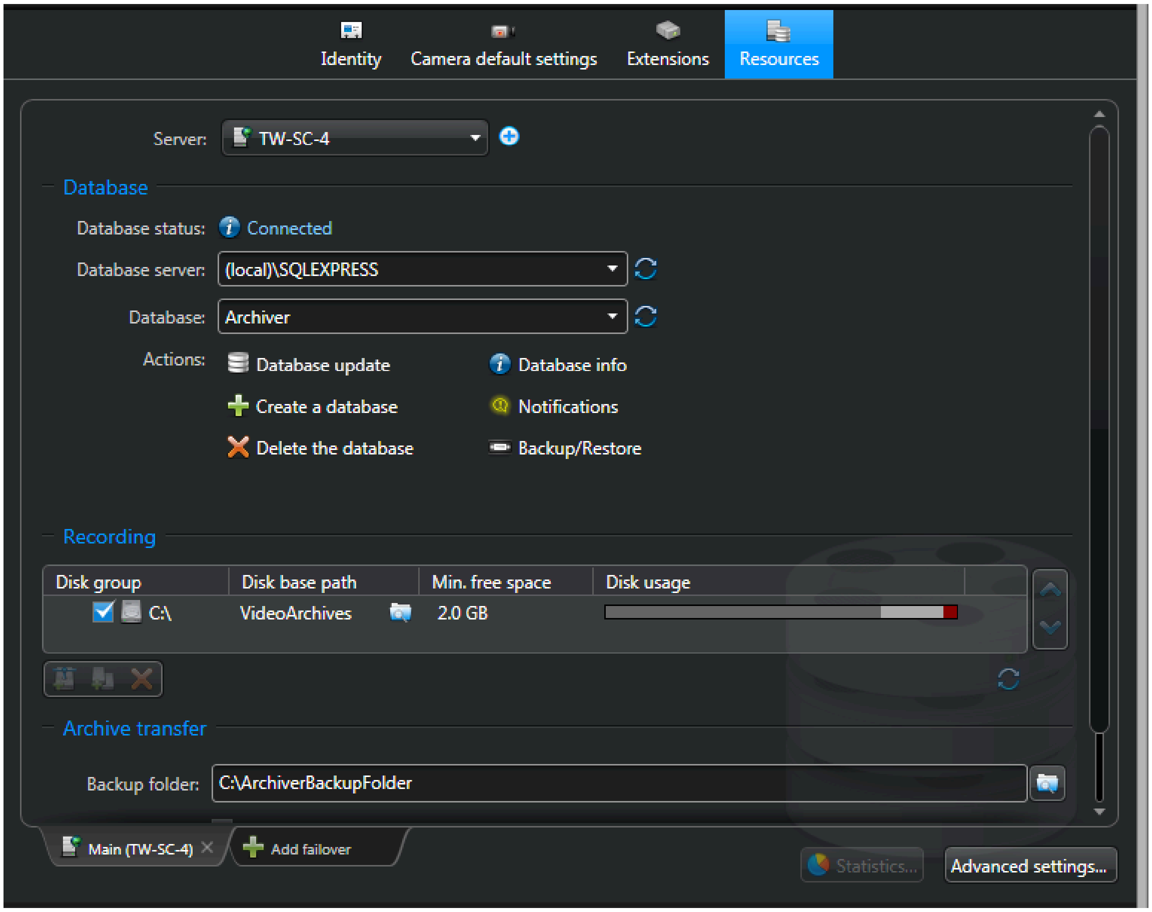
3 Click **Database properties** (☰) to confirm the version of the database and the number of entities in the database.

4 Log off from Server Admin, and then log on to Config Tool.

5 Open the *System* task, and select **Roles**.

6 Select the Archiver role, and click **Resources**.

7 In the **Actions** section, click **Database update** (🗄) .



Server: TW-SC-4

Database

Database status: Connected

Database server: (local)\SQLEXPRESS

Database: Archiver

Actions: Database update, Create a database, Delete the database, Database info, Notifications, Backup/Restore

Recording

Disk group	Disk base path	Min. free space	Disk usage
☑ C:\	VideoArchives	2.0 GB	

Archive transfer

Backup folder: C:\ArchiverBackupFolder

After the upgrade is complete, the **Database status** indicates *Connected*.

8 Repeat the steps for every role that requires a database update. The roles on your system vary depending on your license options.

After you finish

Shrink the Archiver database, and if necessary, other databases that you have upgraded.

Shrinking Security Center databases after an upgrade

After a database upgrade, disk usage might increase due to the temporary storage required to execute the upgrade transactions. The disk space used during the upgrade is not automatically released after the upgrade is complete. To reclaim the unused disk space, you must shrink the database.

Before you begin

Not all database upgrades cause the database to grow in size. If you are not sure whether or not you need to shrink your database after an upgrade, check the disk usage with SQL Server Management Studio.

What you should know

Depending on the recovery model of your database, a transaction log backup might be required to reclaim the unused disk space. For more information, see the following online articles:

- Recovery Models (SQL Server)
- Transaction Log Truncation

To shrink a database:

1 Follow the Shrink a Database procedure from Microsoft.

2 Repeat this procedure for all databases that require shrinking.

Viewing database information

You can view the information about a role's database, such as the database server and database versions, how much disk space is available, and a summary of the data it holds.

What you should know

The database information provided varies depending on the role. You might be asked to provide information on a role’s database when you contact Genetec™ Technical Assistance Center.

All roles' database information are viewed from Config Tool, except for the Directory database, which must be viewed from the Server Admin - Main Server page. The procedures are similar, so only viewing from Config Tool is described here.

To view a role's database information:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Select a role, and click the **Resources** tab.

3 Click **Database info** (ℹ).

The following information can be displayed, depending on the role:

- **Database server version:** Software version of the database server.
- **Database version:** Schema version of the role’s database.
- **Approximate number of events:** (Also called *Approximate number of archived events* and *Event count*) Number of events that are stored in the role’s database.
- **Source count (Archiver and Auxiliary Archiver only):** Number of video sources (cameras) that have archives.
- **Video file count (Archiver and Auxiliary Archiver only):** Number of video files.
- **Size on disk:** Size of the Database files.
- **Approximate number of entities (Directory only):** Number of entities (areas, cameras, doors, schedules, and so on) in the system.
- **Approximate number of active alarms (Directory only):** Number of active alarms (not yet acknowledged) in the system.
- **Approximate number of archived alarms (Directory only):** Number of past alarms available for reporting, excluding the active ones.

Receiving notifications when databases are almost full

You can configure different roles to send you an email notification when their database space is running low.

Before you begin

To make sure that the email notification is sent, configure the **SMTP** and **Watchdog** settings on the server hosting the role.

What you should know

All role database notifications are configured from Config Tool, except for the Directory database, which must be configured in the *Database properties* on the Server Admin - Main Server page. The procedures are similar, so only the configuration from Config Tool is described here.

To receive a notification when a role's database is almost full:

1. From the Config Tool homepage, open the *System* task and click the **Roles** view.
2. Select a role, and click the **Resources** tab.
3. Click **Notifications** ().
4. In the dialog box that opens, set the following options:
   - **Disk space:** Sends a notification when the remaining free space on the disk falls below a certain threshold (in GB).
   - **Database usage:** Sends a notification when the space used by the role's database reaches a certain percentage. This option is only for the Express edition of SQL Server, whose database size is limited to 10 GB. If you are using a full edition of SQL Server, this option has no effect.
5. Click **OK**.

Related Topics

Server Admin - Main server page on page 102

Backing up databases

You can protect your Security Center system data by regularly backing up its databases to a secure location that is separate from your main server. It is best practice to back up your databases before an upgrade.

What you should know

WARNING: Do not use virtual machine snapshots to back up your Security Center databases. During the snapshot process, all I/Os on the virtual machine are suspended, which can affect the stability and the performance of your system. We strongly recommend that you follow the procedure described below.

Depending on which role database you want to back up, the procedure can be different.

To back up a database:

1. For the Directory database without failover, perform the backup from Server Admin.
2. For the Directory database with failover, perform the backup from the Directory Manager's Directory failover page in Config Tool.
3. For any other Security Center role database, perform the backup from Config Tool, on the Resources page of the role.
4. For the Archiver and Auxiliary Archiver roles, after backing up the database, perform an archive transfer to back up the video files.

Backing up the Directory database

You back up the Directory database from Server Admin.

Before you begin

- For non-Directory databases, see Backing up role databases on page 148.
- If the *Backup and restore* failover mode is enabled, perform the backup from Config Tool.

What you should know

There are restrictions regarding the backup and restore of the Directory database when the *Mirroring* failover mode is enabled. For more information, refer to the Microsoft SQL Server Database Mirroring documentation.

To back up the Directory database:

1. Log on to Server Admin on your computer using a web browser.
2. From the server list, select the main server (🌐).

   The Server Admin - Main server page is displayed.
3. Click **Database properties** (🗄) and configure the backup settings:
   - **Destination folder:** Path to the backup folder relative to the server performing the backup. By default, databases are backed up to *C:\SecurityCenterBackup* on the database server, and configuration files are backed up to the same folder on the server hosting the role. If the folder does not exist, it will be created. To save your backups on a shared network drive, enter the path manually, and ensure that both the Genetec™ Server service user and the SQL Server service user have write access to that location.
   - **Compress backup file:** (Optional) Select this option to create a ZIP file instead of a BAK file. If you select this option, you need to unzip the backup file before you can restore it.

IMPORTANT: The **Compress backup file** option only works if the database is local to the server hosting the role.

- **Enable automatic backup:** (Optional but recommended) Select this option to enable automatic backup on a schedule. Specify the frequency and time of the backup, and how many backup files you want to keep.

  NOTE: Backup files you create manually are not counted in the number of retained backup files.

4 Click **OK** > **Save**

5 Click **Backup/Restore** () and then click **Backup now**.

The backup starts and the progress is shown in the dialog box.

6 When the task is completed, click **OK**.

A backup file is created in the backup folder with the file extension BAK (or ZIP if the **Compress backup file** option was selected). The name of the file is the database name, followed by “_ManualBackup_”, and the current date and time.

Backing up role databases

You back up a role database from Config Tool, from the role's *Resources* page.

Before you begin

For the Directory database, see Backing up the Directory database on page 147.

What you should know

You protect the data managed by a role by backing up its database. For the Archiver and Auxiliary Archiver roles, you also need to back up the video archive because the associated video files are not stored in the database.

To back up a role database:

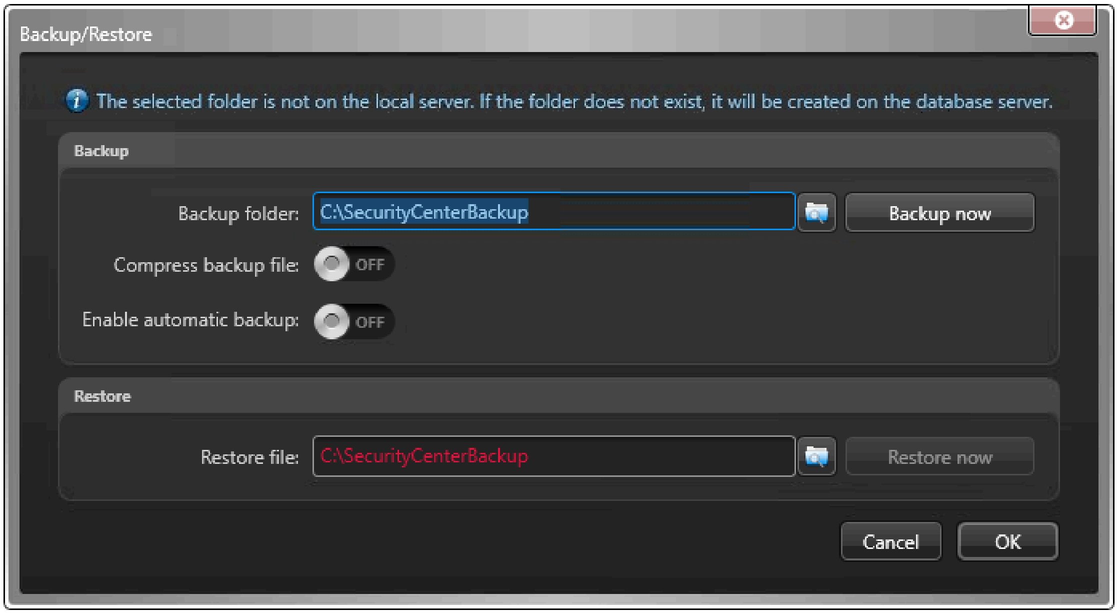
1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Select a role, and click the **Resources** tab.

3 Click **Backup/Restore** ().

4 In the *Backup/Restore* dialog box, beside the **Backup folder** field, click **Select folder** (), and select the folder where you want to save the backup file.

   IMPORTANT: Make sure you select a separate and secure location to store your backups.



Backup/Restore

The selected folder is not on the local server. If the folder does not exist, it will be created on the database server.

Backup

Backup folder: C:\SecurityCenterBackup

Compress backup file: OFF

Enable automatic backup: OFF

Restore

Restore file: C:\SecurityCenterBackup

   NOTE: The location of the **Backup folder** is relative to the server performing the backup. By default, databases are backed up to *C:\SecurityCenterBackup* on the database server, and configuration files are backed up to the same folder on the server hosting the role. If the folder does not exist, it will be created. To save your backups on a shared network drive, enter the path manually, and ensure that both the Genetec™ Server service user and the SQL Server service user have write access to that location.

5 (Optional) Turn on the **Compress backup file** option to create a ZIP file instead of a BAK file.

   If you select this option, you need to unzip the backup file before you can restore it.

   IMPORTANT: The **Compress backup file** option only works if the database is local to the server hosting the role.

6 Click **Backup now**.

A backup file is created in the backup folder with the file extension BAK. The name of the file is the database name, followed by "_ManualBackup_", and the current date and time.

Backing up databases on a schedule

For extra protection for your data, you can back up your databases periodically.

Before you begin

To back up the Directory database on a schedule, see Backing up the Directory database on page 147.

To back up a role database on a schedule:

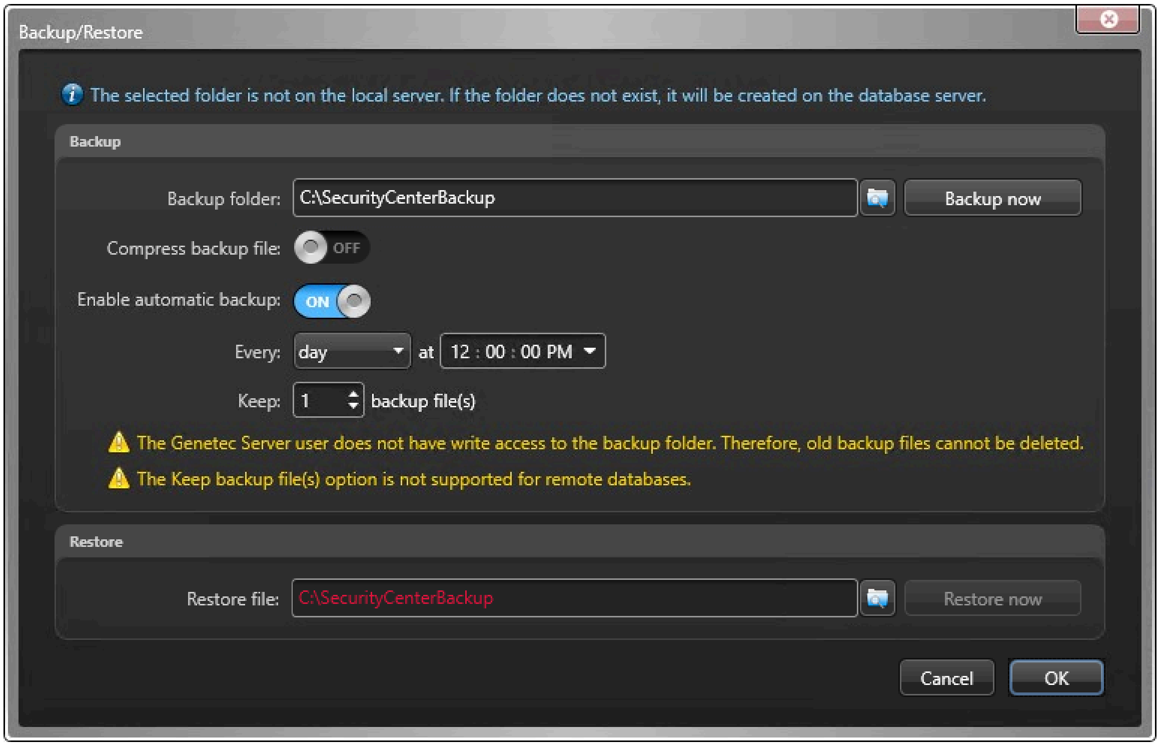
1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Select a role, and click the **Resources** tab.

3 Click **Backup/restore** (▭).

4 In the *Backup/Restore* dialog box, turn on the **Enable automatic backup** option.

5 Select the day and time to perform the backup (every day or once a week).



Backup/Restore

The selected folder is not on the local server. If the folder does not exist, it will be created on the database server.

Backup

Backup folder: C:\SecurityCenterBackup

Compress backup file: OFF

Enable automatic backup: ON

Every: day at 12 : 00 : 00 PM

Keep: 1 backup file(s)

⚠ The Genetec Server user does not have write access to the backup folder. Therefore, old backup files cannot be deleted.

⚠ The Keep backup file(s) option is not supported for remote databases.

Restore

Restore file: C:\SecurityCenterBackup

TIP: It is a good idea to stagger the backup operations if you need to back up different databases on the same machine.

6 Specify how many backup files you want to keep.

NOTE: Backup files you create manually are not counted in the number of retained backup files.

7 Click **OK** > **Apply**.

The automatic backup starts at the next scheduled date and time.

Restoring databases

If you just restored a server, moved a server to another computer, reinstalled or upgraded SQL Server, or made some configuration mistakes that you want to undo, you can restore the old database.

Before you begin

Back up the current database before you restore an old database. If you selected the **Compress backup file** option during backup, you must first unzip the backup file before you can restore it.

What you should know

All role databases are restored from Config Tool, except the Directory database which must be restored from the Server Admin - Main Server page. The procedures are similar, so only restoring databases from Config Tool is described here.

NOTE: The following cases are exceptions:

- You cannot restore the Directory database from Server Admin when the *Mirroring* failover mode is enabled. For more information on the restrictions regarding backup and restore while the *database mirroring session* is active, refer to the Microsoft SQL Server Database Mirroring documentation.
- For the Archiver and the Auxiliary Archiver roles, after restoring the role database, you must also restore the video archives.

To restore a role's database:

1. From the Config Tool homepage, open the *System* task and click the **Roles** view.
2. Select a role, and click the **Resources** tab.
3. Click **Backup/Restore** ().

   For the Directory database, you would click **Backup/Restore** () from Server Admin.
4. In the *Backup/Restore* dialog box, beside the **Restore file** field, click **Select file** (), and select the backup file you want to restore.

   NOTE: By default, databases are backed up to *C:\SecurityCenterBackup* on the database server, and configuration files are backed up to the same folder on the server hosting the role. If your backups are stored on a shared network drive, enter the path manually, and ensure that the service user has read access to that location.
5. Click **Restore now**.
6. Click **OK**.

The current content of the database is replaced by the content restored from the backup file.

About networks

The network entity is used to capture the characteristics of the networks used by your system so that proper stream routing decisions can be made.

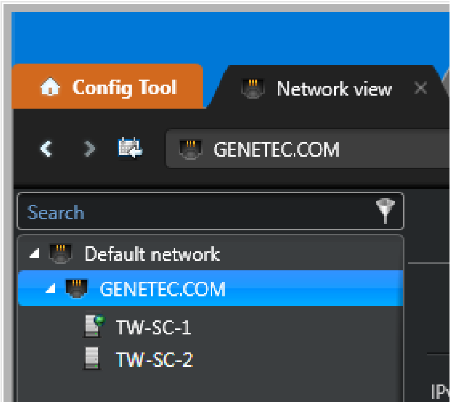
Unless your entire system runs from a single private network without communicating with the outside world, you must configure at least one network entity other than the *Default network* to describe your networking environment.

How network entities are created

Network entities are created automatically by the system.

After installing Security Center on your main server, you will have the following two network entities on your system:

- The *Default network* is the root node on the network tree. Its video transmission capabilities are set to *Unicast TCP*, which is the characteristic shared by all IP networks. You cannot delete the *Default network* entity.
- A second network entity attached to the *Default network*, that corresponds to your company's network (where your main server is located).



After that, more network entities are added to your system when you add new servers belonging to different networks.

When a server with multiple network interface cards (NIC) is added to the system, only the first address defined in the operating system is represented by default as a network entity. However, you can add the other network entities manually, if later, you need to have a better control of the routing capabilities.

A federated network () is created for every federated system. It allows you to control how media from that system is accessed from the local system, to force media redirection, and to set the route capabilities.

Network routes

Between every two networks on your system there is a route. The data transmission capabilities of the route are limited to the smallest capability set of the two end points.

For example, if one end is capable of multicast and the other end is only capable of unicast UDP, the capabilities of the route between these two end points cannot be more than unicast UDP.

If the connection between the two end points (for example VPN) only supports unicast TCP, you might have to further limit the capabilities of a route.

Related Topics

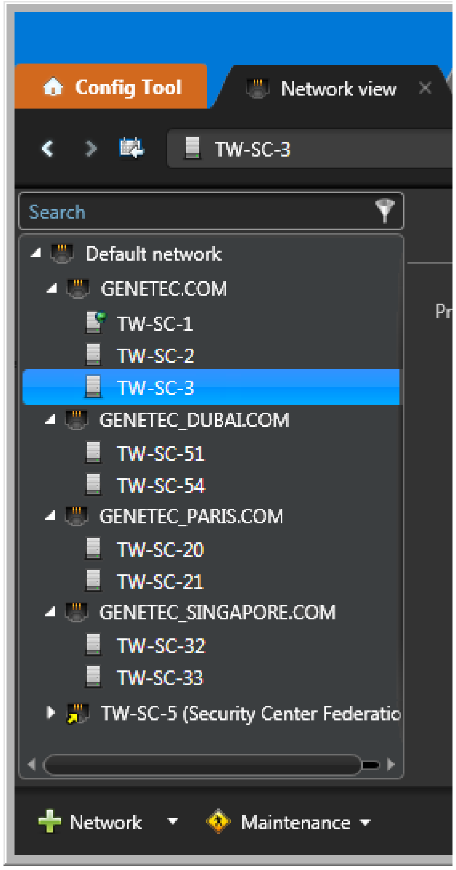
Adding networks on page 155

About the Network view

The network view is a browser view that illustrates your network environment by showing each server under the network they belong to.

You can manage this view through the *Network view* task. The hierarchy in the *Network view* task displays the networks () and the *servers* () found in your system, and lets you configure them. The *main server* hosting the *Directory* role is shown with a different icon ().

Accurate representation in the network view helps you visualize your system setup.



A federated network () is created for every federated system. It allows you to control how media from that system is accessed from the local system, to force media redirection, and to set the route capabilities.

Adding networks

If your system spreads across multiple networks or you allow your users to connect to the main server over the Internet, you must configure the network view and add additional networks.

To add a network:

1 Open the *Network view* task.

2 If you are creating a subnet, select the parent network in the network tree. Otherwise, select the *Default network*.

3 Click **Network** (✚) and enter the name of the network entity.

You are automatically placed in the network's **Properties** tab.

4 From the **Capabilities** list, select the data transmission type for streaming live video on the network.

TIP: Always select the largest set of capabilities that your network supports.

- **Unicast TCP:** Unicast (one-to-one) communication using TCP protocol is the most common mode of communication. It is supported by all IP networks, but it is also the least efficient method for transmitting video.
- **Unicast UDP:** Unicast (one-to-one) communication using UDP protocol. Because UDP is a connectionless protocol, it works better for live video transmission. When the network traffic is busy, UDP is much less likely to cause choppy video than TCP. A network that supports unicast UDP necessarily supports unicast TCP.
- **Multicast:** Multicast is the most efficient transmission method for live video. It allows a video stream to be transmitted once over the network to be received by as many destinations as needed. The gain could be very significant if there are many destinations. A network supporting multicast necessarily supports unicast UDP and unicast TCP.

  NOTE: Multicast requires specialized routers and switches. Make sure you confirm this with your IT department before setting the capabilities to multicast.

5 Under the **Routes** section, verify that all the routes created by default are valid.

- You may have to change the default capabilities, or force the use of private address when public addresses cannot be used between servers within the same subnet. To edit a route, select it in the list and click **Edit the item** (✎).
- If there is no connection between this network and another network on the system, select the route, and click **Delete** (✖).
- You may want to add a direct route between this network and another child network, bypassing its parent network.

6 Click **Apply**.

Related Topics

Configuring the Media Router role on page 597

Network - Properties tab on page 1281

Creating direct connections between networks

You can create a new route between two networks in your system if your network configuration allows it.

What you should know

Security Center creates by default a route between a network and its parent, and between two networks under the same parent.

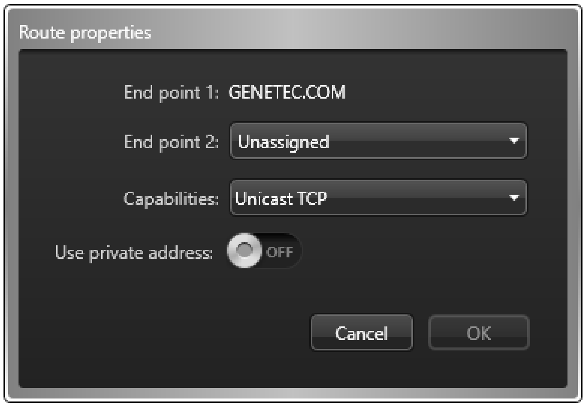
To add a route between two networks:

1 Open the *Network view* task.

2 Select the network you want to establish the route from, and click the **Properties** tab.

3 Under the **Routes** sections, click **Add an item** (+).

The *Route properties* dialog box opens.



Route properties

End point 1: GENETEC.COM

End point 2: Unassigned

Capabilities: Unicast TCP

Use private address: OFF

4 From the **End point 2** list, select another network you want to establish the route to.

5 From the **Capabilities** list, select the smallest set of capabilities.

6 If public addresses cannot be used between these two networks, switch the **Use private address** option to **ON**.

7 Click **OK**, and then click **Apply**.

Customizing network options

You can customize your network card, how your network is selected, and your port range to ensure the best communication to and from your workstation.

What you should know

The network settings apply to the local workstation, and affect Security Desk and Config Tool for all users.

To customize network options:

1. From the homepage, click **Options** > **General**.
2. If your computer is equipped with more than one network card, select the one used to communicate with Security Center applications from the **Network card** list.
3. Choose how to select the **Network**:
   - **Auto-detect:** Security Center automatically detects the network your workstation is connected to.
   - **Specific:** Manually select the network you are on from the drop-down list. This option is helpful if you have trouble getting video feeds.
4. In the **Incoming UDP port range** option, select the port range used for transmitting video to your workstation using *multicast* or unicast *UDP*.
5. Click **Save**.

Example

Let’s consider the following use case. You have a network 10.1.x.x that has a route to 10.2.x.x. But for some reason, a specific workstation at address 10.1.2.3 cannot access 10.2.x.x. Specifying a network manually on that workstation allows the Media Router to know that it has to redirect the media from 10.2.x.x for that workstation instead of making it try to connect directly to 10.2.x.x and fail.

8

High availability

This section includes the following topics:

About the high availability features in Security Center

High availability is a design approach that enables a system to perform at a higher than normal operational level. This often involves failover and load balancing.

To ensure that there is uninterrupted access and data protection for your system, Security Center offers the following high availability features:

- **Directory failover:** Ensure that the Directory role remains available when its primary server fails. The Directory role handles failover for all other roles, so it is important that the Directory role remains available at all times.
- **Directory load balancing:** Additional benefit of Directory failover. Up to 5 servers can be assigned to the Directory role to share its workload. All servers that are set up for Directory failover are automatically used for load balancing.
- **Database failover (only for Directory role):** Protect the Directory database, using one of the following methods:
  - **Backup and restore:** Regularly backup your database, and restore it if a failover occurs.
  - **Microsoft SQL Server Database Mirroring:** The database instances are kept in sync by Microsoft SQL Server.
- **Archiver failover:** Ensure that the Archiver role and video archiving capability remains available when the Archiver's primary server fails.
- **Other role failover:** Ensure that other roles in your system remain available when their primary server fails. If the role database must be protected, you should consider one of the following third party solutions: *SQL Server Clustering* or *Database Mirroring*.
- **Windows Server failover cluster:** Third party solution for roles that do not support failover. For more information, see *Security Center Installation Guide for Windows Cluster*.

Other ways you can ensure high availability are to detect problems early, and prevent those problems from reoccurring.

Role failover

Failover is a backup operational mode in which a role (system function) is automatically transferred from its primary server to a secondary server that is on standby. This transfer between servers occurs only if the primary server becomes unavailable, either through failure or through scheduled downtime. Role failover is managed by the Directory role.

How role failover works in Security Center

For failover to work in Security Center, you need to define the following two types of servers:

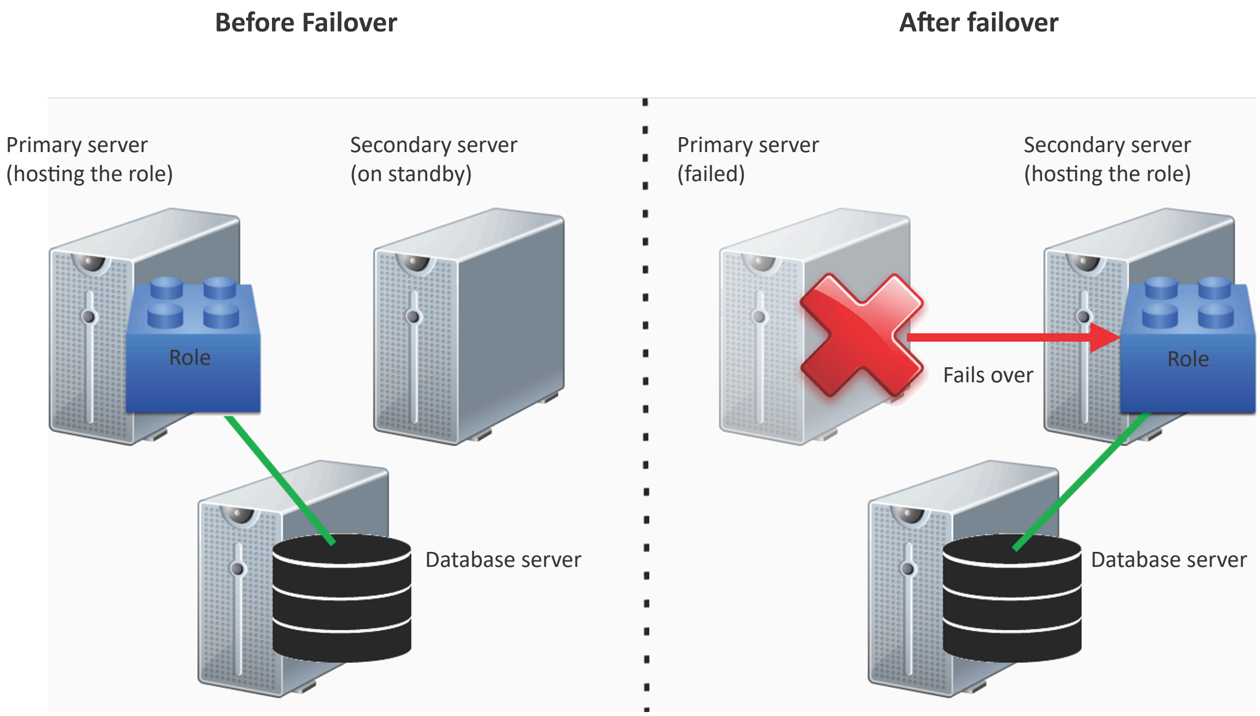
- **Primary server:** Server that normally hosts a role for it to work on the system.
- **Secondary server:** Servers on standby that are assigned to a role to keep it running in case the primary server becomes unavailable.

There is no limit to the number of secondary (or standby) servers you can assign to most roles. However, the more servers you add, the less cost-effective it might be for you.

The secondary server of one role can be the primary server of another role, provided that both servers have enough resources (CPU, memory, disk space, and network bandwidth) to handle the combined load of both roles in case of a failover.

IMPORTANT: Security Center does not handle the failover of role databases. For roles that connect to a database, the database server must be hosted on a third computer, separate from the servers hosting the role. All role servers must have read and write access to the database server. To protect your data, perform regular backups of the role database.

Before failover, a role is hosted on the *primary server* and connects to a *database server* hosted on a third computer. When the *primary server* fails, the role automatically fails over to the *secondary server* and reconnects to the **same** *database server*.



Roles supporting failover

Some roles in Security Center do not support failover, and others only support failover under certain conditions.

The following table lists which Security Center roles support failover, the failover approach they use, and any special requirements they might have.

Role	Supports failover	Comments and exceptions
Access Manager	Yes	
Active Directory	Yes	
ALPR Manager	Yes	Extra resources must be shared between the servers assigned to the role. The *Root* folder of the role must follow the UNC convention and must be accessible to all servers. The paths to the hotlist and permit entities must also follow the UNC convention and be accessible to all servers. The *WatermarkEncryptionParameters.xml* file found in the installation folder of the primary server must be copied to all secondary servers.
Archiver	Yes	Can have up to two secondary servers assigned to an Archiver role. Each server requires its own database, hosted locally or on a separate computer. **NOTE:** Failover and redundant archiving are not supported on Archiver roles used for wearable (or body-worn) cameras.
Authentication Service	Yes	The Authentication Service role runs on the same server as the Directory role. If Directory failover is used, endpoint URIs for each Directory server on your system must be added to the *identity provider* configuration for Security Center.
Auxiliary Archiver	No	The function of the Auxiliary Archiver is to ensure that video archives remain available when the Archiver fails.
Camera Integrity Monitor	No (load distribution)	The Camera Integrity Monitor role can distribute its workload over multiple servers. This should not be confused with failover, where only one server bears the full load of the role at all times.
Cloud Playback	Yes	
Directory	Yes	Can run simultaneously on up to five servers. Also supports Directory database failover.
Directory Manager	Not applicable	The function of the Directory Manager is to manage the Directory failover and load balancing.
Global Cardholder Synchronizer	Yes	
Health Monitor	Yes	

Role	Supports failover	Comments and exceptions
Intrusion Manager	Yes	Only when the *intrusion panels* are connected using IP. Failover is not supported if the intrusion panels are connected using serial ports.
KiwiVision™ Analyzer	Yes	
KiwiVision™ Manager	Yes	
Map Manager	Yes	**BEST PRACTICE:** It is best to set the map cache to a location that can be reached by all servers assigned to the role.
Media Gateway	Yes	
Media Router	Yes	The primary and secondary servers can each have a separate database, hosted locally, or on another computer.
Mobile Credential Manager	Yes	
Mobile Server	Yes	
Omnicast™ Federation™	Yes	
Plugin	Yes	Plugin (with an uppercase, in singular) is the role template that serves to create specific plugin roles. All roles created from this template support failover.
Privacy Protector™	No (load distribution)	The Privacy Protector role can distribute its workload over multiple servers. This should not be confused with failover, where only one server bears the full load of the role at all times. If one of the assigned servers fails, and the remaining servers cannot handle their increased load, the resulting streams will have dropped frames.
Record Caching Service	Yes	
Record Fusion Service	Yes	
Report Manager	Yes	
Reverse Tunnel	Yes	
Reverse Tunnel Server	Yes	This is taken care by Genetec™ Cloud Operations.
Security Center Federation™	Yes	
Unit Assistant	Yes	
Wearable Camera Manager	No	If the role fails, the body-worn camera stations (clients) cumulates the data until the role is up again.
Web-based SDK	Yes	

Role	Supports failover	Comments and exceptions
Web Server	Yes	The Web Client and Genetec™ Web App must reconnect to a different URL when the role fails over to a different server.
Zone Manager	Yes	

Related Topics

Adding a relying party trust for Security Center on page 532

Setting up role failover

To configure failover for roles on your system, you must select secondary servers to be on standby in case the primary server hosting the role becomes unavailable.

Before you begin

For roles that require a database (with the exception of the Archiver role), the database must be hosted on a different computer than any of the servers assigned to the role. All servers assigned to the role must be able to connect to the server managing the role database.

IMPORTANT: All servers assigned to the same role must be running the same version of Security Center.

What you should know

To set up failover for an Archiver role, see Archiver failover on page 191.

To set up role failover:

1 From the Config Tool home page, open the *System* task, and click the **Roles** view.

2 Select the role you want to configure failover for, and then click the **Resources** tab where the role's primary server is listed

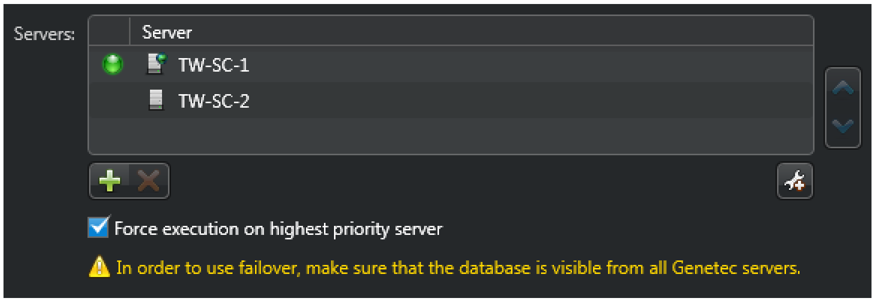
3 Under the **Servers** list, click **Add an item** (➕).

A dialog box opens, listing all remaining servers on your system that are not yet assigned to this role.

4 Select the server that you want to add as a secondary server and click **Add**.

The secondary server is added below the primary server. The green LED indicates which server is hosting the role.

NOTE: The servers are listed in the order that they are picked if a failover occurs. When the primary server fails, the role automatically switches to the next server on the list.



Servers:

	Server
●	TW-SC-1
	TW-SC-2

☑ Force execution on highest priority server

⚠ In order to use failover, make sure that the database is visible from all Genetec servers.

5 To change the priority of a server, select it from the list, and click the ⌃ or ⌄ buttons to move it up or down the list.

6 If you want the primary server to retake control after it is restored from a failover, select the **Force execution on highest priority server** option.

To minimize system disruption, the role remains on the secondary server after a failover occurs, by default.

7 Click **Apply**.

Changing the server priority for role failover

You can make secondary servers into primary servers, or ensure that a primary server is always the one hosting the role as long as it is running.

What you should know

To minimize system disruption, the role remains on the secondary server after a failover occurs, by default. You can change the server priority and force the highest priority server to always be the one hosting the role.

To change the server priority for failover:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Select the role and then click the **Resources** tab where the role’s primary server is listed.

3 Select a server from the list, and click the ⌄ or ⌃ buttons to change the server priority.

The higher a server is in the list, the higher its priority.

4 Select the **Force execution on highest priority server** option and click **Apply**.

This option forces the server with the highest priority (at the top of the list) to always be the one hosting the role, as long as it is online. If the first server is offline, then the priority goes to the second sever on the list, and so on and so forth.

After a few seconds, the green LED moves to the server that is at the top of the list, indicating that it is now the one hosting the role.

IMPORTANT: Servers are displayed in the order they are picked if a failover occurs. When the primary server fails, the role automatically switches to the next server in the list.

Directory failover and load balancing

Since the Directory is the main role that manages all entity configuration in your system, you must ensure that the Directory service is always available, and does not become overloaded.

The Directory service is available as long as its two components are available:

- **Directory role:** Manages your system configuration, and handles failover for all other roles.
- **Directory database:** Stores your system configuration.

The *Directory Manager* role handles Directory *failover* and *load balancing* for your system. It manages failover for the Directory role and Directory database independently, allowing you to have separate lists of *servers* assigned to host the two components. These two lists of servers can overlap or be completely separate.

NOTE: There can only be one Directory Manager role in your system. It is created automatically when your software license supports multiple Directory servers.

Differences between Directory servers and the main server

To configure Directory failover and load balancing, you must know the difference between Directory servers and the main server.

- **Directory server:** Servers assigned to host the Directory role. The Directory role can run on five Directory servers simultaneously for *load balancing*. They distribute the workload for credential authentication, software license enforcement, Directory database report queries, and so on.

  Users can log on to Security Center through any of the Directory servers. By default, the Directory Manager redirects the connection requests across all Directory servers in a round robin fashion, but you can bypass load balancing on specific workstations as needed.
- **Main server:** The primary Directory server in your system (🖥). It has full read/write access to the Directory database. If your system is configured for Directory failover and load balancing, the additional Directory servers (🖥) only have read access to the database.

When a Directory server fails, only the client applications connected to Security Center through that server must reconnect. If the main server fails, then *all* clients on the system must reconnect, and the responsibility of being the *main server* is passed down to the next Directory server in the failover list.

Preparing Directory failover and load balancing

Before you can configure the Directory for failover and load balancing, there are some pre-configuration steps required.

Before setting up Directory failover and load balancing:

1. Make sure your Security Center license supports multiple *Directory servers*.

   NOTE: The *Directory Manager* (🌐) role is created automatically in Config Tool when your license supports multiple Directory servers.

   a) From the homepage, click **About** > **Security Center**.

   b) In the **Number of additional Directory servers** option, note the number of supported servers.

   If you need to update your license, see the *Security Center Installation and Upgrade Guide*.

2. Have your *System ID* and *Password* on hand, found in the *Security Center License Information* document.

   Genetec™ Technical Assistance sends you this document when you purchase the product.

3. Make sure that all the servers you plan to use as Directory servers are up and running as expansion servers.

   For more information about installing expansion servers, see the *Security Center Installation and Upgrade Guide*.

4. Host the Directory database on a remote computer from the Directory servers.
5. Make sure the database server is accessible from all Directory servers.

Related Topics

Server Admin - Main server page on page 102

Setting up Directory failover and load balancing

To protect your information in case the main server fails, you can set up Directory failover and load balancing by assigning expansion servers as Directory servers.

Before you begin

Prepare for Directory failover and load balancing.

What you should know

- You can convert up to five expansion servers as *Directory servers* to be used for load balancing and failover. The order of appearance of the servers in the list corresponds to the order they are picked if a failover occurs. If the main server fails, the role switches to the next server in the list, and that server becomes the main server.

  IMPORTANT: Do not try to add a server to the Directory failover list by activating the Directory on that expansion server with Server Admin. This action disconnects the server from your current system and transforms it into the *main server* of a new system.
- If you want to exclude a Directory server from load balancing because either the server or the connection between the client and the server is slow, you can enable the **Disaster recovery** option. This removes the server from participating in load balancing, but the server will still be available to take over as the main server in the event of a Directory failover.

To set up Directory failover and load balancing:

1. From the Config Tool homepage, open the *System* task and click the **Roles** view.
2. Select the **Directory Manager** () role, and click the **Directory servers** tab.
3. Click **Add an item** (+).
4. In the dialog box that appears, select the server you want to add, its connection port (default=5500), and click **Add**.

   The server is added to the failover list.
5. Add more Directory servers if necessary.
6. Update your license to include the servers you've just promoted to Directory servers.
7. Click **Apply**.

The expansion servers are converted into Directory servers and the updated license is applied to all Directory servers in the list. Client applications and roles on expansion servers can connect to Security Center using any of the Directory servers.

Related Topics

Setting up a Directory server for disaster recovery on page 169

Forcing a Directory server to always be the main server

If one of the *Directory servers* is your preferred choice to be the *main server*, you can force it to always be the main server whenever it is available.

What you should know

The first server in the Directory servers list is your *default* main server. When a Directory failover occurs, the next server in line becomes the new main server (). When the first server is back online after a failover, the default behavior is to keep the current server as the main server and not switch back to the first server. This behavior minimizes system disruptions caused by applications having to disconnect and reconnect to the main server. If this is not the behavior you want for your system, you can change it in the **Directory servers** tab.

To change the priority of the servers in the Directory failover list:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Select the **Directory Manager** (🌐) role, and click the **Directory servers** tab.

3 Select a server in the list, and click **Up** (▲) or **Down** (▼) to move the Directory servers up or down in the list.

4 To force the first server in the failover list to be the main server whenever it is available, select **Force the first server in the list to be the main server** option.

5 Click **Apply**.

Setting up a Directory server for disaster recovery

Configuring a Directory server to be a *disaster recovery* server excludes the server from load balancing. A disaster recovery server only activates if it takes over as the main server during a Directory failover.

Before you begin

Set up Directory failover and load balancing.

What you should know

- If a *Directory server* is at a remote location or has a slow connection, you can enable the disaster recovery option so that it does not slow down the system by participating in load balancing.
- A disaster recovery server does not accept client connections unless it becomes the *main server* during a Directory failover.
- Roles such as the Media Router, Health Monitor, and Report Manager are often hosted on Directory servers. If you are enabling disaster recovery, you must enable the **Force execution on highest priority server** option on all roles that are hosted on Directory servers. This ensures that these roles do not continue to run on the disaster recovery server after the primary Directory server is back online. For more information, see Role failover on page 160.

To set up a disaster recovery server:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Select the **Directory Manager** (🌐) role, and click the **Directory servers** tab.

3 At the bottom of the server list, click **Advanced** (⚙).

An extra column, **Disaster recovery**, is displayed in the list.

4 Select **Disaster recovery** for one or more Directory servers.

NOTE: The **Disaster recovery** option only applies to Directory servers, not to Gateways.

5 Click **Apply**.

The server is excluded from load balancing and only accepts client connections if it becomes the main server during a Directory failover.

Related Topics

Setting up Directory failover and load balancing on page 168

Switching the main server

If necessary, you can assign any server in the Directory failover list to be the main server. For example, when maintenance work needs to be done on the current main server.

To switch the main server:

1. From the Config Tool homepage, open the *System* task and click the **Roles** view.
2. Select the **Directory Manager** (🌐) role, and click the **Directory servers** tab.
3. Select a server, and click **Activate Directory** (●).
4. Click **Apply**.

All client applications and roles are disconnected, the main server switches to the Directory server you selected, and all applications and roles reconnect.

Reactivating Security Center license for Directory failover systems

Every time you add, remove, or change the servers in the Directory failover list, you must generate a new validation key and reactivate your Security Center license from Config Tool.

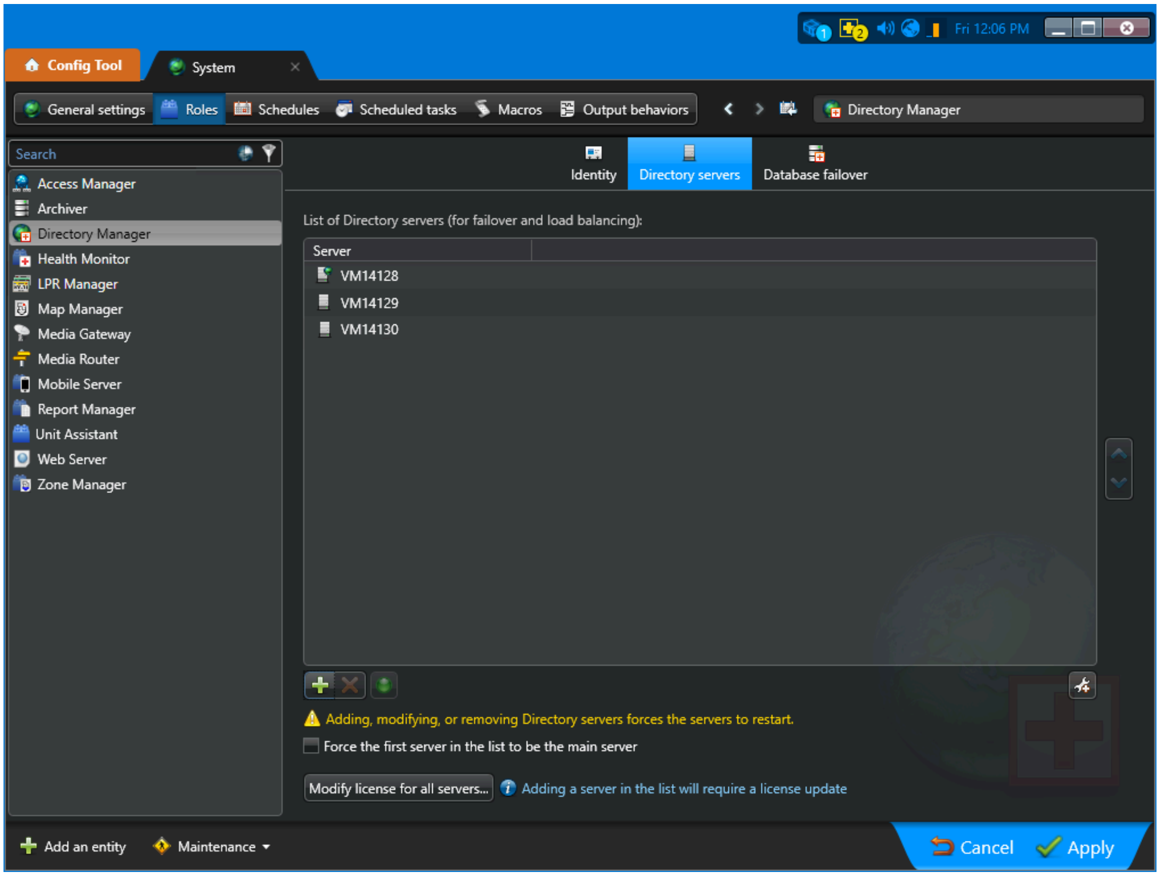
What you should know

IMPORTANT: When you have multiple Directory servers configured for failover, you must generate the validation key and apply the license key from Config Tool instead of Server Admin. All Directory servers must be up and running for the license update to work.

To reactivate the Security Center license for a multiple Directory server system:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Select the **Directory Manager** ( ) role, and click the **Directory servers** tab.



List of Directory servers (for failover and load balancing):

Server
VM14128
VM14129
VM14130

Adding, modifying, or removing Directory servers forces the servers to restart.

□ Force the first server in the list to be the main server

Adding a server in the list will require a license update

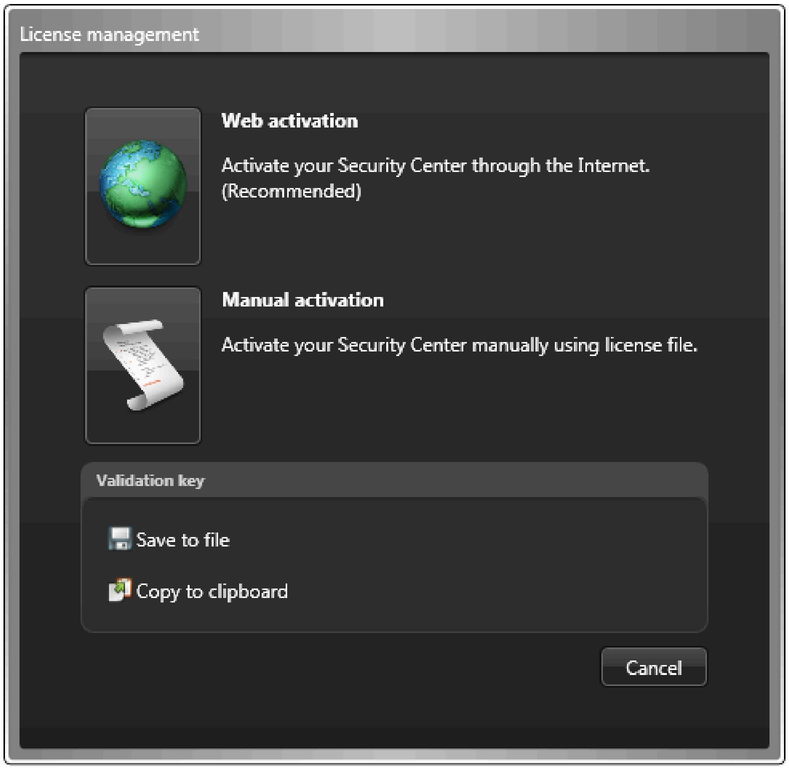
3 Click **Modify license for all servers**.

4 In the *License management* dialog box, reactivate your license one of the following ways:

- **Web activation:** (Recommended) Reactivate your license from the Internet. In the dialog box that opens, enter your *System ID* and *Password*, and click **Activate** > **Apply** > **Apply**. The process is complete.

Your system ID and password are specified in the *Security Center License Information* document. Our Customer Service team sends you this document when you purchase the product.

- **Manual activation:** If your workstation has no Internet access, reactivate your Security Center license manually using a license file. Continue with the next step.

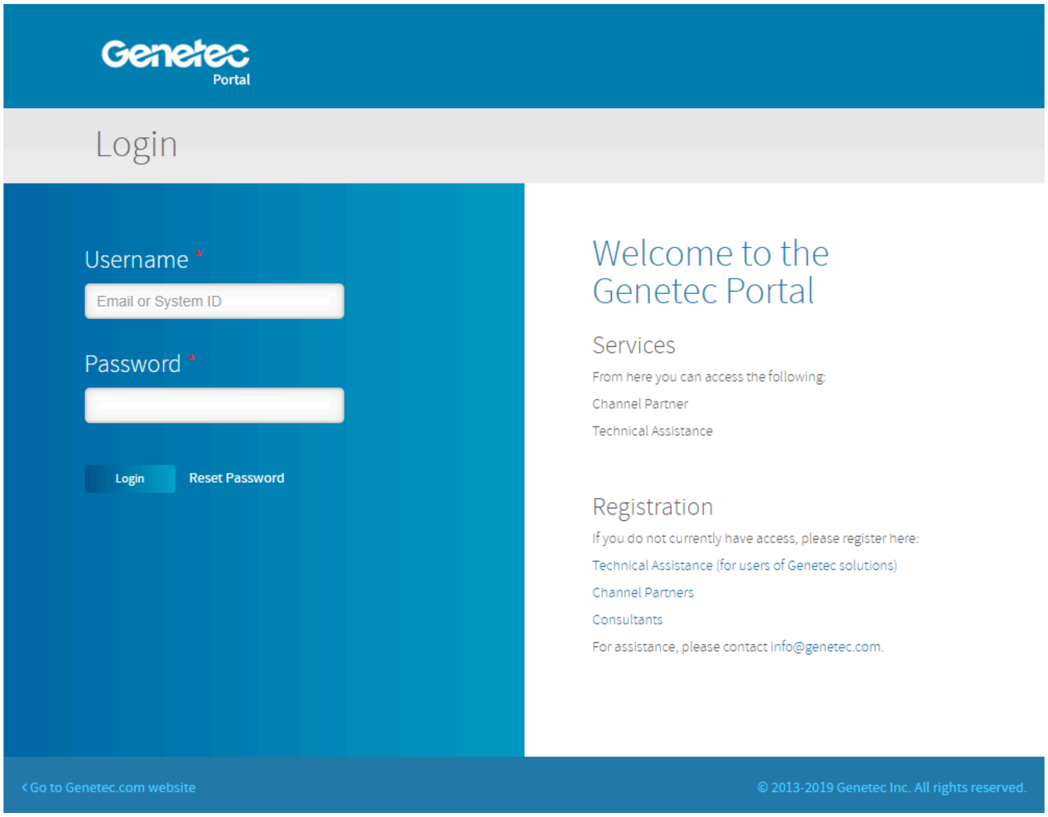

License management
Web activation
Activate your Security Center through the Internet. (Recommended)
Manual activation
Activate your Security Center manually using license file.
Validation key
Save to file
Copy to clipboard
Cancel

5 Click **Save to file** to save the composite validation key to a file.

IMPORTANT: You must use the *composite* validation key that comprises all Directory servers, or the license reactivation fails silently and the Directory failover does not work.

A text file named *validation.vk* is saved to your default *Downloads* folder. Copy the file to a USB key or a location that you can access from a computer that has internet access.

6 From a computer with internet access, open GTAP at: https://portal.genetec.com/support.



Welcome to the Genetec Portal

Services

From here you can access the following:

Channel Partner

Technical Assistance

Registration

If you do not currently have access, please register here:

Technical Assistance (for users of Genetec solutions)

Channel Partners

Consultants

For assistance, please contact info@genetec.com.

© 2013-2019 Genetec Inc. All rights reserved.

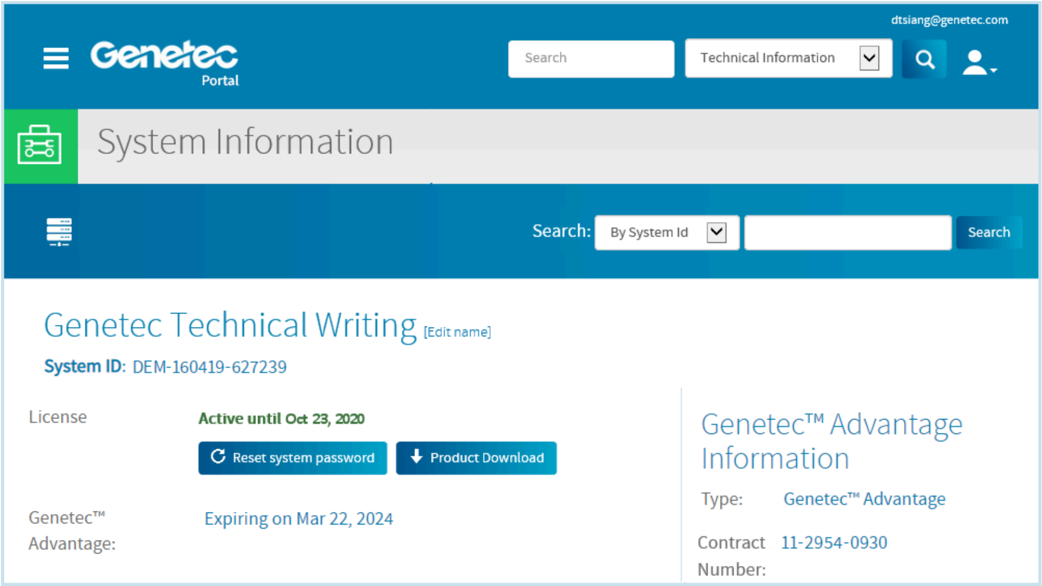
7 On the *Login* page, do one of the following:

- Enter your system ID and password, and then click **Login**.
- Enter your GTAP user account (your email address) and password, and then click **Login**

8 On the GTAP homepage, open the **Genetec Portal** menu and click **Technical Assistance** > **System Management**.

9 On the *System Management* page, type your system ID and click **Search**.

The *System Information* page opens.



Genetec Technical Writing

System ID: DEM-160419-627239

License: Active until Oct 23, 2020

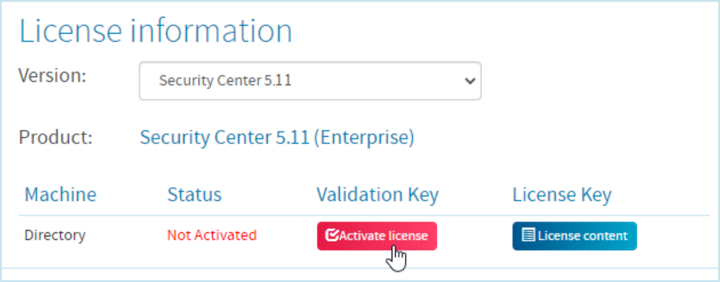
Genetec™ Advantage: Expiring on Mar 22, 2024

Genetec™ Advantage Information

Type: Genetec™ Advantage

Contract Number: 11-2954-0930

10 In the *License information* section, click **Activate license**.



License information

Version: Security Center 5.11

Product: Security Center 5.11 (Enterprise)

Machine	Status	Validation Key	License Key
Directory	Not Activated	Activate license	License content

11 In the dialog box that opens, browse to your validation key (.vk file), and click **Submit**.

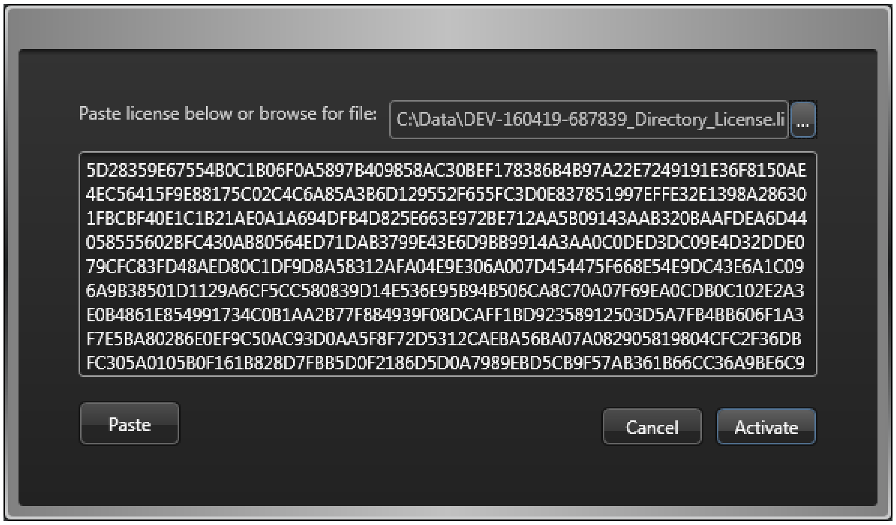
12 When you receive the License activation successful message, click **Download** under *License Key* and save the license key to a file.

The default file name is your system ID, followed by *_Directory_License.lic*.

13 Return to the Config Tool workstation.

14 In the *License management* dialog box, click **Manual activation**.

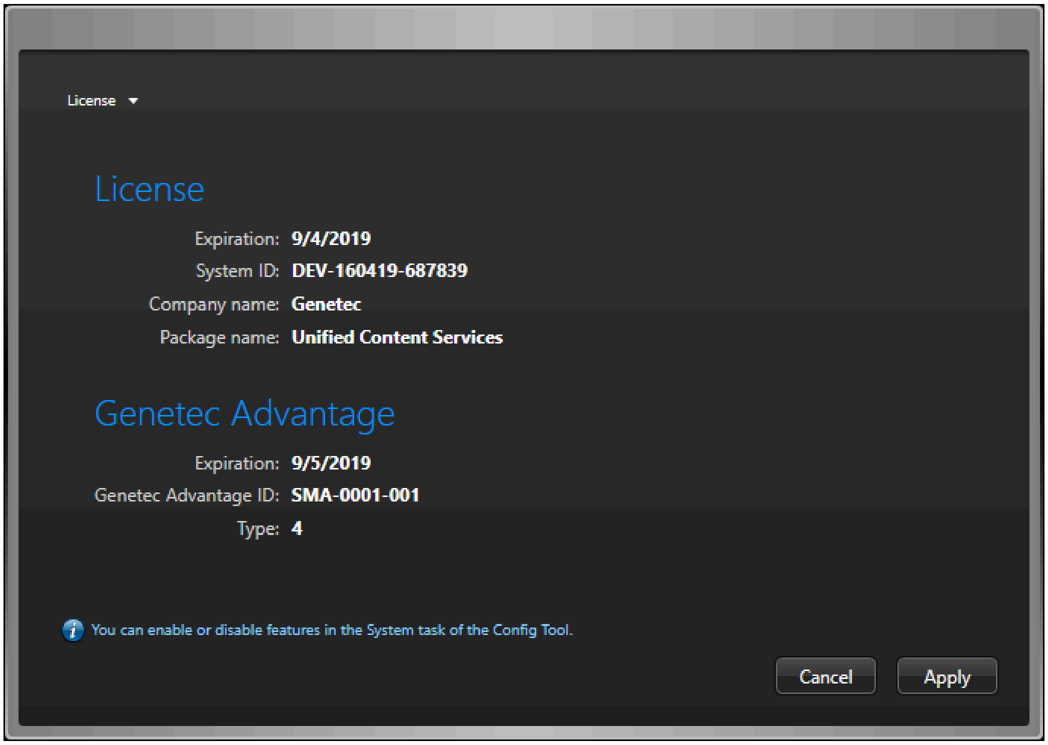
15 In the *Manual activation* dialog box, browse for the license key file, and click **Open**.



Paste license below or browse for file: C:\Data\DEV-160419-687839_Directory_License.li

```
5D28359E67554B0C1B06F0A5897B409858AC30BEF178386B4B97A22E7249191E36F8150AE
4EC56415F9E88175C02C4C6A85A3B6D129552F655FC3D0E837851997EFFE32E1398A28630
1FBCBF40E1C1B21AE0A1A694DFB4D825E663E972BE712AA5B09143AAB320BAAFDEA6D44
058555602BFC430AB80564ED71DAB3799E43E6D9BB9914A3AA0C0DED3DC09E4D32DDE0
79CFC83FD48AED80C1DF9D8A58312AFA04E9E306A007D454475F668E54E9DC43E6A1C09
6A9B38501D1129A6CF5CC580839D14E536E95B94B506CA8C70A07F69EA0CDB0C102E2A3
E0B4861E854991734C0B1AA2B77F884939F08DCAFF1BD92358912503D5A7FB4BB606F1A3
F7E5BA80286E0EF9C50AC93D0AA5F8F72D5312CAEBA56BA07A082905819804CFC2F36DB
FC305A0105B0F161B828D7FBB5D0F2186D5D0A7989EBD5CB9F57AB361B66CC36A9BE6C9
```

16 Click **Activate**.
A dialog box showing your license information opens.



License

Expiration: 9/4/2019
System ID: DEV-160419-687839
Company name: Genetec
Package name: Unified Content Services

Genetec Advantage

Expiration: 9/5/2019
Genetec Advantage ID: SMA-0001-001
Type: 4

You can enable or disable features in the System task of the Config Tool.

17 Click **Apply** to close the dialog box, and click **Apply** at the bottom of the Config Tool window to save your changes.

Reapplying Security Center license on Directory failover systems

Whenever your Security Center license for a Directory failover system is updated, you must reapply the license from Config Tool for the changes to take effect. Updates include adding new camera connections, extending expiry dates, and so on.

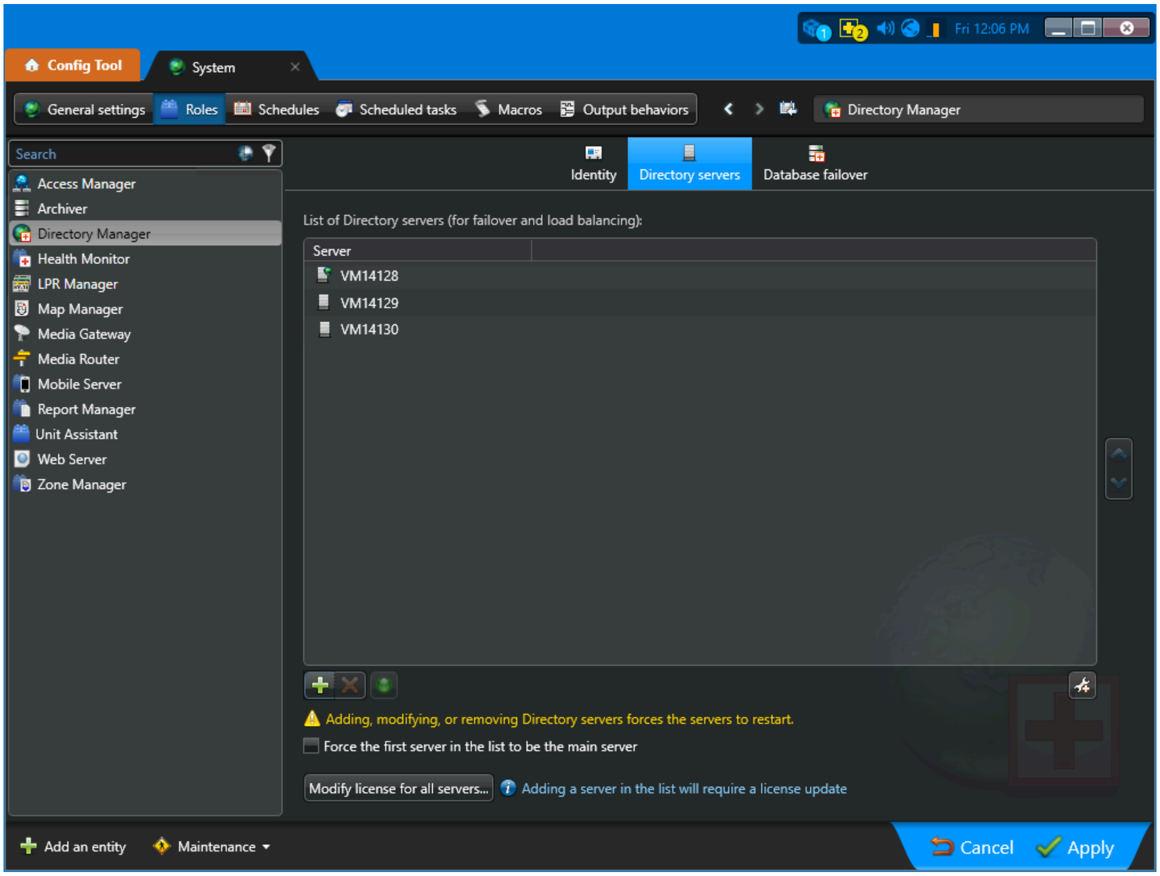
What you should know

If you added, removed, or changed the servers in the Directory failover list, you must generate a new validation key and reactivate your Security Center license instead.

To reapply the Security Center license to a Directory failover system:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Select the **Directory Manager** (🌐) role, and click the **Directory servers** tab.



List of Directory servers (for failover and load balancing):

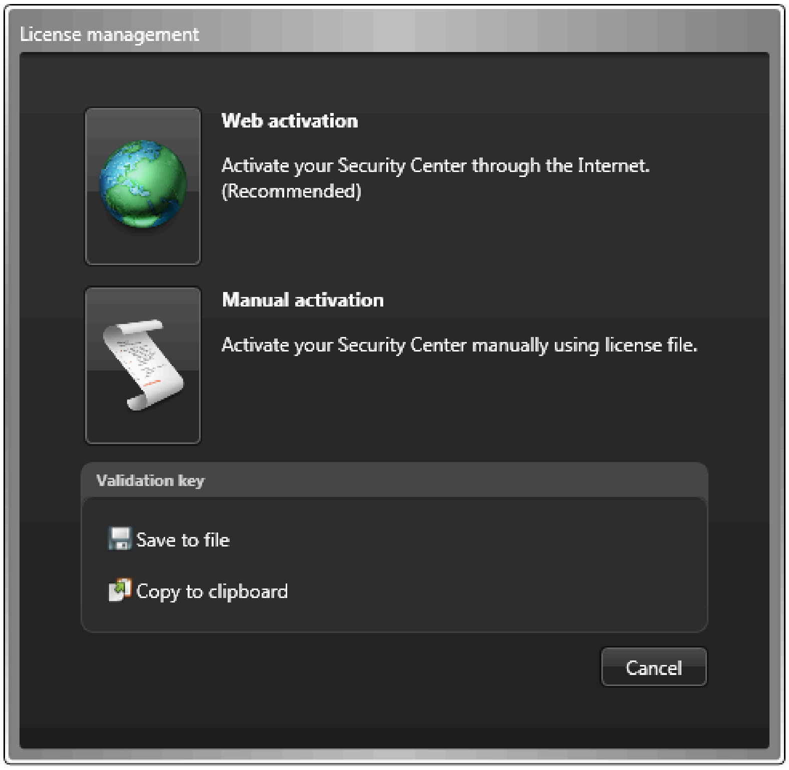
Server
VM14128
VM14129
VM14130

⚠ Adding, modifying, or removing Directory servers forces the servers to restart.

□ Force the first server in the list to be the main server

Adding a server in the list will require a license update

3 Click **Modify license for all servers**.
The *License management* dialog box opens.

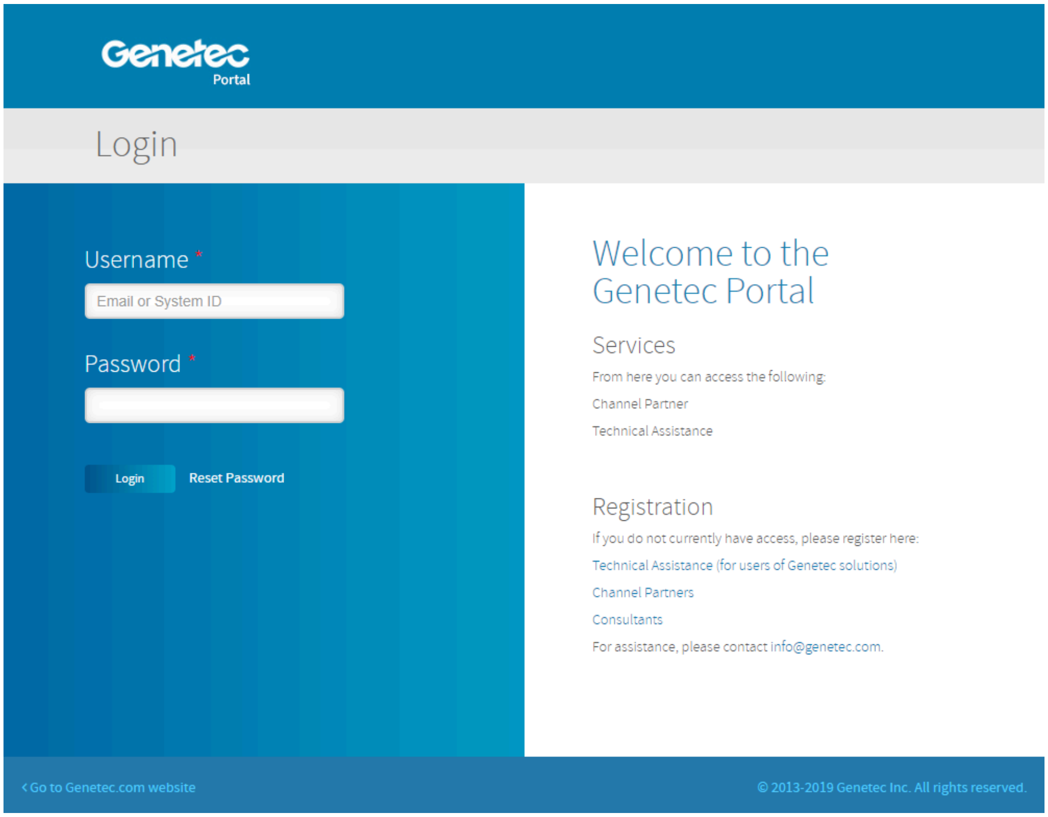


4 In the *License management* dialog box, reapply your license in one of the following ways:

- **Web activation:** (Recommended) Reapply your license from the Internet. In the dialog box that opens, enter your *System ID* and *Password*, and click **Activate** > **Apply** > **Apply**. The process is complete.

  Your system ID and password are specified in the *Security Center License Information* document. Our Customer Service team sends you this document when you purchase the product.
- **Manual activation:** If your workstation has no Internet access, reapply your Security Center license manually using a license file. Continue with the next step.

5 From a computer with internet access, open GTAP at: https://portal.genetec.com/support.



Genetec Portal

Login

Username *

Email or System ID

Password *

Login Reset Password

Welcome to the Genetec Portal

Services

From here you can access the following:

Channel Partner

Technical Assistance

Registration

If you do not currently have access, please register here:

Technical Assistance (for users of Genetec solutions)

Channel Partners

Consultants

For assistance, please contact info@genetec.com.

‹ Go to Genetec.com website

© 2013-2019 Genetec Inc. All rights reserved.

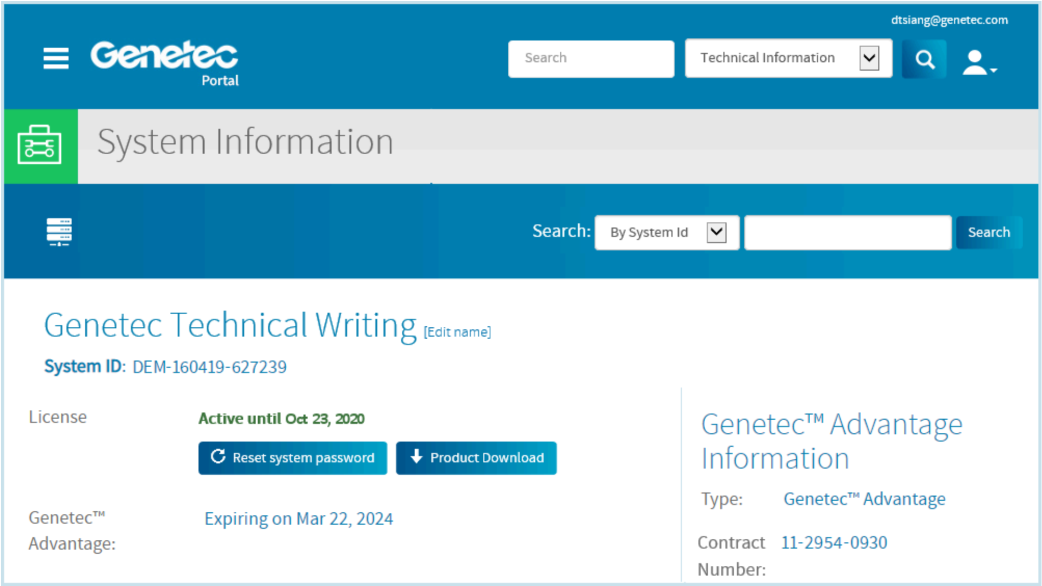
6 On the *Login* page, do one of the following:

- Enter your system ID and password, and then click **Login**.
- Enter the email address for your GTAP user account and password, and then click **Login**

7 On the GTAP homepage, open the **Genetec Portal** menu and click **Technical Assistance** > **System Management**.

8 On the *System Management* page, type your system ID and click **Search**.

The *System Information* page opens.



dtsiang@genetec.com

Genetec Portal

Search

Technical Information

System Information

Search: By System Id Search

Genetec Technical Writing [Edit name]

System ID: DEM-160419-627239

License: Active until Oct 23, 2020

Reset system password Product Download

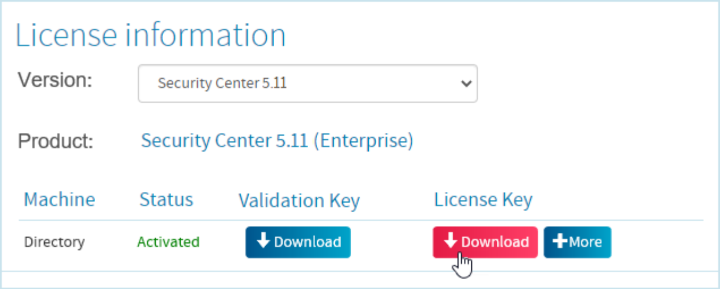
Genetec™ Advantage: Expiring on Mar 22, 2024

Genetec™ Advantage Information

Type: Genetec™ Advantage

Contract Number: 11-2954-0930

9. In the *License information* section, click **Download** under *License Key* and save the license key to a file.



License information

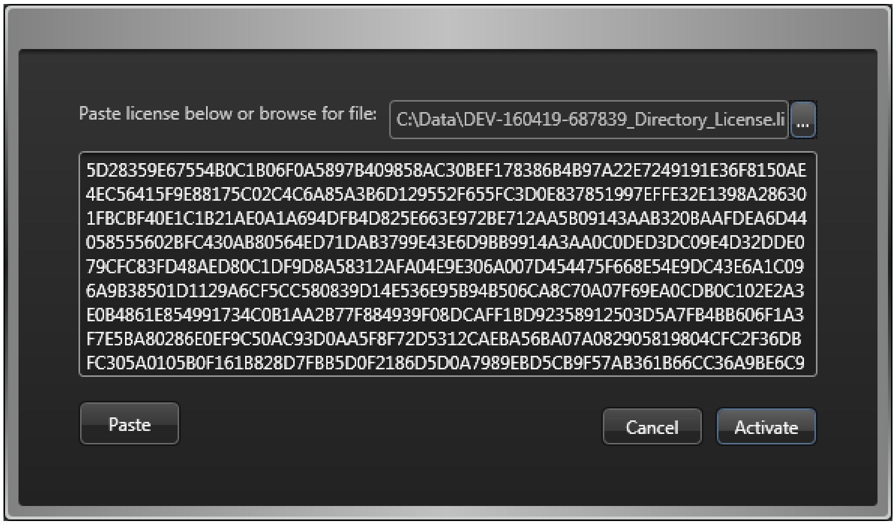
Version: Security Center 5.11

Product: Security Center 5.11 (Enterprise)

Machine	Status	Validation Key	License Key
Directory	Activated	Download	Download More

The default file name is your system ID, followed by *_Directory_License.lic*.

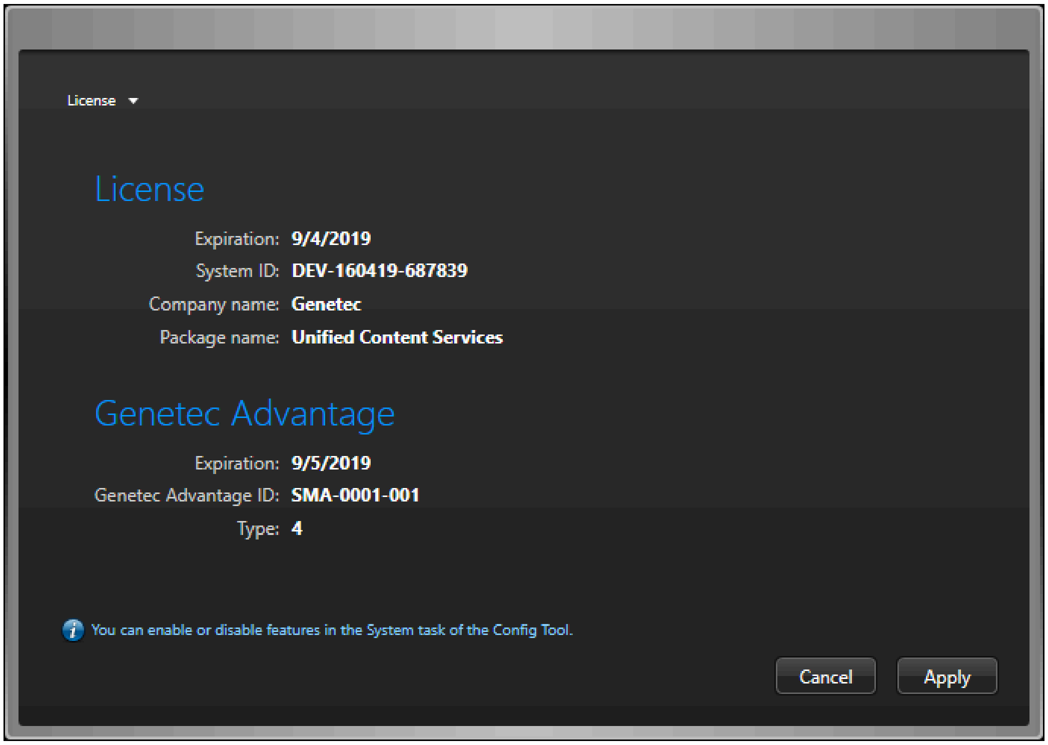
10. Return to the Config Tool workstation with the license key file.
11. In the *License management* dialog box, click **Manual activation**.
12. In the *Manual activation* dialog box, do one of the following:
    - Paste your license information from the license key file by copying the content from a text editor.
    - Browse for the license key (.lic file), and click **Open**.



Paste license below or browse for file: C:\Data\DEV-160419-687839_Directory_License.li

```
5D28359E67554B0C1B06F0A5897B409858AC30BEF178386B4B97A22E7249191E36F8150AE
4EC56415F9E88175C02C4C6A85A3B6D129552F655FC3D0E837851997EFFE32E1398A28630
1FBCBF40E1C1B21AE0A1A694DFB4D825E663E972BE712AA5B09143AAB320BAAFDEA6D44
058555602BFC430AB80564ED71DAB3799E43E6D9BB9914A3AA0C0DED3DC09E4D32DDE0
79CFC83FD48AED80C1DF9D8A58312AFA04E9E306A007D454475F668E54E9DC43E6A1C09
6A9B38501D1129A6CF5CC580839D14E536E95B94B506CA8C70A07F69EA0CDB0C102E2A3
E0B4861E854991734C0B1AA2B77F884939F08DCAFF1BD92358912503D5A7FB4BB606F1A3
F7E5BA80286E0EF9C50AC93D0AA5F8F72D5312CAEBA56BA07A082905819804CFC2F36DB
FC305A0105B0F161B828D7FBB5D0F2186D5D0A7989EBD5CB9F57AB361B66CC36A9BE6C9
```

13 Click **Activate**.
A dialog box showing your license information opens.



License

Expiration: 9/4/2019
System ID: DEV-160419-687839
Company name: Genetec
Package name: Unified Content Services

Genetec Advantage

Expiration: 9/5/2019
Genetec Advantage ID: SMA-0001-001
Type: 4

You can enable or disable features in the System task of the Config Tool.

14 Click **Apply** to close the dialog box, and click **Apply** at the bottom of the Config Tool window to save your changes.

Replacing the main server in a Directory failover environment

In a Directory failover environment, when your main server is no longer adequate, you can replace one of your secondary Directory servers with a new machine, then switch the main server to that machine with minimal downtime.

Before you begin

- If you have a single Directory system, read Replacing the main server on page 125, instead.
- Have your System ID and password ready.

  Your system ID and password are specified in the *Security Center License Information* document. Our Customer Service team sends you this document when you purchase the product.

What you should know

This server migration scenario works with the following assumptions:

- None of your existing Directory servers is adequate to assume the role the main server in the long run.
- You have an adequate new machine ready to replace the old main server.
- All your Directory servers are up and running.
- You do not intend to increase the number of Directory servers in your system. Therefore, you do not need to update your current license.

NOTE: There is a brief system downtime when all roles and applications switch from the old main server to the new one. So pick the right time to perform this operation.

To replace the main server in a failover environment:

1. Install Security Center on the new machine using the *Expansion server* configuration and connect it to the main server.

   For more information, see the *Security Center Installation and Upgrade Guide*.

   The new machine is now part of your system as an expansion server.
2. Log on to your system with Config Tool.
3. If there are roles other than the Directory role hosted on the main server, move them to the new server.

   You need to do this if you intend to decommission your old main server at the end of this operation. To see which roles are running on the main server:

   a) Open the *Network view* task.

   b) Select the main server () and click the **Identity** tab.

   c) In the **Relationships** tree, expand the **Roles** node.
4. Open the *System* task and click the **Roles** view.
5. Select the **Directory Manager** () role, and then click the **Directory servers** tab.
6. Select a server that is not your main server, and click **Remove the item** (✗).

   This is only temporary so you do not exceed the number of Directory servers permitted by your license.
7. Click **Add an item** (➕), select the server you just added, and click **Add**.
8. Reactivate your Security Center license with the new list of Directory servers from Config Tool.
9. Select the new server, click **Activate Directory** (●) and then click **Apply**.

   The new server is now your main server. This causes a brief disruption to your system as all roles and client applications must disconnect from the old server and connect to the new one.

10 Select the old main server and click **Remove the item** (✖).

11 Click **Add an item** (✚), select the server you temporarily removed from the Directory failover list, and click **Add**.

12 Reactivate your Security Center license one more time for the new list of Directory servers from Config Tool.

The old main server is now running as a regular expansion server.

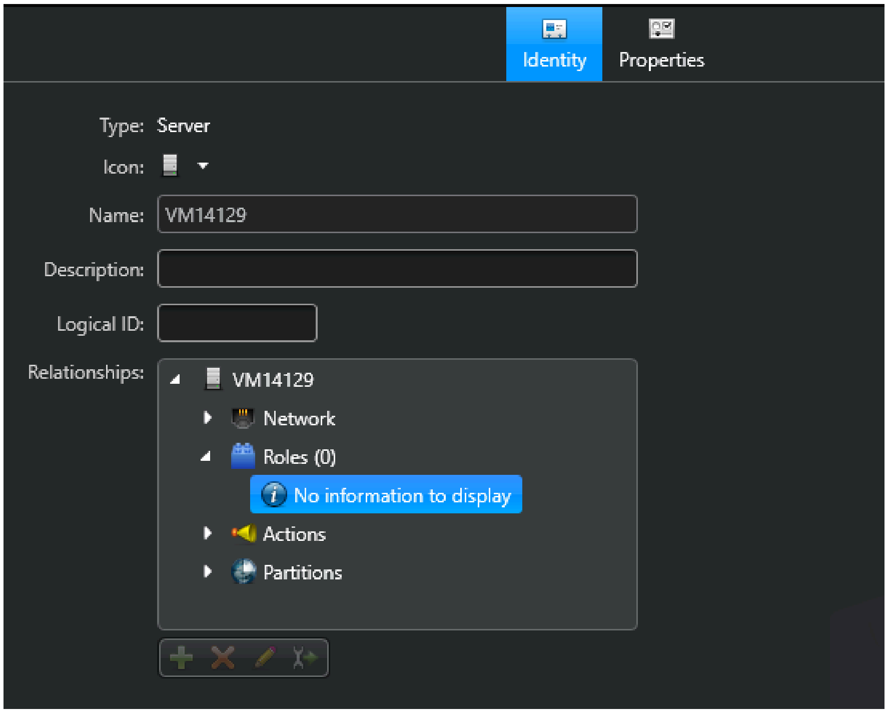
13 (Optional) Decommission your old main server.

a) Open the *Network view* task, and confirm that all your expansion servers are online (🖥).

b) Select the old main server and click **Delete** (✖) and **Delete**.

No role should be running on the old main server, otherwise the deletion would fail.

TIP: The list of roles should be empty in the **Identity** tab.



Type: Server
Icon:
Name: VM14129
Description:
Logical ID:
Relationships:
VM14129
Network
Roles (0)
No information to display
Actions
Partitions

c) Uninstall Security Center from your old server.

After you finish

Notify your users with the DNS name or IP address of your new main server.

Removing servers from the Directory failover list

If you no longer need a server as a Directory server for Directory failover or load balancing, you can remove it from the Directory failover list.

What you should know

Do not try to remove a server from the Directory failover list by deactivating the Directory on that server from Server Admin. Your change will not be permanent because the Directory Manager will change it back to a Directory server.

To remove a server from the Directory failover list:

1. From the Config Tool homepage, open the *System* task and click the **Roles** view.
2. From the Config Tool homepage, open the *System* task and click the **Roles** view.
3. Select the **Directory Manager** (🌐) role, and then click the **Directory servers** tab.
4. Select the servers you want to remove, and click **Remove the item** (✖).
5. Update your license to exclude the servers you've just removed.
6. Click **Apply**.

The removed servers become expansion servers, and the updated license is applied to all remaining Directory servers. Users can no longer connect to the system using the servers that have been removed. Clients connected to Security Center through these servers are disconnected, and reconnected to the remaining Directory servers.

Example

You just added a new computer to your system and want to use the server on that computer as a Directory server; however, you are already using five Directory servers. You can remove one of the existing servers from the Directory failover list to make room for the new server.

Bypassing load balancing on workstations

If you have more than one Directory server on your system, but you do not want users to be redirected to another server when they log on to Security Center, you can bypass the load balancing.

What you should know

When you have more than one Directory server on your system, load balancing is automatically in effect. This means that every time a user logs on to Security Center, the Directory Manager redirects their logon request to the next Directory server in the list, based on the server that the previous user connected to.

You can bypass the load balancing behavior on specific workstations (applied to Config Tool and Security Desk), which is helpful when a client is on a remote LAN.

To bypass load balancing on a workstation:

1. From the homepage, click **Options** > **General**.
2. Select the **Prevent connection redirection to different Directory servers** option.
3. Click **Save**.

Directory database failover

You can fail over the Directory database using either the backup and restore failover mode or the mirroring failover mode.

Three database failover modes are supported for the Directory:

- **Backup and restore:** The Directory Manager protects the Directory database by regularly backing up the master database instance (source copy). During a failover, the Directory connects to the backup database containing the data from the last restore operation. Two schedules can be defined: one for full backups, and another for differential backups.
- **Mirroring:** Database failover is taken care of by Microsoft SQL Server and is transparent to Security Center. The *Principal* and *Mirror* instances of the Directory database are kept in sync at all times. There is no loss of data during failover.
- **SQL AlwaysOn:** Use this failover mode if you are using the Windows feature SQL AlwaysOn as your high availability and disaster recovery solution.

Limitations of the backup and restore failover mode

- To preserve the changes made to your system configuration while you were operating from the backup database, you must restore the latest contingency backup (created in the *ContingencyBackups* subfolder under the restore folder) to your master database after reactivating it.
- To avoid losing the configuration changes made while you were operating from the backup database, you can change the backup database to the master database. To do this, select it from the database failover list to move it to the top of the list. However, keep in mind that your backup database is only as up to date as the most recent backup before the failover took place.

Differences between the backup and restore mode and the mirroring mode

The following table compares the differences between the two database failover modes.

Backup and restore (Directory Manager)	Mirroring (Microsoft SQL Server)
Multiple backup instances of the Directory database are kept relatively in sync with its master instance through regular backups performed by the Directory Manager role.	A single copy (the mirror instance) of the Directory database is kept perfectly in sync with the master copy (or principal instance) using SQL Server database mirroring.
The failover database can only be as up to date as the most recent backup.	The failover database is an exact copy of the principal database.
Changes made while the Directory is connected to the backup database are lost when the Directory switches back to the master database.	Changes can be made to the Directory database at any time without ever losing data.
Both master and backup databases must be hosted on Security Center *servers*.	The principal and mirror database instances can be hosted on any computer.
Can work with SQL Server Express edition which is free.	Requires SQL Server 2008 Standard Edition or better, that supports mirroring.
Recommended when the entity configurations are not frequently updated.	Recommended when entity configurations are frequently updated, such as for cardholder and visitor management.

Backup and restore (Directory Manager)	Mirroring (Microsoft SQL Server)
Causes a temporary disconnection of all client applications and roles while the database failover is in progress.	Causes the Directory to restart if the principal server is unavailable for longer than a few seconds.
Database failover is handled by the Directory Manager role.	Database failover is executed by a separate *Witness server* running on SQL Server Express (optional but highly recommended) or it has to be manually detected and executed by the database administrator.

Related Topics

Setting up Directory database failover through backup and restore on page 187
Setting up Directory database failover through mirroring on page 189
Setting up Directory database failover through SQL AlwaysOn on page 190

Setting up Directory database failover through backup and restore

To protect the Directory database by regularly backing up the master database instance, you can set up Directory database failover using the backup and restore method.

Before you begin

- Your Security Center license must support multiple *Directory servers*. If you need to update your license, see the *Security Center Installation and Upgrade Guide*.

  NOTE: The *Directory Manager* () role is created automatically in Config Tool when your license supports multiple Directory servers.
- All database servers must be accessible from all Directory servers. You must configure the remote database server (SQL Server) to accept connection requests from the roles.
- All database instances must be the same version, and an expansion server must be installed on each database server. For more information about installing expansion servers, see the *Security Center Installation and Upgrade Guide*.

What you should know

Once *Backup and restore* failover mode is enabled, you no longer back up the Directory database from Server Admin, but from Config Tool.

Changes made to the system configuration while you were operating from the backup database are not automatically restored to the master database when it is restored to active service.

To use backup and restore as your Directory database failover solution:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

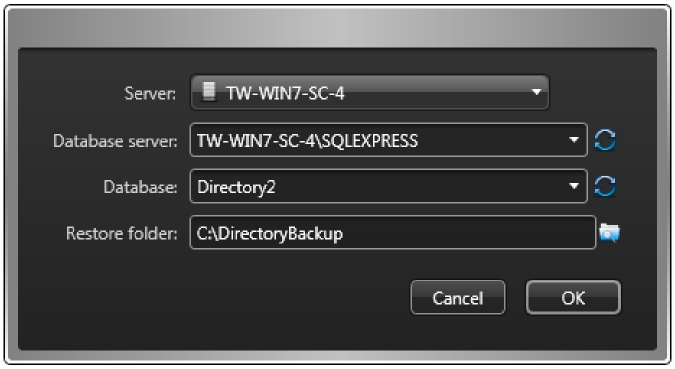
2 Select the Directory Manager () role, and click the **Database failover** tab.

3 Switch the **Use database failover** option to **ON**.

4 Select **Backup and restore** for **Failover mode**.

5 Click **Add an item** (✚).

6 In the dialog box that appears, specify the Security Center server, the database server, the database instance, and the folder where the backup files should be copied.



Server: TW-WIN7-SC-4

Database server: TW-WIN7-SC-4\SQLEXPRESS

Database: Directory2

Restore folder: C:\DirectoryBackup

You can assign as many backup databases as you want. However, the more backup databases you have, the longer it takes to back up the Directory database content.

7. Click **OK**.

   The new backup database instance is added.

   NOTE: The server flagged as **(Master)** is the one hosting the database. The green LED (●) indicates the database that is active, which is not necessarily the *master*.

8. To force all Directory servers to reconnect to the master database after it is back online after a failover, select the **Automatically reconnect to master database** option. Note that this option only works if the primary Directory server is online.

   CAUTION: Switching the active database causes a short service disruption, and all changes made to the system configuration while the master database was offline are lost. Use this option only if you are ready to lose the changes made to the system configuration while you were operating from the backup database.

9. Under **Master backup**, specify the frequency at which the *full backup* and the *differential backup* should be generated.

   A differential backup only contains the database transactions made since the previous backup, so it is much faster to generate than a full backup. Frequent differential backups ensure that your backup database is most up to date when you fail over, but might take longer to restore.

10. Click **Apply**.

After you finish

CAUTION: After the *Backup and restore* failover mode is enabled, all subsequent changes to the master database from Server Admin (restoring a previous backup for example) must immediately be followed by a full manual backup executed from Config Tool. Failing to do so causes your master and backup databases to become out of sync and the database failover mechanism to no longer work.

Related Topics

Directory database failover on page 185

Backing up the Directory database with failover

Once the *Backup and restore* failover mode is enabled, all manual backups of the Directory database must be performed from the Directory Manager's *Database failover* page in Config Tool.

What you should know

If the *Backup and restore* failover mode is not enabled, back up the Directory database from Server Admin.

To generate a full backup of the Directory database:

1. From the Config Tool homepage, open the *System* task and click the **Roles** view.
2. Select the Directory Manager (🌐) role, and click the **Database failover** tab.
3. In the *Master backup* section, click **Generate full backup**.

A full Directory backup is generated in the Security Center backup folder (default=*C:\SecurityCenterBackup*) on the database server. All configuration files (*config*, *gconfig*, and *xml* files) are backed up on the main server.

Setting up Directory database failover through mirroring

To protect the Directory database so you do not lose any data if a failover occurs, you can set up Directory database failover to use Microsoft SQL Server Database Mirroring.

Before you begin

- Microsoft Database Mirroring is being phased out. For new installations, it is recommended to use SQL AlwaysOn.
- The *Principal* database server, the *Mirror* database server, and the *Witness* server (the *Witness* server is optional, but highly recommended) must be configured. For the configuration of SQL Server for mirroring, please refer to Microsoft SQL Server Database Mirroring documentation.
- Your Security Center license must support multiple *Directory servers*. If you need to update your license, see the *Security Center Installation and Upgrade Guide*.

  NOTE: The *Directory Manager* () role is created automatically in Config Tool when your license supports multiple Directory servers.
- The database servers must be running on remote computers from the Directory servers. Move the databases to other computers.
- All database servers must be accessible from all Directory servers. You must configure the remote database server (SQL Server) to accept connection requests from the roles.
- The *Principal* and the *Mirror* databases must be of the same version. For more information on database mirroring, such as how to perform manual backup and restore, refer to the Microsoft SQL Server Database Mirroring documentation.

What you should know

With Database Mirroring, the database failover is handled by Microsoft SQL Server. The *Principal* and *Mirror* instances of the Directory database are kept in sync at all times. There is no loss of data during failover.

NOTE: Following a database failover, the first database query performed by Security Center client applications are likely to fail. When a query fails, the message "Database transaction has failed" appears on screen. Close the message box and try again to resume normal operation.

To use Database Mirroring as your Directory database failover solution:

1. From the Config Tool homepage, open the *System* task and click the **Roles** view.
2. Select the Directory Manager () role, and click the **Database failover** tab.
3. Switch the **Use database failover** option to **ON**, and select the **Mirroring** option.

   The database you're currently connected to is the *Principal* database.
4. Under **Mirror database**, enter the database server name of the *Mirror* database.
5. Click **Apply**.

Related Topics

Directory database failover on page 185

Setting up Directory database failover through SQL AlwaysOn

If you are using the Windows feature *SQL AlwaysOn* as your Directory database failover solution, you must configure the Directory Manager to use SQL AlwaysOn in Config Tool.

Before you begin

All database servers must be accessible from all Directory servers. You must configure the remote database server (SQL Server) to accept connection requests from the roles.

To use SQL AlwaysOn as your Directory database failover solution:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Select the Directory Manager ( ) role, and click the **Database failover** tab.

3 Switch the **Use database failover** option to **ON**, and select the **SQL AlwaysOn** option.

4 Click **Apply**.

Related Topics

Directory database failover on page 185

Archiver failover

Adding a standby server to your Archiver role minimizes the downtime of your live video if a hardware failure occurs.

How Archiver failover works

If the server hosting the *Archiver* role fails, you lose access to live video and archived video. Live video is disabled because the Archiver controls the *video units*. Access to archived video is disabled because your archives can only be accessed through the Archiver that created them (even if your *database server* is not the computer that failed).

For Archiver failover, the following conditions apply:

- You can assign a primary server, a secondary server, and a tertiary server to an Archiver role. This is especially useful in multi-site systems, as you can protect the primary and secondary servers at a local site with a tertiary server located at a remote site.
- The primary, secondary, and tertiary servers must each have their own database, hosted locally, or on another computer.
- To make sure that the video and audio archived by the *primary server* is still available if it fails to a secondary or tertiary server, you must turn on *redundant archiving*. This ensures that all servers can archive video at the same time, and that they each manage their own copy of the video archive. You can set up redundant archiving on all cameras managed by the Archiver role, or protect just a few important cameras

Careful load planning for failover

If failover occurs, the performance of a standby server might be affected by the additional archiving load (number of cameras, video quality, and so on) from the new Archiver role. If the standby server hosts other roles, this also affects archiving capability.

When selecting a server as a standby server for an Archiver role, consider the following:

- If the server has other functions, it might not be able to absorb the full load of another server.

  TIP: To lessen the failover load on a server, create multiple Archiver roles with fewer video units each. Also, configure all the Archiver roles to share the same primary server, but to fail over to different secondary or tertiary servers.
- How long is a typical failover expected to last? The longer a failover lasts, the more additional disk space you need to reserve for archiving.
- A server can handle more video units when only command and control functionality is needed. If video archiving is not important on all cameras, you can associate all important cameras to one Archiver role and give it a higher *archiving priority* than the rest. That way, if multiple Archiver roles fail over to the same server at the same time, archiving will be maintained for the important cameras.

WARNING: Never have two distinct Archiver roles share a same logical disk for archive storage. A common mistake is to configure the primary server of two Archiver roles as the standby server of the other, while sharing the same archive storage space. This means that when one of the role's primary server fails, both roles end up running on the same server and writing to the same logical disk. The proper way to configure this type of cross-failover is to have each server control two logical disks, but only assign one logical disk to each Archiver role, so that when both roles are running on the same server, each role writes to its own disk.

Limitations of Archiver failover

The failover process can take 15-30 seconds for cameras to come back online. During this time, live video cannot be viewed and Auxiliary Archiver roles do not record. However, the gap in recorded video is much shorter: no more than 5 seconds.

If an Archiver role (A) is configured with a secondary and tertiary server, and the secondary server is shared with another Archiver role (B) which has higher archiving priority, then if both primary Archiver servers fail at the same time, the secondary server starts archiving for the highest priority Archiver role (B). However, this configuration prevents Archiver role (A) from archiving on the secondary or tertiary servers.

BEST PRACTICE: If you have a tertiary server configuration for Archiver failover, do not share the secondary server if the Archiver role does not have the highest archiving priority. If you must share a standby server, share the tertiary one.

Related Topics

Creating Auxiliary Archiver roles on page 590

About video archives on page 661

Setting up Archiver failover

You can set up the Archiver role to fail over to a secondary server if the primary server fails, and to a tertiary server if both the primary and secondary servers fail. With this setup, you can maintain control of the video units, access live video, and minimize potential downtime.

Before you begin

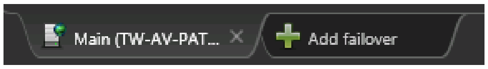
A license is required to assign a tertiary server for Archiver role failover. See License options in Security Center on page 1447 for more details.

What you should know

The servers assigned to the Archiver must be configured separately, and must have their own database and storage system for the video archive.

To set up Archiver role failover:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select an Archiver role, click the **Resources** tab, and then click **Add failover** (✚).

3. In the dialog box that opens, select a server and click **Add**.

   The server you added for failover becomes the secondary server tab.
4. From the secondary server tab, configure archive database and archive storage settings.
5. (Optional) If the secondary server is also on standby for other Archiver roles, then you might have to adjust the archiving priorities for standby servers.
6. (Optional) Add a tertiary server in case both the primary and secondary servers fail:
   a) Click the **Add failover** tab.
   b) Select a tertiary server and click **Add**.

      The server you added for failover becomes the tertiary server tab.
   c) From the tertiary server tab, configure archive database and archive storage settings.
   d) (Optional) If the tertiary server is also on standby for other Archiver roles, then you might have to adjust the archiving priorities for standby servers.
7. Click **Apply**.
8. To have the primary and standby servers archive video at the same time, click the **Camera default settings** tab, click **Show advanced settings**, and switch the **Redundant archiving** option to **ON**.

   This ensures that the recorded video and audio are stored in three places, for additional protection.

Related Topics

Archiver failover on page 191

Databases on page 134

About video archives on page 661

Changing the server priority for Archiver failover

You can decide which Archiver is the primary server, which one is the secondary, and which one is the tertiary server for failover.

Before you begin

You must have at least two servers assigned to the Archiver role.

What you should know

You can configure different archiving and retention settings for each server assigned to the Archiver role. When you change failover order, the settings follow the server.

CAUTION: To avoid losing video, change the server priority for Archiver failover when the Archiver is not archiving.

To change the server priority for Archiver failover:

1 Click **Failover** () at the bottom of the **Resources** tab.

A dialog box opens, showing the servers assigned to this Archiver role.

2 To move a server up or down the list, select it and click ▲ or ▼.

3 Click **OK**.

The *Failover* dialog box closes and the server tabs switch places.

4 When a standby server hosts other Archiver role, you might have to adjust the archiving priorities for the standby server.

5 Click **Apply**.

Assigning archiving priorities for standby servers

If all the Archiver roles fail over to the same standby server at the same time, you can assign archiving priorities to the roles to avoid overloading the server.

What you should know

One server can be designated as the standby server for multiple Archiver roles. If all Archiver roles fail over to the same server at the same time, their combined load might be too much for the server to handle. To avoid overloading a server, you can assign a lower archiving priority to the less important roles so they are not competing for computer resources.

NOTE: At any time on a given server, only the Archiver role with the highest archiving priority is able to archive. The archiving priority only affects archiving. Having a lower archiving priority does not prevent a failed over Archiver role from performing its command and control functions.

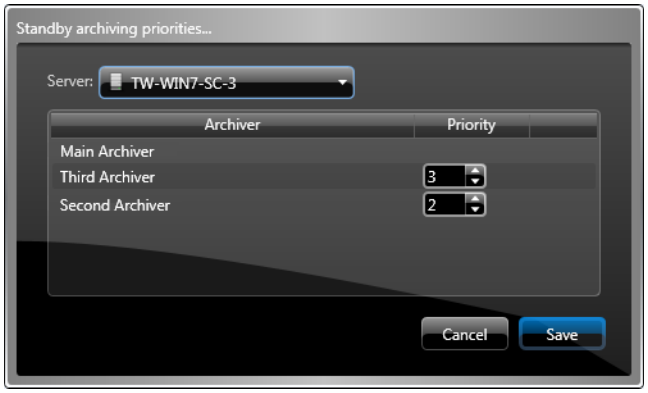
To assign archiving priorities for standby servers:

1 Open the *Video* task, and select the Archiver role to configure.

2 Click the **Resources** tab, and click **Failover** ().

3 In the *Failover* dialog box, click **Standby archiving priorities**.

4 Select a server from the **Server** drop-down list.



Archiver	Priority
Main Archiver	
Third Archiver	3
Second Archiver	2

All Archiver roles that rely on this server as their primary or *secondary server* are listed. The archiving priority can only be set when the server is used as a standby. For roles that rely on the server as their *primary server*, the archiving priority is implicitly locked at 1 (the highest).

5 Set the priority of the roles, and click **Save**.

NOTE: The archiving priority is specific to each Archiver role on each server. When the archiving priority has never been set, its default value is 1.

6 Repeat these steps to configure all servers hosting Archiver roles on your system.

Configuring different retention periods for each Archiver server

To manage your data storage, you can set a different recording retention period or disable archiving for any of the servers assigned to the Archiver role.

Before you begin

Archiver failover must be configured.

What you should know

- Recording settings defined for cameras supersede the settings defined for the Archiver.
- If you disable archiving for a server, recording stops for all the cameras when the role is running on that server,regardless of any recording schedule configurations or custom recording settings. The cameras are used only for live viewing.
- If the secondary or tertiary servers run version 5.11.0.0-5.11.2.0, the custom retention settings apply, but archiving stays enabled by default.
- When setting retention periods, consider the following:
  - For cameras that have more important video footage, set a longer retention period at the camera level.
  - For PTZ cameras, set a shorter retention period because they often use more storage.
  - Reduce the retention periods for additional servers if storage is limited. Ensure that archive consolidation is enabled so that if the primary server fails, any missing video files are copied over when the server restarts.

To configure different recording retention periods for additional servers:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select an Archiver and click the **Camera default setting** tab.
3. In the *Per-server settings* section, turn on the **Custom settings per server** option.

   NOTE: A section appears with tabs for each server assigned to the Archiver role. By default, each server has the same retention setting as the primary server. An option is also available to disable archiving for that server.
4. Click the second tab and configure the settings for the secondary server.
5. If you have a tertiary server, click the third tab and configure its settings.
6. Click **Apply**.

Consolidating video archives after Archiver failover

If your primary Archiver server goes offline and failover occurs, you can later consolidate video archives for the period it was offline. Using the *archive consolidation* feature, you can duplicate the video archives from the secondary or tertiary servers to the primary server.

Before you begin

Archiver failover must be configured.

What you should know

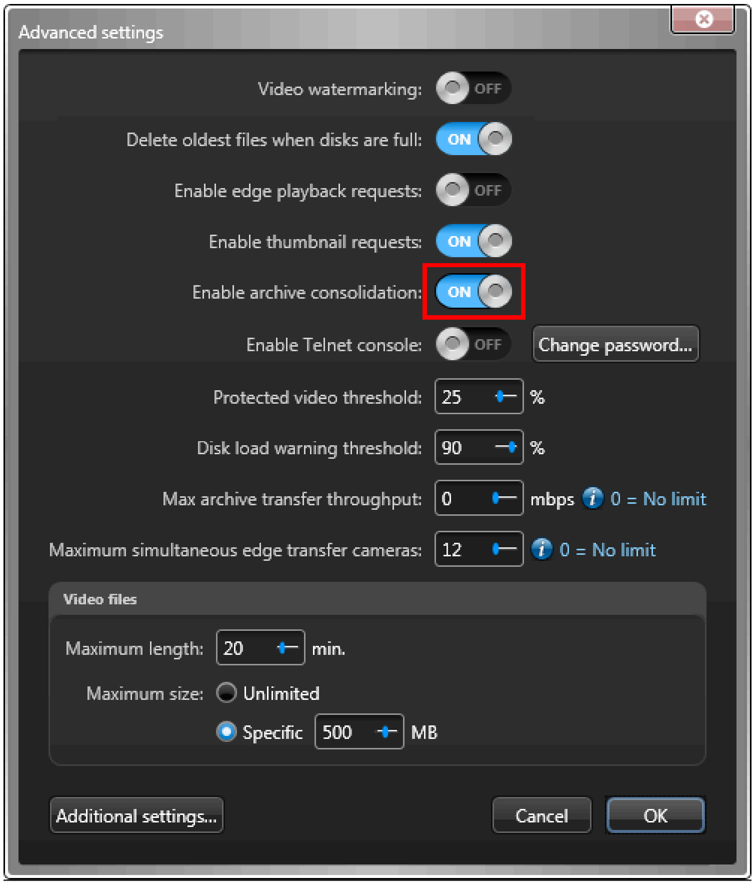
- By default, the primary Archiver server checks every hour for video archives to consolidate from the secondary or tertiary servers. Video archives are consolidated from all cameras controlled by the Archiver.
- If archive consolidation is enabled and you change the primary Archiver server, archives that are missing from the timeline of the new primary server are copied from the secondary and tertiary servers, if the archives are available.
- You can configure different retention periods for each server assigned to the Archiver role. If the retention period of the primary server is shorter than the secondary or tertiary servers, consolidation will only copy over archives that fall within the retention period of the primary server.

To consolidate video archives after an Archiver failover:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Select an Archiver, click the **Resources** tab, and then click **Advanced settings**.

3 In the *Advanced settings* dialog box, switch the **Enable archive consolidation** option to **ON**.



Advanced settings

Video watermarking: OFF

Delete oldest files when disks are full: ON

Enable edge playback requests: OFF

Enable thumbnail requests: ON

Enable archive consolidation: ON

Enable Telnet console: OFF

Protected video threshold: 25 %

Disk load warning threshold: 90 %

Max archive transfer throughput: 0 mbps 0 = No limit

Maximum simultaneous edge transfer cameras: 12 0 = No limit

Video files

Maximum length: 20 min.

Maximum size: ○ Unlimited

● Specific 500 MB

4 Click **OK** > **Apply**.

The archive consolidation feature is enabled, and a *Default consolidation transfer group* is created. If the primary Archiver server fails and restarts, video archives from the additional servers copy over to fill in the gaps every hour, if archives are available.

5 (Optional) To see the *Default consolidation transfer group* and its transfer settings in Config Tool, do the following:

a) Open the *GeneralSettings.gconfig* file that is found in the Security Center installation folder.

The default location is *C:\Program Files (x86)\Genetec Security Center 5.11\ConfigurationFiles* on a 64-bit computer and *C:\Program Files\Genetec Security Center 5.11\ConfigurationFiles* on a 32-bit computer.

b) Add the following line of code:

```
<archiveTransfer ViewArchiveConsolidationTransfer="true" />
```

c) Save the file.

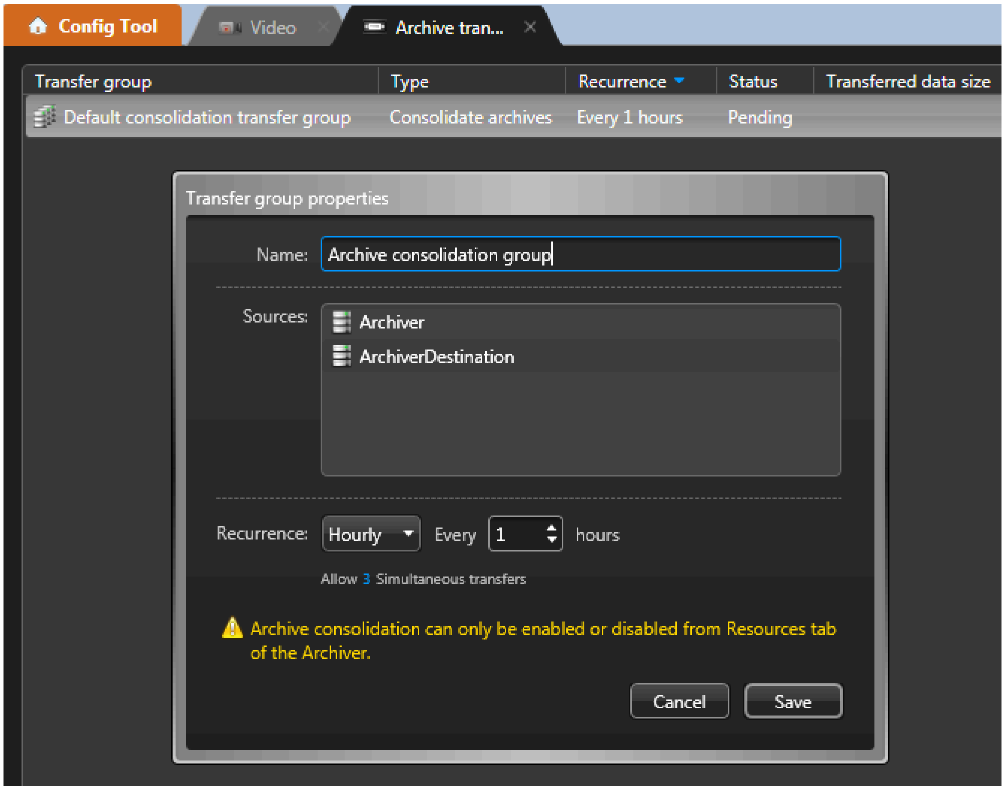
You can now see the *Default consolidation transfer group* from the *Archive transfer* page in the Config Tool *Video* task.

6 (Optional) To change the video transfer settings, do the following:

a) Open the *Video* task and click the **Archive transfer** view.

b) Double-click the **Default consolidation transfer group**.

c) In the *Transfer group properties* dialog box, enter a new name for the group in the **Name** field.



Transfer group	Type	Recurrence	Status	Transferred data size
Default consolidation transfer group	Consolidate archives	Every 1 hours	Pending	

Transfer group properties

Name: Archive consolidation group

Sources: Archiver
ArchiverDestination

Recurrence: Hourly Every 1 hours

Allow 3 Simultaneous transfers

⚠ Archive consolidation can only be enabled or disabled from Resources tab of the Archiver.

d) In the **Recurrence** option, select how often you want the transfer to occur.

e) In the **Allow n Simultaneous transfers** option, select the number of cameras for which to transfer video from simultaneously.

f) Click **Save**.

Related Topics

Transferring video archives on page 668

Troubleshooting failover

If you encounter problems when configuring failover for your system, there are a few things you can check to resolve the issues.

To troubleshoot failover:

1. Make sure the correct ports are open on your network (see Ports used by core applications in Security Center on page 1452).
2. Make sure your database connections are configured properly, and that the servers being used for failover can communicate with the database server (see Connecting roles to remote database servers on page 136).
3. Make sure the database path is correct in the Server Admin - Main Server page.
4. Make sure the Genetec™ Server and SQL Server services are running under a local Windows administrator user account (see Connecting roles to remote database servers on page 136).
5. (Directory database failover using Backup/Restore method only) Make sure that the user account has access read/write access to the backup folder.
6. (Directory database failover using Backup/Restore method only) Make sure that Security Center Server is installed on the remote database server.

   For more information about installing expansion servers, see the *Security Center Installation and Upgrade Guide*.

9

System automation

This section includes the following topics:

About schedules

A schedule is an entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).

Each time constraint is characterized by a date coverage (date pattern or specific dates covered by the schedule) and a time coverage (time periods that apply during a 24-hour day).

When the Security Center Directory is installed, the *Always* schedule is created by default. This schedule has a 24/7 coverage. It cannot be renamed, modified, or deleted, and has the lowest priority in terms of schedule conflict resolution.

Time zones for schedules

By default, the time of day for a schedule is based on the local time zone set in each individual context where it is applied. For example, if the schedule is used to set continuous video recording from 9 am to 5 pm, whether the *video unit* is in Tokyo or London, the recording occurs on schedule according to the local time. This is because every video unit has a time zone setting to control video settings and recordings relative to the unit’s local time.

When a schedule is applied to an entity that has no time zone settings, such as the logon schedule for a user, the local time is taken from the *server* hosting the Directory role.

To use the time zone of the server hosting the source entity, enable the **Use source time** option in the *Event-to-action* configuration window.

NOTE: The **Use source time** option is unavailable for custom events.

Related Topics

Customizing time zone settings on page 61

About twilight schedules

A twilight schedule is a schedule entity that supports both daytime and nighttime coverages. A twilight schedule cannot be used in all situations. Its primary function is to control video related behaviors.

Benefits of twilight schedules

Twilight schedules are designed for situations where the sunlight has an impact on the system’s operation, such as video settings and recording. Some typical uses of the twilight schedules are the following:

- To record video only during daytime.
- To boost the *video encoder*’s sensitivity after sunset.
- To disable *motion detection* during twilight.

Limitations of twilight schedules

Twilight schedules have the following limitations:

- They cannot be used in any situation involving access control entities.
- The entity the schedule applies to must have a geographical location setting, such as video units and *ALPR units*.
- The *Weekly* option for date coverage is not available.

- The *All day* and *Range* options for time coverage are not available.
- They are not visible in contexts where they are not applicable.

Related Topics

Setting geographical locations of entities on page 79

Creating schedules

To define a set of time constraints for a multitude of situations, such as when a user can log on to the system or when video from a surveillance camera can be recorded, you can create schedules and then apply them to specific entities.

What you should know

When the Security Center Directory is installed, the *Always* schedule is created by default. This schedule has a 24/7 coverage. It cannot be renamed, modified, or deleted, and has the lowest priority in terms of schedule conflict resolution.

To use schedules for any of your settings in Security Center, you must create the schedules in advance.

To create a schedule:

1. Open the *System* task and click the **Schedules** view.
2. Click **Schedule** (➕), type a name for the schedule, and press Enter.
3. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply.**
4. Click the **Properties** tab.
5. From the **Date coverage** drop-down list, choose one of the following:
   - **Daily:** Defines a pattern that repeats every day.
   - **Weekly:** Defines a pattern that repeats every week. Each day of the week can have a different time coverage. This option is unavailable for twilight schedules.
   - **Ordinal:** Defines a series of patterns that repeat on a monthly or yearly basis. Each date pattern can have a different time coverage. For example, on July 1st every year, on the first Sunday of every month, or on the last Friday of October every year.
   - **Specific:** Defines a list of specific dates in the future. Each date can have a different time coverage. This option is ideal for special events that occur only once.

   NOTE: The *Daily*, *Ordinal*, and *Specific* schedules allow you to define twilight settings.
6. Click **Apply**.

Defining daily schedules

To define a set of time constraints for situations that occur daily, you can define daily schedules and then apply them to entities.

What you should know

Time ranges are shown as colored blocks on a time grid. Each block represents 30 minutes. When you click and hold your left mouse button, a pop-up window opens. Each block on the grid represents one minute.

To define a daily schedule:

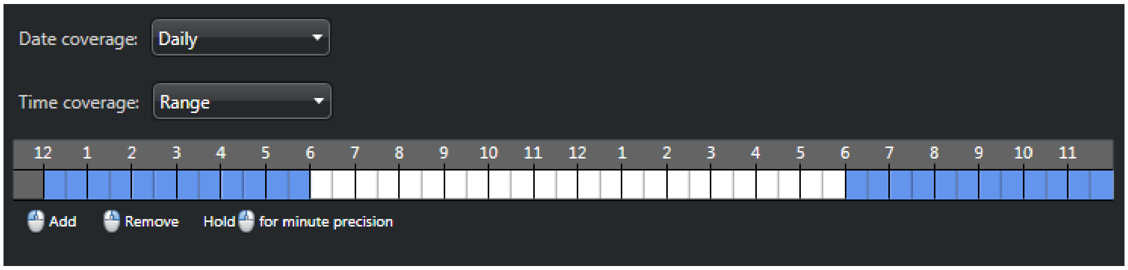
1. Open the *System* task and click the **Schedules** view.
2. Click **Schedule** (➕), type a name for the schedule, and press Enter.
3. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply.**
4. Click the **Properties** tab.
5. From the **Date coverage** list, select **Daily**.
6. From the **Time coverage** drop-down list, select **All day** or **Range**.

7 Using the time grid, set the time coverage as follows:
   - To select blocks of time, left-click your mouse.
   - To remove blocks of time, right-click your mouse.
   - To select or remove a successive block of time, click and drag your mouse.
   - To zoom in on the time grid and select specific minutes, click and hold your left mouse button.

8 Click **Apply**.

Example

The following example shows a daily schedule from 6 pm to 6 am The time grid shows a 24-hour day in blocks of 30 minutes.



Date coverage: Daily

Time coverage: Range

Defining weekly schedules

To define a set of time constraints for situations that occur weekly, you can define weekly schedules and then apply them to entities.

What you should know

Time ranges are shown as colored blocks on a time grid. Each block represents 30 minutes. When you click and hold your left mouse button, a pop-up window opens. Each block on the grid represents one minute.

To define a weekly schedule:

1 Open the *System* task and click the **Schedules** view.

2 Click **Schedule** (➕), type a name for the schedule, and press Enter.

3 In the **Identity** tab, enter basic properties of the schedule, and then click **Apply.**

4 Click the **Properties** tab.

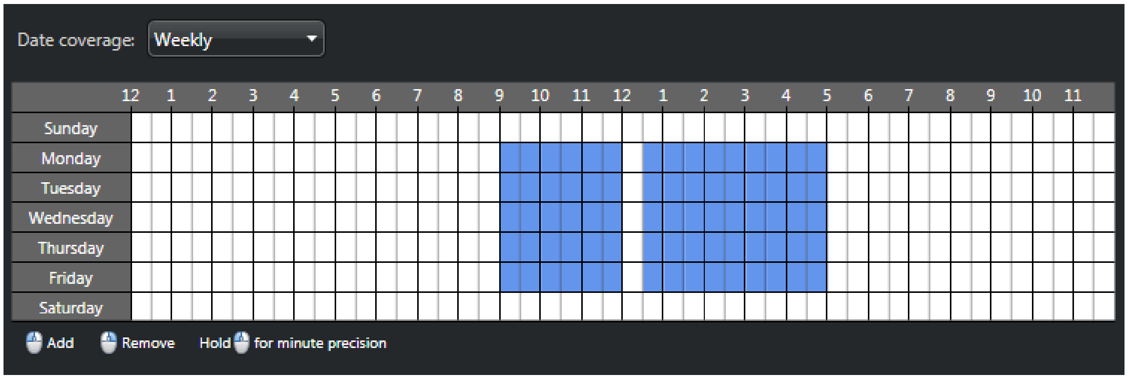
5 From the **Date coverage** list, select **Weekly**.

6 Using the time grid, set the time coverage as follows:
   - To select blocks of time, left-click your mouse.
   - To remove blocks of time, right-click your mouse.
   - To select or remove a successive block of time, click and drag your mouse.
   - To zoom in on the time grid and select specific minutes, click and hold your left mouse button.

7 Click **Apply**.

Example

The following example shows a weekly schedule from 9 am to 5 pm, from Monday to Friday, with a half-hour break between 12:00 pm and 12:30 pm



Date coverage: Weekly

Defining ordinal schedules

To define a set of time constraints for situations that include a series of repetitive patterns, each with a different time coverage, you can define ordinal schedules and then apply them to entities.

What you should know

Ordinal schedules are ideal for events that repeat. You can define as many dates as needed within a single schedule entity.

To define an ordinal schedule:

1 Open the *System* task and click the **Schedules** view.

2 Click **Schedule** (✚), type a name for the schedule, and press Enter.

3 In the **Identity** tab, enter basic properties of the schedule, and then click **Apply.**

4 Click the **Properties** tab.

5 From the **Date coverage** list, select **Ordinal**, and then click **Add an item** (✚).

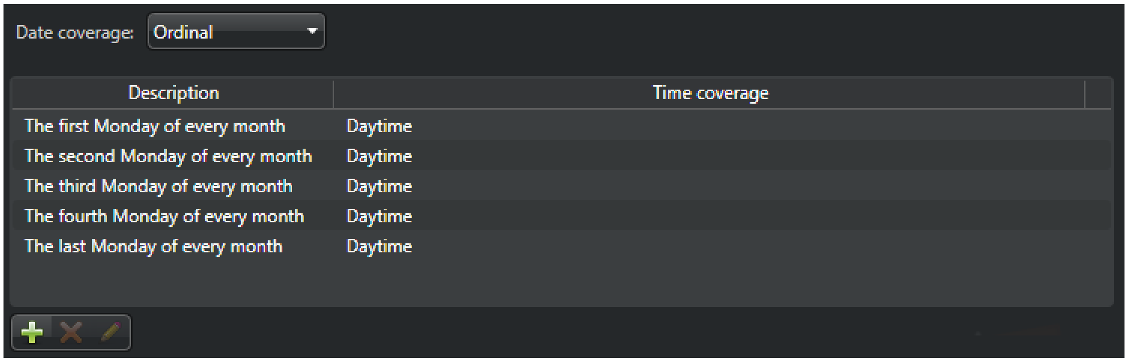
6 Select a day and a month.

7 From the **Time coverage** drop-down list, select **All day**, **Range, Daytime**, or **Nighttime** (see Defining twilight schedules for information on daytime and nighttime time coverages).

8 Click **OK** and then click **Apply**.

Example

You can configure something similar to the *Weekly* pattern using the *Ordinal* pattern. The following example shows a schedule that cover the daytime of every Monday of the year.



Date coverage: Ordinal

Description	Time coverage
The first Monday of every month	Daytime
The second Monday of every month	Daytime
The third Monday of every month	Daytime
The fourth Monday of every month	Daytime
The last Monday of every month	Daytime

Defining schedules with specific dates

To define a set of time constraints for situations that will occur on specific dates, where each date can have a different time coverage, you can define schedules with specific dates and then apply them to entities.

What you should know

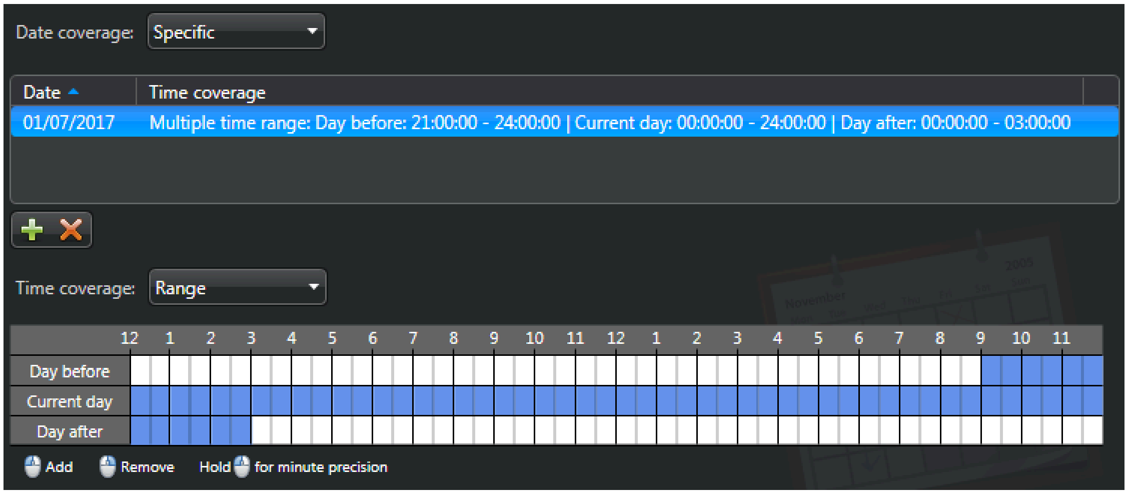
You can set a different time range for each date in the schedule.

To define a schedule with specific dates:

1. Open the *System* task and click the **Schedules** view.
2. Click **Schedule** (+), type a name for the schedule, and press Enter.
3. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply.**
4. Click the **Properties** tab.
5. From the **Date coverage** list, select **Specific**, and then click **Add an item** (+).
6. Select dates on the calendar and click **Close**.
7. Select an entry and, from the **Time coverage** drop-down list, do one of the following:
   - Select **All day**.
   - Select **Range** and then select specific times on the grid for the *Day before*, the *Current day*, or the *Day after*.
   - Select **Daytime** or **Nighttime** (see Defining twilight schedules for information on daytime and nighttime time coverages).
8. Click **Apply**.

Example

The following example shows a specific schedule covering July 1st 2017 from 9 pm the day before to 3 am the day after.



Date coverage: Specific

Date	Time coverage
01/07/2017	Multiple time range: Day before: 21:00:00 - 24:00:00 | Current day: 00:00:00 - 24:00:00 | Day after: 00:00:00 - 03:00:00

Time coverage: Range

	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Day before																						🟦	🟦	🟦
Current day	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Day after	🟦	🟦	🟦																					

Defining twilight schedules

To define a set of time constraints for situations that cover either daytime or nighttime, where the calculation of exactly when the sun rises and sets is based on a geographical location (latitude and longitude), you can define twilight schedules.

What you should know

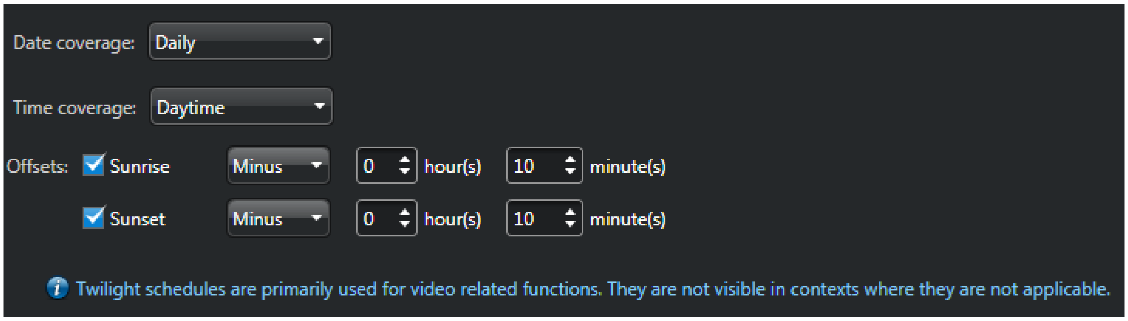
Twilight schedules are designed for situations where the sunlight has an impact on the system's operation, such as with video settings and video recording.

To define a twilight schedule:

1. Open the *System* task and click the **Schedules** view.
2. Click **Schedule** (✚), type a name for the schedule, and press Enter.
3. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply.**
4. Click the **Properties** tab.
5. From the **Date coverage** list, select **Daily**, **Specific**, or **Ordinal**.
6. If you selected **Specific** or **Ordinal**, set up the date coverage.
7. From the **Time coverage** list, select **Daytime** or **Nighttime**.
8. Select the **Sunrise** or **Sunset** options, and then select the amount of time to offset the sunrise time or sunset time (up to 2 hours before or after).

Example

The following example shows a daily schedule using a *Daytime* coverage. The time coverage starts 10 minutes after the sun rises and ends 10 minutes before the sun sets.



Date coverage: Daily

Time coverage: Daytime

Offsets: ☑ Sunrise Minus 0 hour(s) 10 minute(s)

☑ Sunset Minus 0 hour(s) 10 minute(s)

Twilight schedules are primarily used for video related functions. They are not visible in contexts where they are not applicable.

About events

In the context of Security Center, an event indicates the occurrence of an activity or incident, such as access denied to a cardholder or motion detected on a camera. Events are automatically logged in Security Center. Every event has an entity as its main focus, called the event source.

Events can arise from many different sources, such as a user starting a recording on a camera, a door being left open for too long, or an attempt to use a stolen credential. The types of events generated by Security Center vary by the entity. For example, *Access denied* events relate to cardholders, *Signal lost* events relate to cameras, *License plate hit* events relate to hotlists, and so on.

Some ways that you can use events include the following:

- View live events in Security Desk.
- View past events in reporting tasks for analysis and investigation.
- Configure the system to take action automatically by associating actions to various types of events, such as triggering an alarm or sending a message. This is called an *event-to-action*. This is the most powerful method for handling events.

System versus custom events

Security Center is installed with predefined event types called *system events*. You can add new event types to your system, either by installing plugins or by defining them yourself. These are called *custom events*, which you can use in the same way that you use system events.

Live versus offline events

When the event source is a device or an external application, live event and offline events must be differentiated.

- A live event is an event that Security Center receives when the event occurs. Security Center processes live events in real-time. Live events are displayed in the event list in Security Desk and can be used to trigger event-to-actions.
- An offline event is an event that occurs while the event source is offline. Security Center only receives the offline events when the event source is back online.

Depending on how old the event is when it is received, Security Center can be configured to do one of the following:

- Treat it as a live event, typically within a few minutes of the event occurrence.
- Record the event in the database for reporting without sending notifications to online users: suitable for when the event is less than a predefined number of days old.
- Discard the event without saving it to the database: suitable for when the event is more than a predefined number of days old.

Related Topics

Event types on page 1410
Creating event-to-actions on page 212
Creating custom events on page 211

Assigning colors to events

For users to quickly assess and respond to events when they are received in Security Desk, you can assign different colors to Security Center events.

What you should know

Event colors are used as visual cues in the Security Desk. When a *system event* is generated, the event color is indicated in the event list and in the canvas tile.

If you have a large system, this helps you focus on events that are more important. For example, you can use red to indicate a critical event (someone attempted to use a stolen credential), and blue to indicate a less critical event (*Access granted*).

To assign a color to an event:

1 Open the *System* task, click the **General settings** view, and go to the *Events* page.

2 Next to an event in the **Event colors** tab, select a color from the **Color** list.

3 Click **Apply**.

Creating custom events

You can create your own custom Security Center events that you can use for event-to-actions.

What you should know

Custom events allow you to give descriptive names to standard events generated by input signals from zones, intrusion panels, and so on. They are used to configure custom event-to-actions.

For example, you can associate an input state (normal, active, trouble) of a zone entity to a custom event that describes what is happening, such as *Illegal entry* or *Door open too long for this zone*. When this custom event is received in Security Desk, it can trigger an action, using event-to-actions.

To create a custom event:

1. Open the *System* task, click the **General settings** view, and go to the *Events* page.
2. Click **Add an item** (➕).
3. In the **Create custom event** dialog box, type a **Name** for the new event.
4. From the **Entity type** list, select the entity type that triggers this event.
5. In the **Value** field, type a unique number to identify the custom event from other custom events.
   These values are not related to the logical IDs of entities.
6. Click **Save** > **Apply**.

Creating event-to-actions

If you want certain events that occur in your system to automatically trigger an action, such as sounding an alarm or recording a camera, you can create event-to-actions.

What you should know

An event-to-action links an *action* to a particular *event*. For example, you can configure Security Center to trigger an alarm when a door is forced open.

To create an event-to-action:

1. Open the *System* task, and click the **General settings** view.
2. Go to the *Actions* page.
3. (Optional) From the **Domain** list, select a subject domain.

   Selecting a domain limits the configured actions displayed on this page to the ones associated to an event in that domain. The same filter also applies to all subsequent event selection drop-down lists.

   You can select the following domains:

   - All
   - Access control
   - ALPR
   - Intrusion detection
   - Video

4. Click **Add an item** (✚).
5. From the **When** list in the *Event-to-action* dialog box, select an event type.
   a) (Optional: ALPR only) If you select **License plate read**, you can specify a condition for LicensePlateRead events.
   b) (Optional: Custom events only) If you select a custom event, you can specify a text string in the **and** field, which must be included in the macro that triggers the event-to-action.
6. In the **From** option, click **Any entity**, and then select an entity that triggers the event.

   By default, the event-to-action occurs when any entity triggers the event type you select. If you select a specific entity, you might have to set other parameters. For example, if you select a door, you must also select a door side.
7. From the **Action** list, select an action type and configure its parameters.

   For example, if you select the *Send an email* action, you can create an email template message that can include fields that are related to the report or event. In this case, using the {CardholderName} field, you could create the message: *Unauthorized access attempt by {CardholderName}*.
8. In the **Effective** option, click **Always**, and select a schedule when this event-to-action is active.

   If the event occurs outside of the defined schedule, the action is not triggered. For example, you might want to sound an alarm only when a window is opened during the weekend. By default, **Always** is selected.
9. (Optional) Enable the **Use source time zone** option to configure the schedule's start and end using the time zone of the source entity's server.

   NOTE: This option is only available for cameras, video units, access control units, and doors.
10. Click **Save**.

    The **Save** button is only available when all the arguments required by the event-to-action type are specified.

The new event-to-action is added to the list of system actions.

Related Topics

Event types on page 1410
Action types on page 1434
Setting up alarms using event-to-actions on page 1183

Adding conditions when creating event-to-actions for license plate reads

When creating event-to-actions for license plate reads, you can specify additional conditions based on Sharp analytics to trigger an action. For example, you can specify that an action occur only when the plate number contains “123”, or the vehicle is traveling at a certain speed.

Before you begin

Enable and configure analytics for your Sharps. For more information, see the administrator guide for your Sharp camera and the *Genetec Patroller™ Administrator Guide.*

What you should know

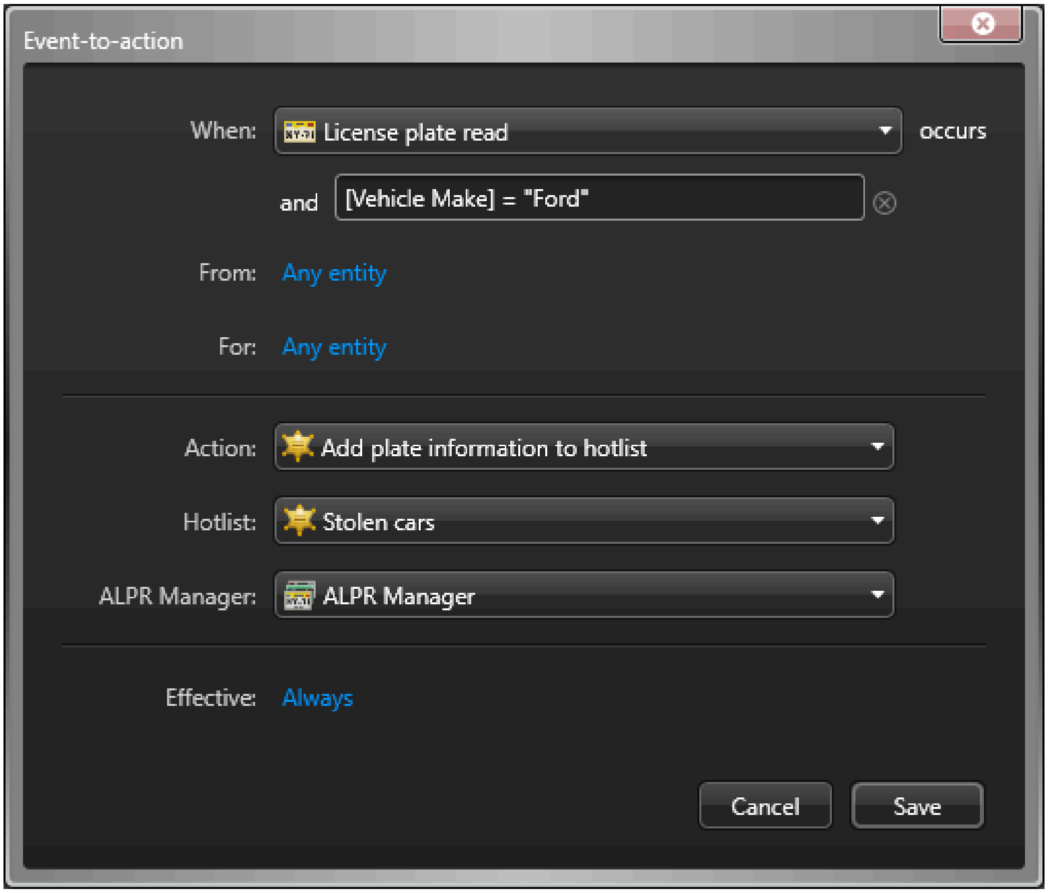
- Conditions must be typed as an expression that contains an identifier, operator, and a value (not case sensitive). For example, [PlateNumber] = "ABC123". To know more about the operators and identifiers that can be used, see Elements used in event-to-action conditions for license plate reads on page 216.
- Identifiers must be typed in square brackets: [PlateNumber].
- Text values must be typed in quotation marks: "ABC123".
- You can use AND and OR to combine multiple expressions. When doing this, it's preferable to use parentheses to force the order of the evaluation. For example, if you type ([Speed] > 20 AND [Speed.unit] = "mph") OR ([Speed] > 50 AND [Speed.Unit] = "km/h") the AND operator takes precedence.
- You can use the exclamation point (!) to exclude an expression. For example, if you type [PlateNumber] contains "123" AND !([PlateState] = "QC"), any plate reads with a plate number that contains the value "123" and a plate state other than "QC" will trigger an action.
- Sharp analytics are not generated 100% of the time. An event-to-action might not be executed if the Sharp is not able to generate the analytic specified in the condition. For example, if the condition is **[Speed] > 50** and the Sharp cannot produce a value for speed, Security Center will evaluate the condition as being false and the action will not be executed.
- When the outputs of an SharpZ3 base unit are used to control building access through event-to-actions in Security Center, rebooting the base unit causes the outputs to activate which could lead to the opening of the access point. This output behavior is not ideal for access control, but is required in order to power the in-vehicle computer on vehicle startup. Create an event-to-action in Security Center that will send a "Normal" state to the outputs following a "Unit Connected" event. The access points will still open, but will close shortly afterward.

To add a condition when creating an event-to-action for a license plate read:

1. Open the *System* task, and click the **General settings** view.
2. Go to the *Actions* page.
3. From the **Domain** list, select **ALPR**.
4. Click **Add an item** (➕).
5. From the **When** list in the *Event-to-action* dialog box, select **License plate read**.
6. Click **Specify a condition**, and type the expression.

   TIP: Hover your mouse over the field for examples of valid expressions. The field will appear in red if the expression you enter is invalid.
7. In the **From** list, select the ALPR unit that triggers the event.
8. In the **For** list, select the desired entity.

9 From the **Action** list, select an action type and configure its parameters.
Example: If you select *Add plate information to the hotlist*, you must also select the required hotlist.



Event-to-action

When: License plate read occurs

and [Vehicle Make] = "Ford"

From: Any entity

For: Any entity

Action: Add plate information to hotlist

Hotlist: Stolen cars

ALPR Manager: ALPR Manager

Effective: Always

10 In the **Effective** option, click **Always**, and select a schedule when this event-to-action is active.
If the event occurs outside of the defined schedule, the action is not triggered.

11 Click **Save**.
The **Save** button is only available when all the arguments required by the event-to-action type are specified.

Elements used in event-to-action conditions for license plate reads

If you add a condition when creating an event-to-action for a license plate read, the condition must contain an identifier, an operator, and a value (text or numeric).

Operators

The following table lists operators that can be used and the corresponding value types, as well as descriptions and examples.

Operator	Description	Type of value	Example
>	Greater than the specified value.	Numeric	[Confidence Score] > 80
<	Less than the specified value.	Numeric	[Confidence Score] < 75
=	Equal to the specified value.	Numeric	[Confidence Score] = 80
		Text	[Vehicle Make] = "Toyota"
contains	Contains the specified value.	Text	[PlateNumber] contains "123"
startsWith	Starts with the specified value.	Text	[PlateNumber] startsWith "X"
endsWith	Ends with the specified value.	Text	[State Name] endsWith "C"
matches	Respects the regular expression.	Text	[PlateNumber] matches "[02468]$"

Identifiers

The following table lists the common identifiers that can be used and the corresponding value type, as well as descriptions and examples.

Identifier	Description	Type of value	Example
PlateNumber	Plate Number read by the Sharp.	Numeric	[PlateNumber] contains "123"
State Name	State Name read by the Sharp.	Text	[State Name] = "QC"
Vehicle Type	Certain license plates include character symbols that identify specific vehicle types (for example, taxi, transport, and so on). The Sharp can read these symbols, and display the vehicle type.	Text	[Vehicle Type] = "Taxi"
Relative Motion	The Sharp can detect if the vehicle is getting closer or moving away from the Sharp.	Text	[Relative Motion] = "Approaching"

Identifier	Description	Type of value	Example
Context	Type of ALPR context for a specific region.	Text	[Context] = "Brazil"
Characters Height	Height in pixels of the context characters.	Numeric	[Characters Height] = 26
Vehicle Make	Sharp cameras can recognize the make of certain vehicles.	Text	[Vehicle Make] = "Toyota"
Confidence Score	The Sharp assigns a numerical value (from 0 to 100) to each license plate read. This value shows the accuracy level of the read.	Numeric	[Confidence Score] = 80
Speed	Sharp cameras are able to estimate a vehicle’s approximate speed.	Numeric	[Speed] > 50
Speed.Unit	Depending on the Sharp context used, the unit of speed is measured in *km/h* or *mph*. For the US context speed is measured in *mph*.	Text	[Speed.Unit] = "mph"
Prefix	Leftmost and topmost digits on a United Arab Emirates plate.	Text	[Prefix] = 10

For more information about specifying conditions when creating event-to-actions for license plate reads, see Adding conditions when creating event-to-actions for license plate reads on page 214

Modifying event-to-actions

If you need to modify an event-to-action, but you have a long list of them in Security Center, you can search for them using a combination of source entity (name and type), event type, and action type.

To modify an event-to-action:

1 Open the *System* task, and click the **General settings** view.

2 Go to the *Actions* page.

3 (Optional) From the **Domain** list, select a subject domain.

Selecting a domain limits the configured actions displayed on this page to the ones associated to an event in that domain. The same filter also applies to all subsequent event selection drop-down lists.

You can select the following domains:

- All
- Access control
- ALPR
- Intrusion detection
- Video

4 Click **Advanced search** (⊕) to show the search filters, and filter out the event-to-actions as follows:

- **Entity name:** Search for source entity names starting with the search string.
- **Entity type:** Select a specific source entity type (default=All).
- **Event:** Select a specific event type (default=All).
- **Action:** Select a specific action type (default=All).

5 Select an event-to-action, and click **Edit the item** (✎).

6 From the **When** list in the *Event-to-action* dialog box, select an event type.

a) (Optional: ALPR only) If you select **License plate read**, you can specify a condition for LicensePlateRead events.

b) (Optional: Custom events only) If you select a custom event, you can specify a text string in the **and** field, which must be included in the macro that triggers the event-to-action.

7 In the **From** option, click **Any entity**, and then select an entity that triggers the event.

By default, the event-to-action occurs when any entity triggers the event type you select. If you select a specific entity, you might have to set other parameters. For example, if you select a door, you must also select a door side.

8 From the **Action** list, select an action type and configure its parameters.

For example, if you select the *Send an email* action, you can create an email template message that can include fields that are related to the report or event. In this case, using the {CardholderName} field, you could create the message: *Unauthorized access attempt by {CardholderName}*.

9 In the **Effective** option, click **Always**, and select a schedule when this event-to-action is active.

If the event occurs outside of the defined schedule, the action is not triggered. For example, you might want to sound an alarm only when a window is opened during the weekend. By default, **Always** is selected.

10 (Optional) Enable the **Use source time zone** option to configure the schedule's start and end using the time zone of the source entity's server.

NOTE: This option is only available for cameras, video units, access control units, and doors.

11 Click **Save**.

The **Save** button is only available when all the arguments required by the event-to-action type are specified.

12 To delete an event-to-action, select the item, and click **Delete** (✖).

13 Click **Apply**.

Scheduled tasks

A scheduled task is an entity that defines an action that executes automatically on a specific date and time, or according to a recurring schedule.

Similarities between scheduled tasks and event-to-actions

The similarities are:

- Both have access to the same set of actions.
- Both can trigger more than once.

Differences between scheduled tasks and event-to-actions

The differences are:

- Scheduled tasks are saved as *entities*, event-to-actions are not.
- Scheduled tasks are triggered at specific times, event-to-actions are triggered by events.
- Scheduled tasks are turned on an off manually, event-to-actions are active on a specific schedule.
- The recurrence is different. Unlike event-to-actions, tasks can be scheduled as follows:
  - Once
  - Every minute
  - Hourly
  - Daily
  - Weekly
  - Monthly
  - Yearly
  - On startup
  - Custom interval

Scheduling a task

You can configure an action to execute automatically on system startup or according to a schedule by creating a scheduled task.

To set up an action to trigger on a schedule:

1. From the Config Tool home page, open **System** > **Scheduled tasks**.
2. Click **Scheduled task** (➕).

   A new scheduled task is added to the entity list.
3. Enter a name for the new scheduled task.
4. Click the **Properties** tab for the scheduled task, and switch **Status** to **Active**.
5. For **Recurrence**, select how often you want the task to run:
   - **Once:** Executed once at a specific date and time.
   - **Every minute:** Executed every minute.
   - **Hourly:** Executed at a specific minute of every hour.
   - **Daily:** Executed at a specific time every day.
   - **Weekly:** Executed at a specific time on one or more days of the week
   - **Monthly:** Executed at a specific time on the same day every month.

     CAUTION: Tasks scheduled on day 29, 30, or 31 are not run in shorter months that do not include the selected day.
   - **Yearly:** Executed at a specific time on the same day every year.
   - **On startup:** Executed on system startup.
   - **Interval:** Executed at regular intervals that can be days, hours, minutes, or seconds.

   NOTE: Tasks are skipped if they cannot be executed at the scheduled time because the main server is offline, an entity is unavailable, and so on.
6. Select an **Action** to execute.
7. If required, configure the selected action.

   For example, if you select *Synchronize role*, you must select a role to synchronize.
8. Click **Apply**.

Related Topics

Action types on page 1434

Adding audio files

You can add new audio files that can be played when users receive an alarm in Security Desk, or used with the *Play a sound* action.

What you should know

Security Center supports .mid, .rmi, .midi, .wav, .snd, .au, .aif, .aifc, .aiff, .mp3, and .ogg file types.

As a best practice, do not add audio files that are larger than 100 KB.

To add an audio file:

1 Open the *System* task, click the **General settings** view, and go to the *Audio* page.

2 Click **Add an item** (➕).

3 In the Windows browser, select an audio file, and click **Open**.

The audio file is added to the list.

4 To change the name of the audio file, click **Edit the item** (✏), type a name, and click **OK**.

5 To listen to the audio file, click **Play** (▶).

6 Click **Apply**.

About macros

A macro is an entity that encapsulates a C# program that adds custom functionalities to Security Center.

Macros can be executed either manually or automatically. When automated, it is loaded as a background process and executes when a set of conditions are met.

You create macros by writing a program in C# using Security Center *SDK*, and then loading the program into Security Center. If you need help developing custom macros, contact Genetec™ Professional Services through your sales representative for a quote, or call us at one of our regional offices around the world. To contact us, visit our website at www.genetec.com.

Macro execution context

You can provide input parameters to your macro by declaring mutators. Such mutators must be public. Their type must be one of the following:

- System.Boolean
- System.String
- System.Int32
- System.Guid

By declaring mutators, your macro will have an execution context that can be configured in the *Default execution context* tab. If a macro is run without specifying an execution context, the default execution context is used. This is always the case when a macro is launched from the toolbar at the bottom of Config Tool.

The default execution context can be overridden by specifying your own context.

Creating macros

To create a macro that you can run in Security Center, you must write a C# program using an external text editor or the text editor in Config Tool, and then load the program in Security Center.

What you should know

Security Center prevents a macro that has errors from being saved. If a macro has errors, and you change tabs, it is rolled back to its last error free version.

To create a macro:

1. From the Config Tool home page, open the *System* task, and click the **Macros** view.
2. Click **Macro** (➕), and enter the macro name.
3. Click the **Properties** tab, and do one of the following:
   - To import the source code from a file, click **Import from file**, select the file containing the C# code, and then click **Open**.
   - Write your own program in the **Properties** tab.
4. Click **Apply**.
5. If you added input parameters to the program, click the **Default execution context** tab, and configure the settings.
6. Click **Apply**.

10

Unit management

This section includes the following topics:

About the Unit enrollment tool

Unit enrollment is a tool that you can use to discover IP units (video and access control) connected to your network, based on their manufacturer and network properties (discovery port, IP address range, password, and so on). After you discovered a unit, you can add it to your system.

- The Unit enrollment tool opens automatically after the *Security Center installer assistant* unless you cleared the **Open the unit enrollment tool after the wizard** option.
- When adding access control units, only HID and Synergis™ units can be enrolled with Unit enrollment tool. For complete details on how to enroll Synergis units, see the *Synergis™ Appliance Configuration Guide*.

Configuring unit enrollment settings

You can use the **Settings and manufacturers** button in the Unit enrollment tool to specify which manufacturers to include when searching for new units. You can also configure the discovery settings for units, and specify username and passwords for units so they can be enrolled easily.

To configure your discovery settings:

1 From the homepage, click **Tools** > **Unit enrollment**.

2 In the *Unit enrollment* dialog box, click **Settings and manufacturers** (⚙).

3 Configure the following options:

- **Always run extensive search**. Turn this on if you want all units on the system to be discovered.

  NOTE: Units from other manufacturers may also be discovered because UPnP and *Zero config* are also used in the discovery process.

- **Refuse basic authentication** (video units only). Use this switch to enable or disable basic authentication. This is useful if you turned off basic authentication in the Security Center InstallShield, but you need to turn it back on to perform a firmware upgrade, or enroll a camera that only supports basic authentication. To turn basic authentication back on, you must switch the **Refuse basic authentication** option to **Off**.

  NOTE: This option is only available to users with Administrator privileges.

4 Click **Add manufacturer** (➕) to add a manufacturer to the list of units that will be discovered.

To delete a manufacturer from the list, select it and click ✖.

5 Configure the individual settings for any manufacturers you added. To do this, select the manufacturer and click ✎.

IMPORTANT: You must enter the correct username and password for the unit to enroll properly.

6 (Optional) Remove units from the list of ignored units (see Removing units from list of ignored units on page 228).

7 Click **Save**.

Discovering units on your network

If you do not know the IP address of the video or access control unit you want to add, you can find the unit on your network using the *Unit enrollment* tool.

Before you begin

If you want to discover an access control unit, read Adding access control unit extensions on page 756.

To discover units:

1 From the homepage, click **Tools** > **Unit enrollment**.
2 Configure your unit enrollment settings.
3 Click **Save** > **Start discovery** (🔭).

The units discovered on your network are listed, using the enrollment settings you configured for each manufacturer. You can stop the discovery process at any time.

Adding units

Once new units have been discovered, you can use the Unit enrollment tool to add them to your system.

To add a unit:

1 From the homepage, click **Tools** > **Unit enrollment**.
2 There are three ways to add newly discovered units:

- Add all the new discovered units at the same time by clicking the **Add all** (➕) button at the lower right side of the dialog box.
- Click a single unit in the list, then click **Add** in the **Status** column
- Right-click a single unit from the list and click **Add or Add Unit**.

When a video unit does not have the correct username and password, the **Status** for the unit will be listed as **Bad logon** and you will be prompted to enter the correct information when you add the unit. If you want to use the same username and password for all the cameras on your system, select the **Save as default authentication for all manufacturers** option.

You can also add a unit manually, by clicking the **Manual add** button at the bottom of the *Unit enrollment tool* dialog box.

NOTE:

- For video units, if the added camera is an encoder with multiple streams available, each stream is added with the *Camera - n* string appended to the camera name, *n* representing the stream number. For an IP camera with only one stream available, the camera name is not modified.
- If you are adding a SharpV, by default, the camera units include a self-signed certificate that uses the common name of the SharpV (for example, SharpV12345). To add the SharpV to the Archiver, you must generate a new certificate (signed or self-signed) that uses the camera's IP address instead of the common name. For more information on encrypting the connection to the SharpV Portal using a self-signed certificate, see the *AutoVu™ Handbook for SharpV Fixed Installation*s.

Related Topics

Adding video units manually on page 572

Adding HID access control units on page 769

Clearing added units

You can clear units that have already been added to your system so they are not displayed every time you use the Unit enrollment tool to discover units on your system.

What you should know

The **Clear completed** option in the Unit enrollment tool is permanent, it cannot be reversed.

To clear added units:

1 Add the desired discovered units to your system, see Adding units on page 227.

2 Once the units have been added, click **Clear completed**.

Any unit that has **Added** displayed in the **Status** column will be cleared from the list of discovered units.

Ignoring units

You can choose to ignore units so they don't appear in the list of discovered units of the Unit enrollment tool.

To ignore a unit:

1 From the homepage, click **Tools** > **Unit enrollment**.

The Unit enrollment tool opens with the list of units that have been discovered on the system.

2 Right-click the unit you want to ignore, and select **Ignore**.

The unit is removed from the list and will be ignored when the Unit enrollment tool discovers new units. For information about removing a unit from the list of ignored units, see Removing units from list of ignored units on page 228.

Removing units from list of ignored units

You can remove a unit from the list of ignored units so it's not ignored when a discovery is performed by the Unit enrollment tool.

To remove a unit from the list of ignored units:

1 From the homepage, click **Tools** > **Unit enrollment**.

2 In the upper right corner of the *Unit enrollment* dialog box, click **Settings and Manufacturers** (⚙).

3 Click **Ignored units** and click **Remove all ignored units**, or you can select a single unit and click the **Remove ignored unit** button (✖).

Viewing unit properties

You view at a glance, the list of local and federated units that are part of your system with the *Hardware inventory* report. You can see the unit type, manufacturer, model, IP address, password strength, certificate status, and so on.

What you should know

As an example, you can use the *Hardware inventory* report to see what firmware version a unit has, and determine if it should be upgraded.

NOTE: The *Hardware inventory* report shows information about local and federated units. However, certain functions such as the action commands at the bottom of the screen, the properties *Password*, *Proposed firmware version*, *Proposed firmware description*, and all certificate-related information are not available for federated units. To view federated units in the *Hardware Inventory* task, the **Forward Directory reports** option must be turned ON (default=OFF).

To view the properties of units in your system:

1 From the homepage, open the *Hardware inventory* task.

2 Set up the query filter for your report. Choose one or more of the following filters:

- **Units:** Select individual units or roles to investigate. Selecting a role is equivalent to selecting all units managed by that role.
- **Source group:** Select the category of units (Access control, ALPR, Intrusion detection, or Video).
- **IP address:** Enter the IP address of the unit.

  NOTE: Asterisks (*) can be used as wildcards to replace the following:

  - For IPv4: an entire octet (192.*.1.258), digits within an octet (192.16*.1.25*), or the end of an address (192.*).
  - For IPv6: an entire segment (2001:0db8::*), hexadecimal digits within a segment (2001:0db8::*234), or the end of an address (2001:*).
- **Advanced search:** Select whether to show controllers, expanders, locksets, readers, or a combination thereof.
- **Custom fields:** Restrict the search to a predefined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.

3 Click **Generate report**.

The unit properties are listed in the report pane.

Report pane columns for the Hardware inventory task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the *Hardware inventory* task.

- **Unit:** Name of the unit.
- **Unit type:** Type of unit (Access control, ALPR, Intrusion detection, or Video).
- **Manufacturer:** Manufacturer of the unit.
- **Product type:** Model of the unit.
- **Role:** Role that manages the unit.
- **Firmware version:** Firmware version installed on the unit.
- **IP address:** IP address of the unit or computer.

  NOTE: The IP address is not shown for units enrolled with the hostname and units that belong to an ACaaS system.

- **Physical address:** The MAC address of the equipment's network interface.
- **Time zone:** Time zone of the unit.
- **User:** The user name used to connect to the unit.
- **Password strength:** Strength of the password on the unit. When you hover over the password strength value, a tooltip gives you more information. "Unknown" is shown for federated units. Intrusion detection units are not supported by this feature.
- **Authentication scheme:** Indicates the type of authentication being used by the camera unit, such as basic, digest, anonymous, or third party. If the unit suddenly requests to connect using a less secure authentication scheme, the Archiver rejects communication and the camera goes offline. For example, the Archiver expects the camera to be using digest authentication, but the camera tries to connect using basic authentication. The connection is rejected and the camera goes offline.
- **Security protocol:** The security protocol used by the Access Manager (TLS, Wiegand).
- **Upgrade status:** Status of the firmware upgrade (None, Scheduled, Started, Completed, or Failed).
- **Next upgrade:** The date for the next upgrade based on the units' **Delay upgrade until** setting.
- **Reason for upgrade failure:** Reason that the firmware upgrade failed (for example, Unit offline, or Firmware upgrade path not respected).
- **Proposed firmware version:** The recommended version required for the upgrade. This column is blank for federated units.
- **Proposed firmware description:** The description of the required upgrade. This column is blank for federated units.
  - **Up to date:** No firmware upgrade is necessary.
  - **Optional:** The firmware upgrade is not urgent.
  - **Recommended:** The firmware upgrade is recommended.
  - **Security vulnerability:** The firmware upgrade fixes a security vulnerability issue and is highly recommended.

  NOTE: This information is only available if Genetec Update Service is running.
- **State:** State of the unit (Online, Offline, Warning).
- **Platform version:** Current platform (cumulative security rollup) version installed on the unit.
- **Proposed platform version:** The recommended version required for the upgrade. This column is blank for federated units.
- **Proposed platform description:** The description of the required upgrade. This column is blank for federated units.
  - **Up to date:** No platform upgrade is necessary.
  - **Optional:** The platform upgrade is not urgent.
  - **Recommended:** The platform upgrade is recommended.
  - **Security vulnerability:** The platform upgrade fixes a security vulnerability issue and is highly recommended.

  NOTE: This information is only available if Genetec Update Service is running.
- **Password:** Password shown as a series of '*'.

  If you have the *View/export unit passwords* privilege, click 👁 to show the password.

  Right click the **Password** column to copy your password to the clipboard.
- **Last successful password update:** Time of the last password update.
- **Certificate expiration:** Certificate expiration date. The date is shown only if the certificate is managed by the system. To view the certificate details in a separate window, select the unit and click **View certificate** (📜) at the bottom of the screen.
- **Certificate status:** Certificate management status of the unit.

  - **Managed:** The certificate is managed by the system and is valid.
  - **Expired:** The certificate is managed by the system but has expired.
  - **Unmanaged:** The certificate is not managed by the system but can be. To enroll the unit for certificate management, select the unit and click **Update certificate** (📜) at the bottom of the screen.
  - **Unsupported:** The certificate cannot be managed by the system. The reason might be that the unit model or extension does not support this feature, or that the unit firmware is not up to date.
- **Last certificate update result:** Success or failure of the last certificate update carried out by the system.
- **Last password change result:** Indicates whether or not the password change was successful.
- **Parent:** The direct parent of the interface module or downstream panels. If the direct parent is the access control unit, only the Parent unit column is filled.
- **Parent unit:** The parent access control unit.
- **Secure mode:** (HID units only) Indicates whether secure mode is enabled or disabled.
- **Custom fields:** Predefined custom fields for the entity. The columns only appear if custom fields are defined for the entity and were made visible to you when they were created or last configured.

Undoing the "Never ask me again" option for renaming hardware units

When renaming a hardware unit, users receive the following message: Do you want to rename the related devices?. If you select the **Never ask me again** option, you can undo the setting at a later time from the *Options* dialog box.

What you should know

This setting is saved as part of your user profile.

To undo the "Never ask me again" option for renaming hardware units:

1. From the homepage, click **Options** > **User interaction**.
2. In the **Administration tasks** section, select how Config Tool behaves when you rename a unit from the **Rename all the devices inside the unit** drop-down list:
   - **Ask user:** Ask you before renaming all the devices related to the unit.
   - **Yes:** Rename all related devices without asking you.
   - **No:** Never rename the related devices.
3. Click **Save**.

About the Unit Assistant role

The Unit Assistant is the central role that manages system-wide security operations, such as updating unit passwords and renewing unit certificates, on supported access control and video units.

- The Unit Assistant role manages two types of system-wide operations:
  - Certificate management (requires the Certificate Signing plugin)
  - Password management
- The Unit Assistant role is created by default.
- Unit Assistant features are not supported through Federation™.

Related Topics

Unit certificate management on page 234
Unit password management on page 251
Unit Assistant - Properties tab on page 1385
Unit Assistant - Certificate profile tab on page 1387
About the Unit Assistant role on page 233

Unit certificate management

Unit certificate management is the feature that you need when you wish to deploy trusted certificates on your units from a central location. The Unit Assistant role is responsible for managing the certificates and requires the Certificate Signing role to be its certificate authority (CA).

With the Unit Assistant role, you can configure Security Center to install trusted *identity certificates* on your access control and video units, and automatically renew them when they are about to expire.

To deploy certificates, the Unit Assistant role does two things:

- Install the *certificate authority (CA)*'s root certificate on the servers hosting the Archiver and the Access Manager roles. This ensures that these servers trust the certificates signed by this CA.

  NOTE: The job of the CA is handled by the Certificate Signing *plugin role*. The plugin package is installed by default when you install Security Center, but the plugin role is not created by default. You must create the plugin role if you want to enable unit certificate management in your system.
- Install certificates signed by the trusted CA on selected access control and video units to encrypt communications between Security Center and the units.

  NOTE: It is the role that connects to the units. In this context, the role is the client and the units are the servers. For this reason, the certificates installed on the units are called *server certificates*.

After a certificate is successfully installed on a unit, the unit automatically switches from HTTP to HTTPS by default, and from RTSP to RTSPS if the unit supports it. From that point on, the system manages the unit certificate.

You can perform all certificate deployment operations through the *Hardware inventory* task and scheduled tasks. You need special privileges to perform these operations.

Supported certificate deployment operations

Operation	Required privileges
Manually install or renew certificates on selected access control and video units with the *Hardware inventory* task. You can renew certificates unit by unit or in batches.	*Update access control unit certificate* *Update video unit certificate*
Automatically renew certificates using the *Renew unit certificates* action through scheduled tasks.	*Update access control unit certificate* *Update video unit certificate* *Modify certificate management settings*
Configure the system settings for certificate management in Config Tool. You can configure the settings such as when to send a notification when a certificate is about to expire and the certificate validity period. You can also change the certificate profile followed by the CA from Config Tool.	*Modify certificate management settings*

Supported access control unit models

The following appliances are supported:

- Cloud Link Roadrunner
- Synergis Cloud Link

- Legacy Synergis Cloud Link running Synergis Softwire 11.2 or later

Supported video unit models

Only certain models of video units support the certificate management feature. You might have to upgrade the unit firmware for this feature to work. For the list of manufacturers that support this feature, see "Manufacturers that support certificate management" in the *Security Center Video Unit Configuration Guide*.

Best practices for unit certificate management

- Monitor unit certificate status and update results with the *Hardware inventory* task.

  You can save the report as a public task and monitor the results in the dashboard. For more information, see "Creating a dashboard" in the *Security Center User Guide*.
- Track certificates updated manually with the *Activity trails* task.

  Only manual certificate renewals are tracked as user activities. Certificates renewed automatically through scheduled tasks are not tracked in the *Activity trails* report.
- Changing a unit certificate causes a short recording interruption, so choose a time of day that minimizes disruption to your operations.
- Make sure you do not change the certificate and the password on the same units at the same time.
- When automatically renewing certificates, do not exceed 100 access control units or 1,000 video units per batch.

Limitation

- The Unit Assistant GUI might become unresponsive for several minutes if one of the components involved in certificate signing (Directory, Unit Assistant, Certificate Signing) fails over to their secondary server while the Unit Assistant is performing a large batch of certificate updates.
- When a certificate generated by Security Center expires, the unit (access control or video) continues to operate normally until the next time it reconnects. The unit might take up to 10 hours to display the expired certificate warning status.
- A supported Synergis™ unit cannot be updated if its current self-signed certificate is generated from the Synergis™ Appliance Portal.

  If you ask the system to update the certificate for such a unit, you get the error message Failed to generate certificate signing request. As a workaround, go to the *Properties* page of the Synergis unit in Config Tool, and click **Reset trusted certificate**.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

Related Topics

About the Unit Assistant role on page 233

Viewing unit properties on page 229

Scheduling a task on page 221

Investigating user-related activity on your Security Center system on page 392

Configuring HTTPS for video unit extensions on page 595

Enabling unit certificate management in Security Center

To enable the unit certificate management feature in Security Center, you must create the Certificate Signing role and configure the Unit Assistant role for certificate management.

Before you begin

- Make sure all your access control and video units have a firmware version that supports unit certificate management.
- Make sure all your access control units are enrolled with their IP address.

To enable unit certificate management in your system:

1. Secure the communication between the Unit Assistant role and the Certificate Signing role.
2. Create the Certificate Signing role.
3. Configure the Unit Assistant role for certificate management.
4. Restart the Genetec™ Server service on all servers hosting the Archiver role.
5. Create scheduled tasks to renew unit certificates automatically.

Securing the communication between the Unit Assistant role and the Certificate Signing role

To secure the communication between the Unit Assistant role and the Certificate Signing role, you must create a trusted certificate for the localhost.

What you should know

The Unit Assistant role connects to the Certificate Signing role using a URL of the form https://hostname:*port*/management where hostname is the IP address or the host name of the server hosting the Certificate Signing role. To have a simple and robust failover configuration, the two roles must be hosted on the same server. This way, when a failover occurs, both roles fail over to the same server. This also allows us to use localhost instead of the host name in the connection URL. For this reason, the certificate used to secure the communication between the two must be identified as localhost.

NOTE: A consequence of this approach is that only the Config Tool running on the server hosting the Certificate Signing role can be used to fully configure the Unit Assistant role.

To secure the communication between the Unit Assistant role and the Certificate Signing role:

1 Generate the certificate used to secure the communication between these two roles.

a) In the Windows taskbar, click 🔍 and enter `PowerShell`.

b) In the search result, right-click **Windows PowerShell** and click **Run as administrator**.

The *Windows PowerShell* window opens.

c) Enter the command `$PSVersionTable` to find out the version you are running.

IMPORTANT: You must have PowerShell version 5.1.17763.2931 or later. If your version is too old, you must run PowerShell on a server that has a supported version installed, generate and export the certificate, and then import it on the server hosting your two roles.

d) Enter the following command to generate a self-signed certificate.

```
New-SelfSignedCertificate -Type Custom -Subject "CN=SigningPluginSSL,
 O=Genetec Inc., OU=SigningPluginSSL, C = CA" -TextExtension
 @("2.5.29.37={text}1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1",
 "2.5.29.17={text}DNS=localhost") -KeyUsage DigitalSignature -KeyAlgorithm RSA
 -KeyLength 2048 -CertStoreLocation "Cert:\LocalMachine\My"
```

NOTE: To run this command, first copy the preceding string to Notepad, remove the line breaks, then paste the string without line breaks to the *Windows PowerShell* window.

In our sample command, we use `SigningPluginSSL` as the certificate name. If you prefer a different name, simply replace `SigningPluginSSL`, found in two places, with the name of your choice.

e) Close the *Windows PowerShell* window.

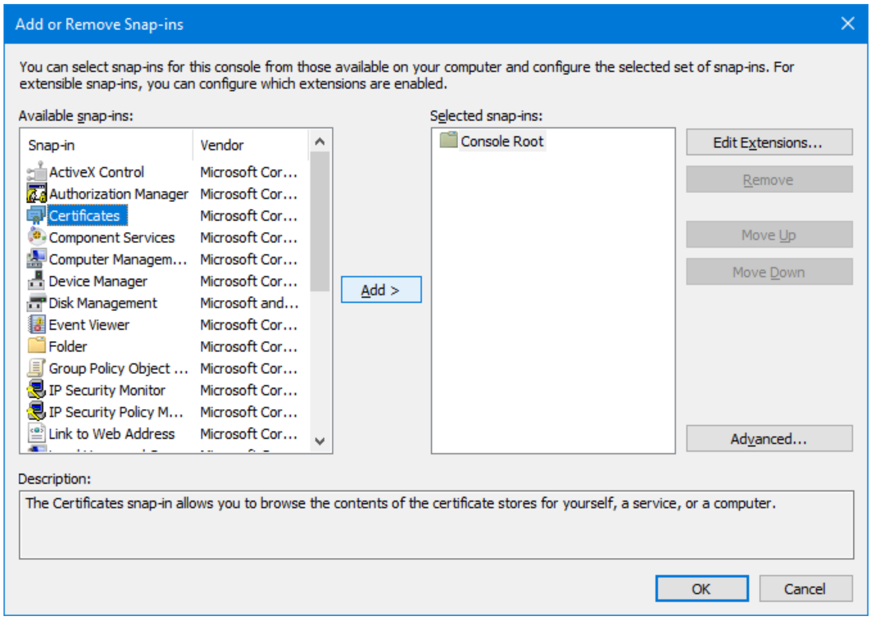
2 Open the *Microsoft Management Console*.

- On Windows Server, do the following:

  a. In the Windows taskbar, click 🔍 and enter `mmc`.

  b. In the windows that opens, click **File** > **Add/Remove Snap-in**.

  c. In the *Add or Remove Snap-ins* window that opens, click **Certificates** > **Add**.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

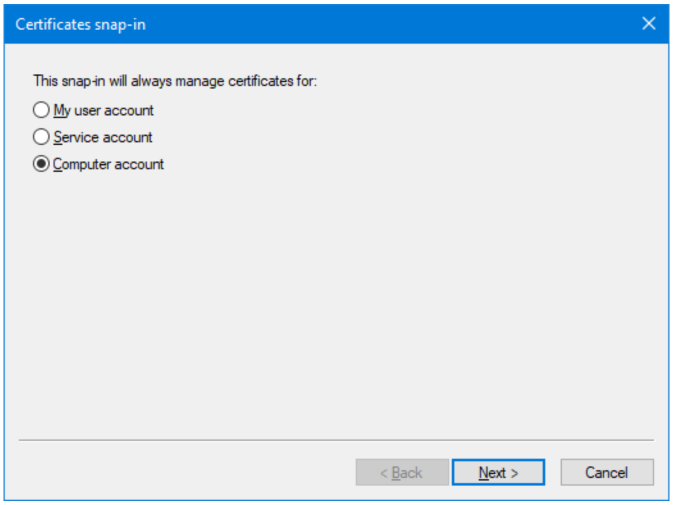
Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins: Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

  d. In the *Certificates snap-in* dialog box that opens, click **Computer account** > **Next**.



Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

  e. Click **Finish** > **OK**.

  The Certificate management snap-in is added.

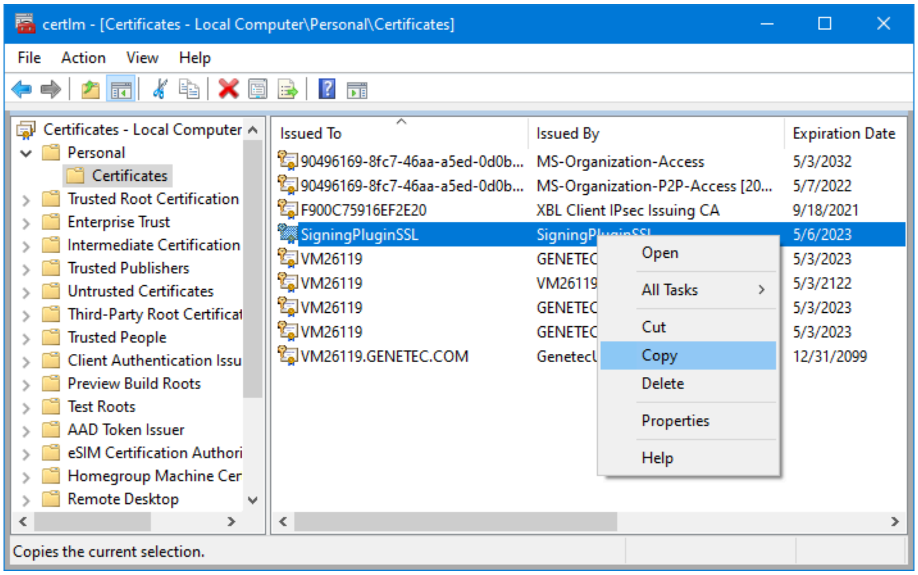
- On Windows 10, do the following:

  a. In the Windows taskbar, click 🔍 and enter `Certificates`.

  b. In the search results, click **Manage computer certificates**.

3 In the left pane of the *Microsoft Management Console* window, expand **Personal** and click **Certificates**.

4 In the right pane of the window, right-click the certificate you created (SigningPluginSSL) and click **Copy**.

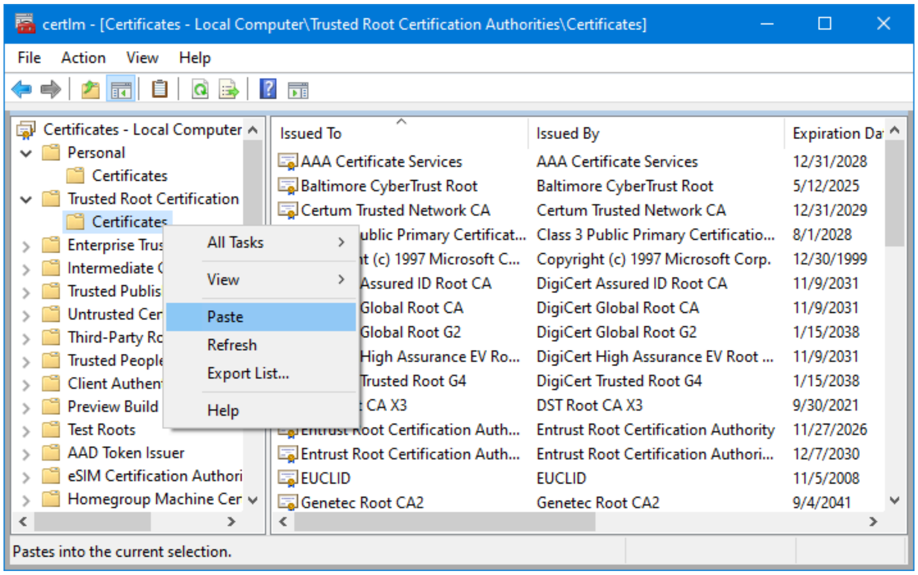


Issued To	Issued By	Expiration Date
90496169-8fc7-46aa-a5ed-0d0b...	MS-Organization-Access	5/3/2032
90496169-8fc7-46aa-a5ed-0d0b...	MS-Organization-P2P-Access [20...	5/7/2022
F900C75916EF2E20	XBL Client IPsec Issuing CA	9/18/2021
SigningPluginSSL	SigningPl	5/6/2023
VM26119	GENETEC	5/3/2023
VM26119	VM26119	5/3/2122
VM26119	GENETEC	5/3/2023
VM26119	GENETEC	5/3/2023
VM26119.GENETEC.COM	GenetecI	12/31/2099

Copies the current selection.

5 In the left pane of the window, expand **Trusted Root Certification Authorities** and click **Certificates**.

6 Right-click **Certificates** and then click **Paste**.



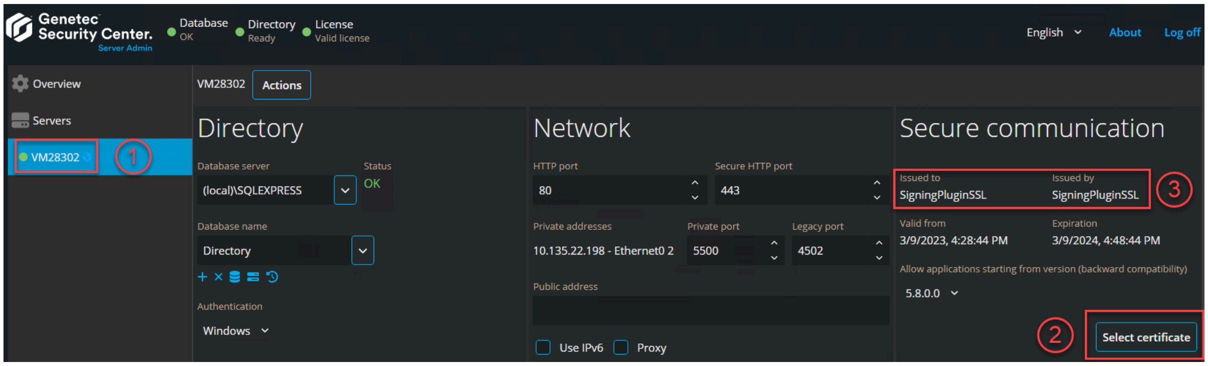
Issued To	Issued By	Expiration Da
AAA Certificate Services	AAA Certificate Services	12/31/2028
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029
ublic Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028
t (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999
Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031
Global Root CA	DigiCert Global Root CA	11/9/2031
Global Root G2	DigiCert Global Root G2	1/15/2038
High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031
Trusted Root G4	DigiCert Trusted Root G4	1/15/2038
CA X3	DST Root CA X3	9/30/2021
oot Certification Auth...	Entrust Root Certification Authority	11/27/2026
Entrust Root Certification Auth...	Entrust Root Certification Authori...	12/7/2030
EUCLID	EUCLID	11/5/2008
Genetec Root CA2	Genetec Root CA2	9/4/2041

Pastes into the current selection.

7 Open Server Admin, and in the left pane, click the name of your server.

8 In the *Secure communication* section, click **Select certificate**.

9 In the dialog box that opens, click the certificate you created earlier (SigningPluginSSL) and click **Select**.



Database OK
Directory Ready
License Valid license

VM28302

Database server: (local)\SQLEXPRESS
Status: OK
Database name: Directory
Authentication: Windows

HTTP port: 80
Secure HTTP port: 443
Private addresses: 10.135.22.198 - Ethernet0 2
Private port: 5500
Legacy port: 4502
Public address:
□ Use IPv6 □ Proxy

Issued to: SigningPluginSSL
Issued by: SigningPluginSSL
Valid from: 3/9/2023, 4:28:44 PM
Expiration: 3/9/2024, 4:48:44 PM
Allow applications starting from version (backward compatibility): 5.8.0.0

10 Click **Save** > **Yes** and close Server Admin

11 If you have more than one server assigned to the Unit Assistant role, repeat the same process on the other servers.

After you finish

Create the Certificate Signing role.

Exporting and importing certificates

If the server hosting the Unit Assistant role does not have a supported version of Microsoft PowerShell, you can generate the certificate on a server that does. Then, export the certificate and import it on the server that hosts the Unit Assistant role.

What you should know

The version of Windows PowerShell must be 5.1.17763.2931 or later.

To generate a certificate on one server and import it on another:

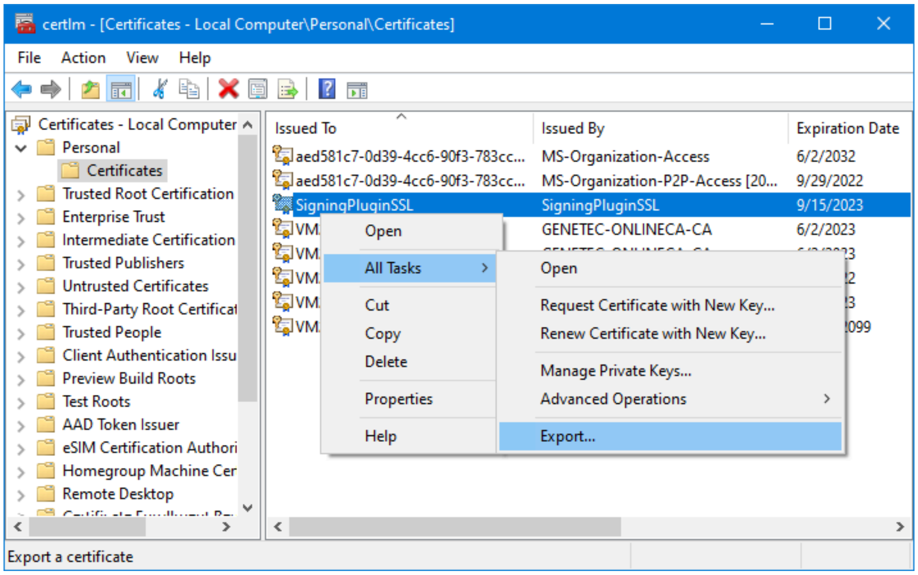
1 On the server that has a supported version of Windows PowerShell installed, generate the self-signed certificate and open the *Microsoft Management Console*.

Follow the instructions found in Securing the communication between the Unit Assistant role and the Certificate Signing role on page 236.

2 Export the certificate that you generated.

a) In the left pane of the *Microsoft Management Console* window, expand **Personal** and click **Certificates**.

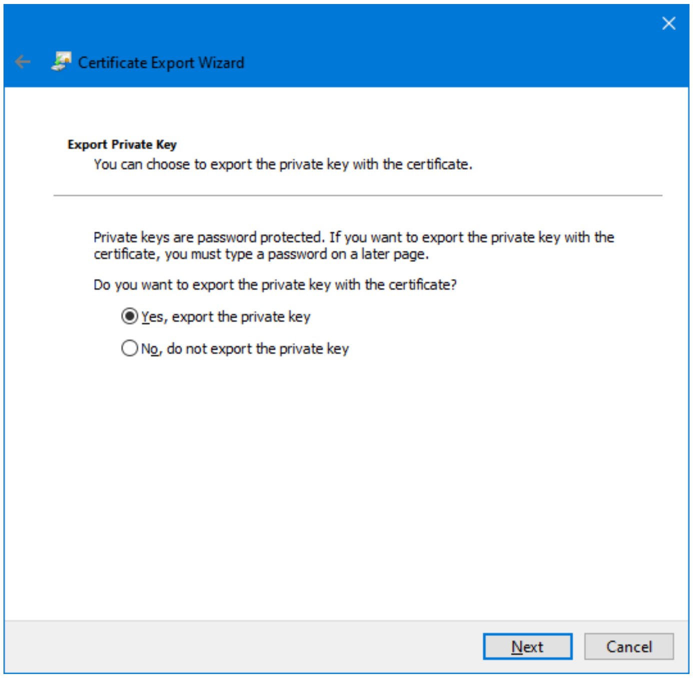
b) In the right pane of the window, right-click the certificate you created (SigningPluginSSL) and click **All Tasks** > **Export**.



Issued To	Issued By	Expiration Date
aed581c7-0d39-4cc6-90f3-783cc...	MS-Organization-Access	6/2/2032
aed581c7-0d39-4cc6-90f3-783cc...	MS-Organization-P2P-Access [20...	9/29/2022
SigningPluginSSL	SigningPluginSSL	9/15/2023
VM	GENETEC-ONLINECA-CA	6/2/2023

The *Certificate Export Wizard* opens.

c) Click **Next** > **Yes, export the private key**.



Export Private Key
You can choose to export the private key with the certificate.

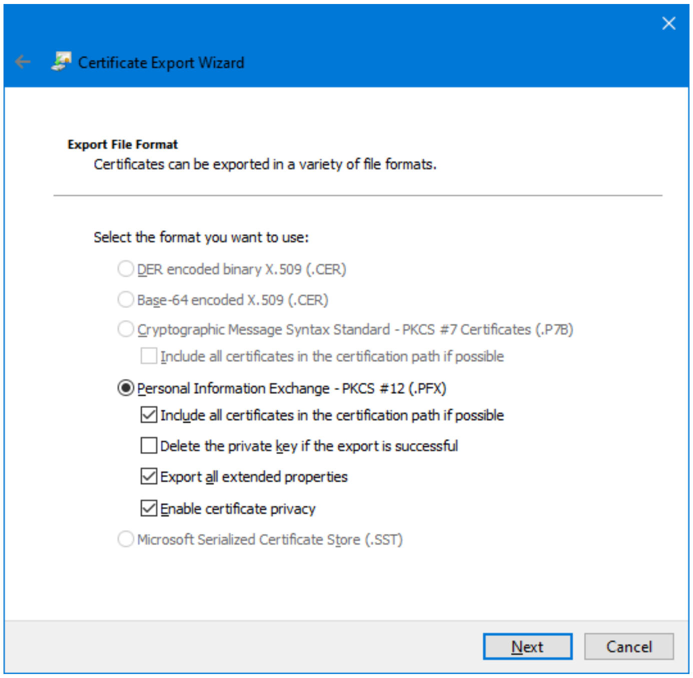
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

d) Click **Next** and select the options to export all extended properties as shown in the following screen capture.



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

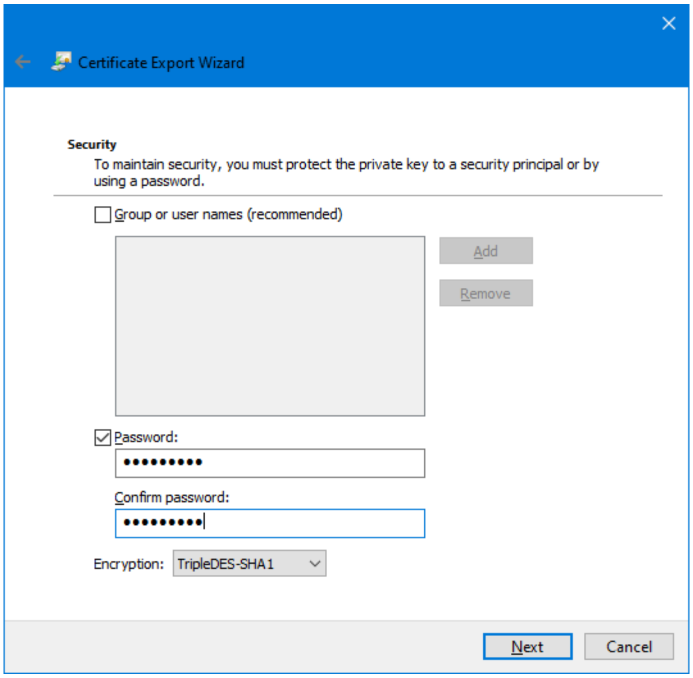
□ Delete the private key if the export is successful

☑ Export all extended properties

☑ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

e) Click **Next** > **Password** and enter a security password.



Security

To maintain security, you must protect the private key to a security principal or by using a password.

□ Group or user names (recommended)

☑ Password:

•••••••••

Confirm password:

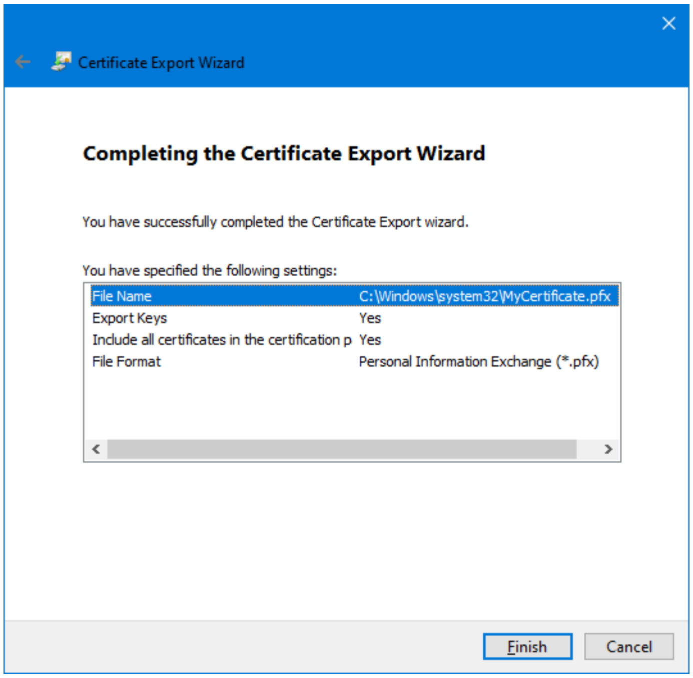
•••••••••

Encryption: TripleDES-SHA1

Be sure you remember the password. You need it to import the certificate.

f) Click **Next** and give a name to your certificate export file (*.pfx*).

g) Click **Next**, take note of the export settings, and click **Finish**.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Windows\system32\MyCertificate.pfx
Export Keys	Yes
Include all certificates in the certification p	Yes
File Format	Personal Information Exchange (*.pfx)

h) Copy the certificate export file to a USB key.

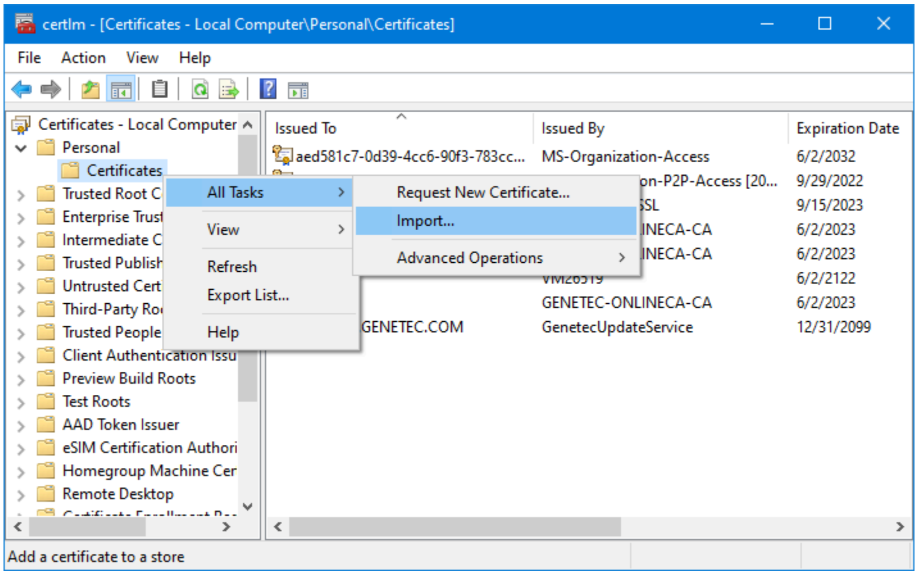
3 Import the certificate on the server hosting the Unit Assistant role.

a) On the server hosting the Unit Assistant role, connect the USB key containing the certificate export file.

b) In the Windows taskbar, click 🔍 and enter `Certificates`.

c) In the search results, click **Manage computer certificates**.

d) In the left pane of the *Microsoft Management Console* window, expand **Personal**, right-click **Certificates**, and click **All Tasks** > **Import**.



The *Certificate Import Wizard* opens.

e) Follow the instructions from the Wizard.

4 After the certificate is imported to the **Personal** store, copy it to the **Trusted Root Certification Authorities** store.

Follow the instructions found in Securing the communication between the Unit Assistant role and the Certificate Signing role on page 236 until the end.

After you finish

Create the Certificate Signing role.

Creating the Certificate Signing role

To fulfill the job of the certificate authority (CA) in your system, you must create the Certificate Signing role.

Before you begin

Secure the communication between the Unit Assistant role and the Certificate Signing role

What you should know

The Certificate Signing role acts as the certificate authority (CA) for all access control and video units whose certificates are managed in Security Center by the Unit Assistant role. You may have only one instance of this role in your system.

To create the Certificate Signing role:

1. Log on to Security Center using Config Tool.

   If you intend to configure failover for the Unit Assistant and Certificate Signing roles, we recommend that you log on from the Config Tool installed on the server hosting the Unit Assistant role. This way, you can continue with the configuration of the Unit Assistant role without switching workstation.
2. From the Config Tool home page, open the *Plugins* task, and click **Add an item** (✚) > **Plugin** (🧩).

   The plugin role creation wizard opens.
3. On the *Specific info* page, select the server on which the plugin role is to be hosted.
4. Select **Certificate Signing** as the plugin type.
5. If the role database is created in advance by your DBA team, select the **Database server** and **Database**, and then click **Next** > **Next** > **Create**.

   The Certificate Signing role is created.
6. Select the Certificate Signing role and click the **Properties** tab.
7. If necessary, change the value of **Port** and click **Apply**.

   This port (default = 6010) is used by the Unit Assistant role to communicate with the Certificate Signing role.
8. If role failover is required, do the following:

   a) Click the **Resources** tab.

   b) Add the necessary secondary servers.

   c) Make sure the database server is hosted on a separate server and accessible to all servers assigned to the role.

   d) Click **Apply**.

After you finish

Configure the Unit Assistant role for certificate management

Configuring the Unit Assistant role for certificate management

Before the Unit Assistant role can effectively manage unit certificates, you must configure the certificate management settings and the certificate profile.

Before you begin

Create the Certificate Signing role

To configure the Unit Assistant role for certificate management:

1 Log on to Security Center with the Config Tool installed on the server hosting the Unit Assistant role.

2 From the Config Tool homepage, open the *System* task and click the **Roles** view.

3 Select the Unit Assistant role and click the **Properties** tab.

4 In the *Security* section, configure the **Certificate management** settings.

- **Security policies:**
  - **Allow renewal of expired certificates:** Turn on this setting (on by default) to allow the system to renew unit certificates automatically, even after they are expired. If you do not want expired certificates to be automatically renewed, turn off this setting. You can always manually renew expired certificates from the *Hardware inventory* task.
  - **Enable HTTPS on units after successful certificate installation:** Turn on this setting (on by default) to force the unit to switch to HTTPS after the certificate is successfully installed. The HTTPS ports configured in Security Center for the units might change during the process if the Unit Assistant can detect the correct port.
- **Notifications:** Specify, in days, how soon you want the system to trigger a warning before a certificate expires (default = 7 days).

  If you configured your system to automatically renew certificates X days before they expire, set this value to X minus N, where N is the number of days you give the system to try to automatically renew a certificate before issuing a warning. Also be sure to give yourself enough time to investigate why a certificate was not renewed after you received the warning.
- **Certificate information:**
  - **Validity period:** This is the validity period of a certificate after a renewal. This value is inherited from the CA. It can only be modified from the *Certificate profile* page.
  - **Show advanced:** Click this button to show the optional properties that you can assign to certificates created by your system. The *Country*, *State*, *Locality*, *Organization*, and *Organizational unit* help you identify certificates issued for your organization. These values can be overwritten on specific certificate renewals.

5 In the *Public key infrastructure* section, click **Set custom endpoint** and enter in the **Endpoint** field, the URL of your *certificate authority (CA)*.

NOTE: For Security Center 5.11, the CA is the Certificate Signing role.

The syntax of the URL is as follows:

```
https://hostname:port/management
```

where *hostname* is the hostname or IP address of the server hosting the Certificate Signing role, and *port* is the port number configured in the *Properties* page of the Certificate Signing role. Make sure the server hosting the Unit Assistant role can access this URL.

IMPORTANT: To simplify the failover configuration, the URL is set by default to https://localhost:*port*/management. This assumes that both the Unit Assistant role and the Certificate Signing role are always hosted on the same server. If you choose to host the two roles on separate servers, then when a failover occurs, you must manually change the value of the URL here and restart the Unit Assistant role.

6 Click **Apply**.

7 Restart the Unit Assistant role.
   a) In the left pane, right-click **Unit Assistant** and then click **Maintenance** > **Deactivate role**.
   b) After the role turned red, right-click **Unit Assistant** and then click **Maintenance** > **Activate role**.

8 Click **Certificate profile** to configure the policies and the limits imposed on certificate requests applied by the CA.

   - **Allowed domain name:** Must match your network domain name. Leave it blank if you do not want to include the domain name in the certificates.
   - **Allowed IPv4 range:** Enter the IPv4 range of the units you expect to connect to on your network. Leave it blank if you do not want the units to use IPv4.

     The IP range must follow the CIDR convention. All units must be found within this range of IP addresses. We do not support discrete ranges of IP addresses.
   - **Allowed IPv6 range:** Enter the IPv6 range of the units you expect to connect to on your network. Leave it blank if you do not want the units to use IPv6.

     The IP range must follow the CIDR convention. All units must be found within this range of IP addresses. We do not support discrete ranges of IP addresses.
   - **Validity period:** Specify, in days or months, the validity period of the renewed certificates according to your security policies. We recommend a period between six months and one year.

9 Click **Apply**.

10 Select the certificate-related health events that you want to monitor.

   The certificate-related health events that you can monitor are:

   - **Certificate warning:** The certificate is about to expire.
   - **Certificate error:** There is an error that makes communications with the unit insecure.
   - **Certificate valid:** The status of the certificate returned to valid after being in error or warning.

   These events are found under the **Access control unit** group and the **Video unit** group.

   BEST PRACTICE: We strongly suggest that you create event-to-actions to inform your system administrator when certificate-related issues occur.

After you finish

If later you must change any of these settings, you must do it at a time when the Unit Assistant role is not updating any certificate.

IMPORTANT: If you change the communication port of the CA (Certificate Signing role) or any setting in the *Certificate profile* page, you must restart the Unit Assistant role for the change to take effect. If you change to a new CA, any unit that has its certificate signed by the old CA must be renewed as soon as possible. Otherwise, when you move your unit to a new role, the unit might stop working because the old CA's root certificate would not be deployed on the server hosting the new role.

Also note that the root certificate of the old CA is not automatically removed when it is no longer in use. If required, after all unit certificates have been renewed, you can manually remove it from the Windows Certificate Store.

Configuring Security Center to renew unit certificates automatically

You can configure Security Center to automatically renew the unit certificates when they are about to expire, using the *Renew unit certificate* action through a scheduled task.

Before you begin

Configure the Unit Assistant role for certificate management.

What you should know

You need the *Update access control unit certificate*, *Update video unit certificate* and *Modify certificate management settings* privileges to configure the *Renew unit certificate* action. This action is executed by the Unit Assistant role and is only available through scheduled tasks, not through event-to-actions. The Unit Assistant role checks the certificate expiration date of the selected units and renews the ones that will expire within the configured time frame.

NOTE: If you cleared the **Allow renewal of expired certificates** option, the Unit Assistant will not renew certificates that are already expired.

To configure a scheduled task for automatic unit certificate renewal:

1. Create a scheduled task.

   The **Recurrence** of the scheduled task is how frequently you want the system to check the certificate expiration dates. We strongly recommend using a daily recurrence to avoid missing any certificate renewal deadline. The system only renews certificates that are about to expire, based on the value of **days before expiration** defined later.

   CAUTION: Changing a unit certificate causes a short recording interruption, so choose a time of day that minimizes disruption to your operations. Make sure you do not change the certificate and the password on the same units at the same time.
2. From the **Action** list, select **Renew unit certificates**.
3. In the **days before expiration** field, specify how soon you want to renew a certificate before it expires.

   This value should be greater than the number of days the system sends the notification (*Certificate warning*) before a certificate expires. As a rule of thumb, if your certificates are valid for one year, renew your certificates one month before they expire, and send the warning 28 days before they expire.
4. Specify the source information the certificates are based on.

   Beside **Certificate information**, select one of the following:

   - **Inherit from Unit Assistant:** Use the information configured in the Unit Assistant role's *Properties* page.
   - **Custom:** Enter specific information for this scheduled task.
     - **Validity period:** This value is a CA setting. It can only be changed from the Unit Assistant role's *Certificate profile* page.
     - **Show advanced:** Click this button to show the optional properties, such as *Country*, *State*, *Locality*, and so on, that you can override here.
5. Select the units that are considered for certificate renewal.

   Beside **Entities**, select one of the following:

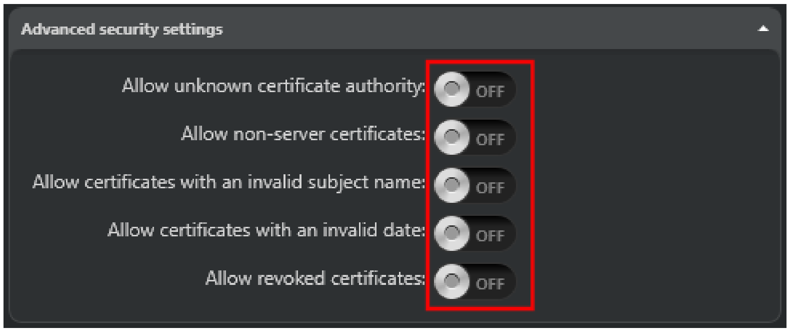
   - **All units:** Consider all units in your system.
   - **Custom:** Select individual or groups of units that should be evaluated. Use this option if you want to assign different time slots to units found in different time zones. The scheduled task follows the time zone of your Directory server. If you select an area, all units within that area are selected.

     BEST PRACTICE: We recommend that you do not exceed 100 access control units or 1,000 video units per batch. If your system has more units than the recommended maximum per batch, divide them into small batches and create separate scheduled tasks running at a different time for each. Make sure the different scheduled tasks do not overlap. As a general rule, allow 15 minutes between batches.
6. Click **Apply**.

   NOTE: After your system installs a certificate on a unit, you should no longer use the or any third-party tool to update the certificate.

After you finish

After the certificates of all Axis units under a given Archiver role are managed by Security Center, turn off the *Advanced security settings* in the Axis extension for that Archiver role to close all potential security holes.



Advanced security settings

Allow unknown certificate authority: OFF

Allow non-server certificates: OFF

Allow certificates with an invalid subject name: OFF

Allow certificates with an invalid date: OFF

Allow revoked certificates: OFF

NOTE: If your system is using IP addresses for cameras and you want to transition to hostnames, you need to turn on the **Allow certificates with an invalid subject name** option during the transition period. This is because the certificates only have a common name containing an IP address and they become invalid when a hostname is added to the unit configuration in Config Tool.

Related Topics

Renewing unit certificates manually on page 248

Renewing unit certificates manually

You can manually install or renew certificates on selected units at any time, using the *Hardware inventory* task.

What you should know

Unit certificates that you renew manually can be logged in the *Activity trails*. To log manual certificate renewals, select **Unit certificate changed** under the *General* category in **Config Tool** > **System** > **General settings** > **Activity trails**.

To manually renew unit certificates:

1. From the homepage, open the *Hardware inventory* task.
2. Right-click the column headers and click **Select columns**.
3. Select the certificate-related columns which are hidden by default.
   - **Certificate status:** Certificate management status of the unit.
     - **Managed:** The certificate is managed by the system and is valid.
     - **Expired:** The certificate is managed by the system but has expired.
     - **Unmanaged:** The certificate is not managed by the system but can be. To enroll the unit for certificate management, select the unit and click **Update certificate** () at the bottom of the screen.
     - **Unsupported:** The certificate cannot be managed by the system. The reason might be that the unit model or extension does not support this feature, or that the unit firmware is not up to date.
   - **Certificate expiration:** Certificate expiration date. The date is shown only if the certificate is managed by the system. To view the certificate details in a separate window, select the unit and click **View certificate** () at the bottom of the screen.
   - **Last certificate update result:** Success or failure of the last certificate update carried out by the system.

4 Set up the query filters to look for access control (or video) units.

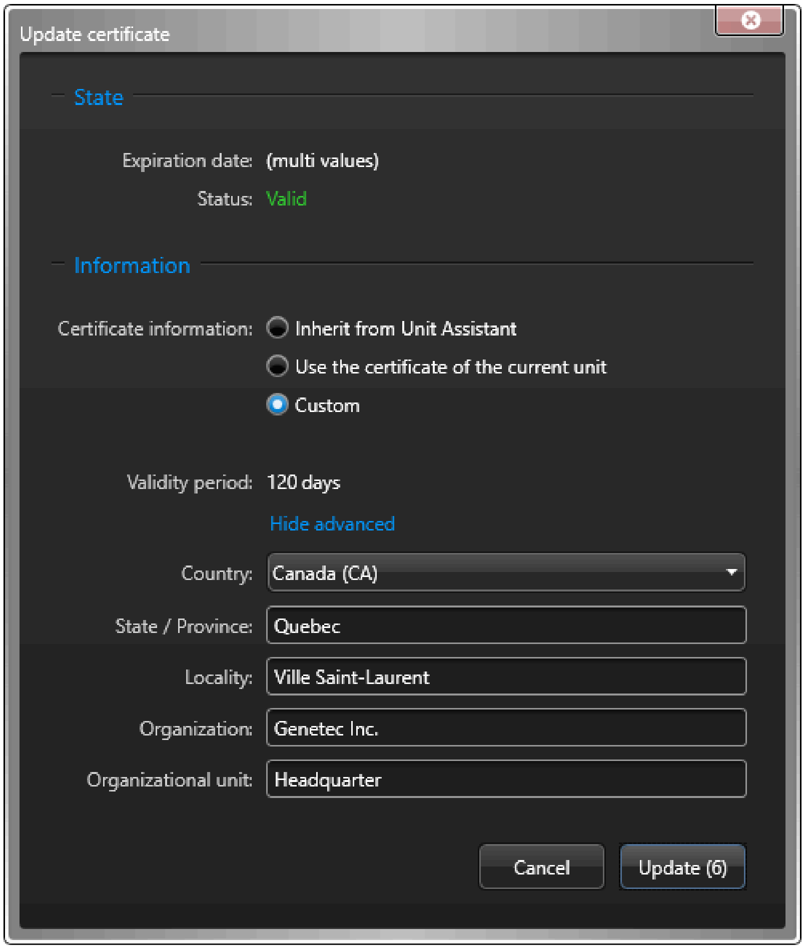
Open the **Units** filter and do one of the following:

- Select **All entities** and select the Access Manager (or Archiver) roles you want to select all the units they control.
- Select **Access control units** and click to apply a custom filter of your choice.
- Select **Video units** and click to apply a custom filter of your choice.

5 Click **Generate report**.

6 Select the units you want to enroll for unit certificate management or certificate renewal, and click **Update certificate** ().

The *Update certificate* dialog box opens.



Update certificate

State

Expiration date: (multi values)

Status: Valid

Information

Certificate information: ○ Inherit from Unit Assistant ○ Use the certificate of the current unit ● Custom

Validity period: 120 days

Hide advanced

Country: Canada (CA)

State / Province: Quebec

Locality: Ville Saint-Laurent

Organization: Genetec Inc.

Organizational unit: Headquarter

7 Under *Certificate information*, select one of the following:

- **Inherit from Unit Assistant:** Use the information configured in the Unit Assistant role's *Properties* page.
- **Use the certificate of the current unit:** Use the information found in the currently installed certificate. This option is only available if some of the selected units have a certificate installed by Security Center. The units that are still unmanaged are skipped when this option is selected.
- **Custom:** Enter specific information for this scheduled task.
  - **Validity period:** This value is a CA setting. It can only be changed from the Unit Assistant role's *Certificate profile* page.
  - **Show advanced:** Click this button to show the optional properties defined in the Unit Assistant role, such as *Country*, *State*, *Locality*, and so on, that you can override here.

8 If you selected **Custom**, enter the custom settings as required.

9 Click **Update**.

10 Confirm that the update was successful.

Wait 10 to 20 seconds and refresh the report. Check the certificate status, last update result, and expiration to confirm that everything worked as expected.

NOTE: After your system installs a certificate on a unit, you should no longer use the or any third-party tool to update the certificate.

Related Topics

Configuring Security Center to renew unit certificates automatically on page 246

Unit password management

Unit password management is the feature set enabled by the Unit Assistant role that you can use to safely and securely update the passwords of all your video units and access control units from a central location.

With the Unit Assistant role, you can change the passwords from Security Center and apply them to your units. To distribute the workload, the password change requests are relayed to the Archiver roles responsible for the video units, and to the Access Manager roles responsible for the access control units.

A successful password change request must pass the following tests:

- Connection with the new password must succeed.
- Connection with the old password must fail.

All password-related operations are controlled by privileges and must be performed from Config Tool. The last five password change requests for every unit are kept, encrypted, in the Unit Assistant database. Should you lose your passwords for any reason, contact Genetec™ Technical Assistance Center.

Supported password operations

- Change passwords individually on each unit, from the unit *Properties* page.

  The following privileges are required, depending on your unit type:

  - *Update video unit password*
  - *Update access control unit password*

  NOTE: Passwords can be manually entered or system generated. We recommend using system-generated passwords because they are more secure. The system always uses the highest password complexity supported by the manufacturers.
- View and export unit passwords from the *Hardware inventory* task.

  The *View/export unit passwords* privilege is required.
- Update unit passwords in batches from the *Hardware inventory* task.

  The following privileges are required, depending on your unit type:

  - *Update video unit password*
  - *Update access control unit password*
- Execute the *Update unit password* action from scheduled tasks and event-to-actions.

Supported access control units

This following types of access control units support the password update feature from Config Tool:

- Synergis™ units running Synergis™ Softwire 11.0 or later
- Axis Powered by Genetec units

Supported video unit models

Only certain models of video units support the password update feature from Config Tool. You might have to upgrade the unit firmware for this feature to work. For the list of manufacturers that support this feature, see "Manufacturers that support password update" in the *Security Center Video Unit Configuration Guide*.

Best practices for password management

- Use HTTPS whenever it is possible.

- Track password change and export operations with the *Activity trails* report.

  Enable the **Unit password changed** and **Unit passwords exported** options in **Config Tool** > **System** > **General settings** > **Activity trails**, under the *General* category.
- Always export the unit passwords from the *Hardware inventory* task after password updates. This ensures that you have a copy of the passwords if you ever need to connect to the units through their web portals.
- Always export the unit passwords when all the units are online. This ensures that all current working passwords are captured in the export.
- Include the Unit Assistant database in your backup procedure. This ensures that your latest password change requests are backed up in the event of a problem.
- Always test this feature on a few units before applying it to a large batch of units of the same brand and model.
- Changing a unit password causes a short recording interruption, so choose a time of day that minimizes disruption to your operations.

Related Topics

About the Unit Assistant role on page 233

Changing video unit passwords on page 574

Updating video unit passwords in batches on page 578

Changing access control unit passwords in Config Tool on page 763

Viewing unit properties on page 229

Scheduling a task on page 221

Investigating user-related activity on your Security Center system on page 392

Exporting unit passwords

After changing the password on a number of units, we recommend that you export the new passwords to a CSV file as a safety measure.

What you should know

- You need the *View/export unit passwords* privilege to perform this operation.
- To ensure that you are exporting the latest Synergis™ Cloud Link unit passwords, you must regenerate the *Hardware inventory* report right before exporting the password. If a report was already generated during a password update, the latest password information will not be included in the report.

To export your current unit passwords to a CSV file:

1. From the Config Tool home page, open the *Hardware inventory* task.
2. Set up the query filters for your report.

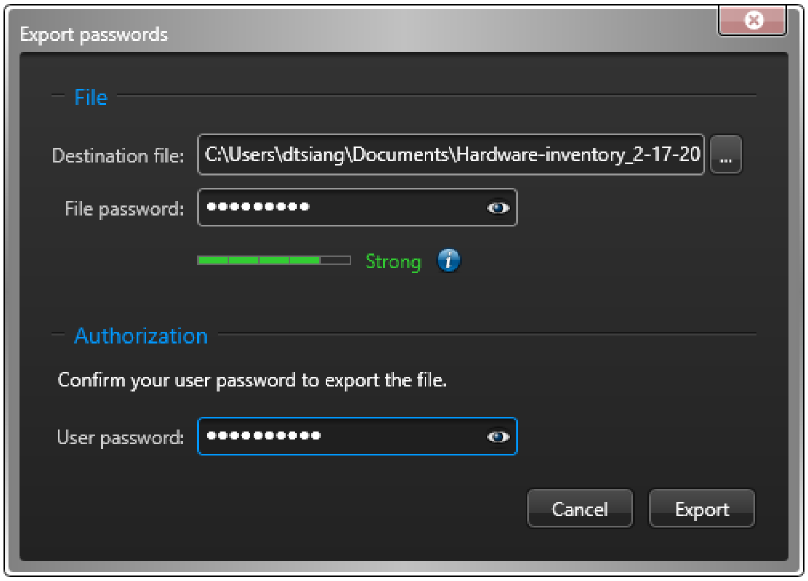
   Choose one or more of the following filters:

   - **Units:** Select individual units or roles to investigate. Selecting a role is equivalent to selecting all units managed by that role.
   - **Source group:** Select the category of units (Access control, ALPR, Intrusion detection, or Video).
   - **Custom fields:** Restrict the search to a predefined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
3. Click **Generate report**.

   The selected units are listed in the report pane.

4 Click **Export passwords**.

The *Export passwords* dialog box opens.



Export passwords

File

Destination file: C:\Users\dtsiang\Documents\Hardware-inventory_2-17-20

File password: ●●●●●●●●●

Strong

Authorization

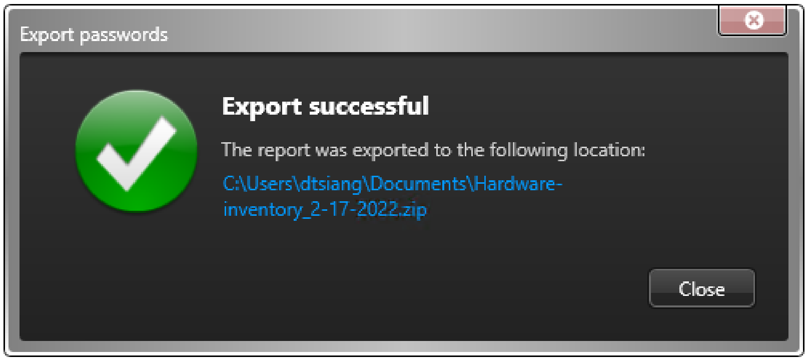
Confirm your user password to export the file.

User password: ●●●●●●●●●●

5 Enter the following and click **Export**.

- **Destination file:** Location of the exported CSV file, compressed as a zip file.
- **File password:** Password used to secure access to the compressed CSV file. Choose a strong password.
- **User password:** Your Security Center password.

If all went well, you get a confirmation that a zip file has been created.



Export passwords

Export successful

The report was exported to the following location:

C:\Users\dtsiang\Documents\Hardware-inventory_2-17-2022.zip

6 Click the blue link in the message box and make sure that you can extract the CSV file using the **File password** you provided.

NOTE: You must use a file extraction tool, such as WinZip or 7-Zip to be able to enter the password for the file. Using the default Windows File Explorer does not work.

7 Keep the password file and its password in a safe place.

11

Record fusion and data ingestion

This section includes the following topics:

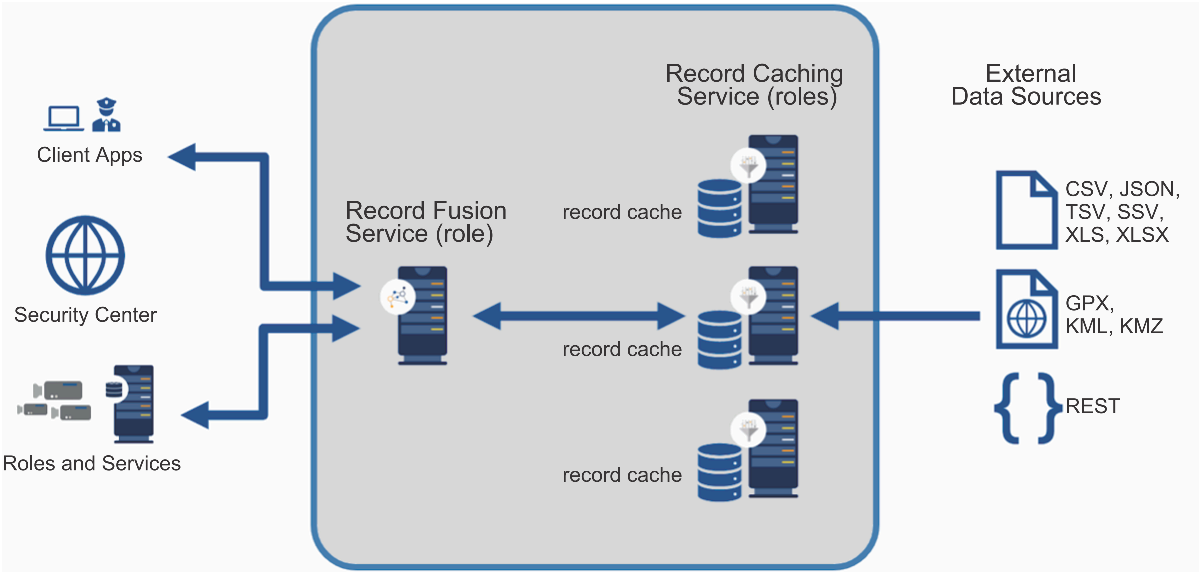
About data ingestion

Data ingestion is the means through which you can import data from external sources into Security Center without having to develop complex code-based integrations.

The Record Caching Service role

The role that handles data ingestion in Security Center is called the Record Caching Service. To make external data accessible to Security Center applications, the Record Caching Service role keeps a copy of the ingested data in a local database called the *record cache*. The data format of the cached Records, including their display properties in Security Center, are stored in the Directory database and called the *record type*.

After a record type is configured, you can use it to ingest external data from a flat file, a REST endpoint, or through custom integration using the Security Center SDK. If you have many different types of records to ingest on a regular basis, you can define multiple Record Caching Service roles to distribute the load.



Any Security Center module can use the ingested data. You can use the *Records* investigation task in Security Desk to view the ingested data and derive new information based on suspected or known *correlations*.

The Record Fusion Service role

The Record Fusion Service is the central role that provides a unified querying mechanism for data records that come from a wide variety of sources, such as Security Center modules or third-party applications. All record requests go through this role, which then queries their respective record providers.

A record provider is either a Security Center role or an SDK application that connects a data source to the Record Fusion Service role. For example, the Record Caching Service is the record provider for data imported from third-party sources. The Map Manager role can also be a record provider by converting map objects into records so they can be uniformly queried through the Record Fusion Service.

Required software license

If your software license supports *Record fusion*, which is included in the Professional and the Enterprise editions, the Record Fusion Service is created by default when the Directory starts. However, you must create the Record Caching Service roles yourself. To create this role, your software license must support *Record* *caching*. The number of different record types you can create is limited by the *Number of record types for caching* option.

Creating Record Caching Service roles

To use data from external sources in Security Center, you must first create a Record Caching Service role to import and store this data in Security Center.

What you should know

The Record Caching Service role is used for *data ingestion*. Using this role, you can import records from external data sources into Security Center. You can share the ingested data across the entire unified platform to enhance awareness and response, to provide contextual information on dynamic maps, or to visualize in operational dashboards. The imported data is stored in a local database called the *record cache* and can be viewed through the *Records* investigation task.

To create a Record Caching Service role:

1 Open the *System* task and click the **Roles** view.

2 Click **Add an entity** > **Record Caching Service**.

3 On the *Specific info* page, do the following:

a) If you have multiple servers in your system, click the **Server** list and select the server where this role is hosted.

b) Select the **Database server** used to manage the role database.

During software installation, a default database server, **(local)\SQLEXPRESS**, might have been installed on your server. You can use it or use another database server on your network.

c) In the **Database** field, enter the name for the database used to store the ingested data.

CAUTION: The default name is *RecordCache*. If the selected server is already hosting another instance of Record Caching Service, you must choose a different name. Otherwise, the new role will corrupt the existing database.

TIP: To avoid confusion, use a different database name for every instance of Record Caching Service, whether or not there is a conflict.

d) From the **Authentication** list, select which SQL Server authentication is to be used:

- **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
- **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.

e) Click **Next**.

4 On the *Basic information* page, enter a name and description for the role.

5 If there is a **Partition** field, select the partition this role is a member of.

Partitions determine which Security Center users have access to this entity. Only users who have been granted access to the partition can see this role.

6 Click **Next** > **Create** > **Close**.

A new Record Caching Service role () is created. Wait a few seconds for the role to create the database on the selected database server.

7 Click the **Resources** tab and configure the server and database for this Record Caching Service.

8 Click the **Properties** tab and define the record types that this Record Caching Service is going to manage.

Related Topics

Record Fusion Service configuration tabs on page 1381

Creating record types

For each external data source you want to use in Security Center, you must first create a *record type*, define the record format, and configure how you want to display this record type in your system.

Before you begin

Create a Record Caching Service role.

What you should know

In Security Center, a record type defines the data format and display properties of a set of records that you can share across the entire system through the Record Fusion Service role. When you create a record type for the Record Caching Service role, the latter automatically registers the record type with the Record Fusion Service.

The following procedure is only for creating record types managed by the Record Caching Service role. To register map objects as record types, see Configuring the Map Manager role on page 288.

You can view the ingested records using the *Records* investigation task. If your records are georeferenced using the WGS84 standard, you can also view them on geographic maps.

To create a record type:

1. Open the *System* task and click the **Roles** view.
2. Select the Record Caching Service you want to use to manage this record type and click the **Properties** tab.
3. Define the record format.
4. Configure the record display properties.
5. If your record type has latitude and longitude fields, configure its map display properties.
6. Click **Apply**.

   The record type is created and listed on the *Properties* page of the Record Fusion Service role. A new set of privileges are also added to the privilege hierarchy on the *User - Privileges* page. Under **Task privileges** > **Investigation** > **Record fusion** > **Records**, a new privilege bearing the name of your record type is added.

   NOTE: If you are not a member of the Administrators user group, an administrator must grant you the new privilege associated to the record type you created before you can access it.
7. Grant the new privilege to the users that you allow to view, modify, and delete data from this record type.

After you finish

Import data through your record type.

Defining the record format

To create a record type, you must first define the format of the records you want to import. You can define the format manually or let the system derive it from a data file.

What you should know

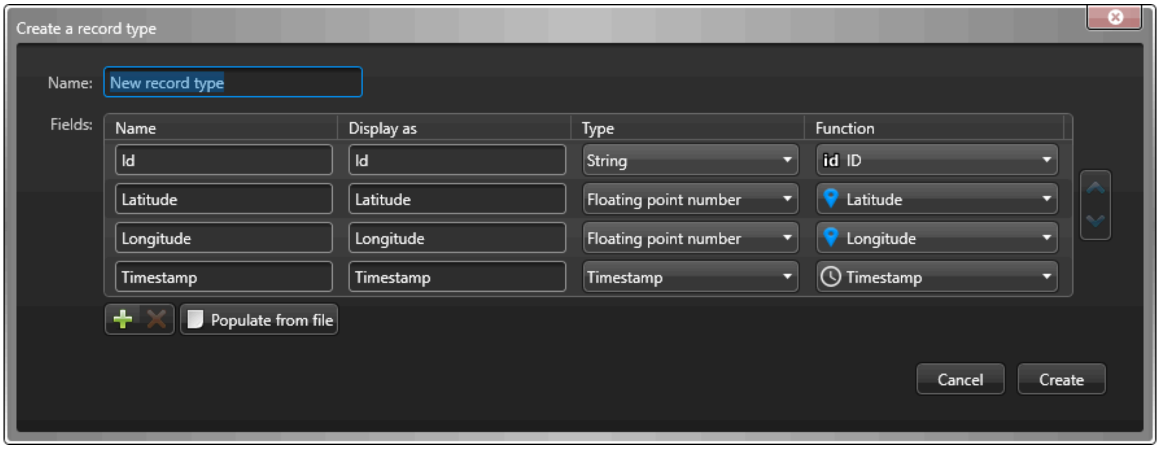
The record format is defined as a list of fields. Each field in the record type is characterized by four properties: name, display name, type, and role. You can either define the field list manually or let the system populate the list automatically by deriving the field definitions from a file containing the records you want to import.

CAUTION: After the record type is created, you can only change how the fields are displayed. If you missed a field or misconfigured a field attribute, you must delete the record type and start over.

To define the record format manually:

1 At the bottom of the *Properties* page, click **Add an item** (✚).

The field definition dialog box opens with four suggested fields.



Name: New record type

Fields:

Name	Display as	Type	Function
Id	Id	String	id ID
Latitude	Latitude	Floating point number	Latitude
Longitude	Longitude	Floating point number	Longitude
Timestamp	Timestamp	Timestamp	Timestamp

2 Give a **Name** to the record type.

3 Adjust the number of fields as needed.

- Click ✚ to add a new field.
- Select a field and click ✖ to remove it.

You can have as many fields as required by your record type.

4 For each data field, define the following attributes:

- **Name:** Name used to identify the field in report filters and display format expressions. All field names are case-sensitive.
- **Display as:** Name used to identify the field in the information bubble when ingested data is displayed on a map.
- **Type:** The type attribute defines both how the data is stored in the ingestion database and how it is read from a data file.

  The following types are supported:

  - **String:** An alphanumeric string.
  - **32 bit integer:** An integer in the range -2,147,483,648 to 2,147,483,647.
  - **64 bit integer:** An integer in the range -9.223372x10^{18} to 9.223372x10^{18}
  - **Floating point number:** A floating point number.
  - **Boolean:** A Boolean value expressed as 1 or 0, or a string containing one of the following: "True", "False", "true", "false", "T", or "F".
  - **Timestamp:** A string or number that can be parsed as either:
    - A timestamp in one of any known formats understood by C#. See DateTime.TryParse Method.
    - A number representing the number of *ticks* elapsed since midnight January 1, 0001 that can be converted to a timestamp. A tick is one-ten-millionth of a second. See DateTime.Ticks.Property.
  - **Security Center entity:** A GUID that represents the internal ID of a Security Center entity.
  - **Binary - Base64:** Binary data represented as text using the Base64 encoding scheme.
  - **Binary - file:** String containing the path to a file on disk.
  - **Extended string:** A long text. The difference between *String* and *Extended string* is their expected size.

The last three data types are used for large data. Fields using these data types are not loaded by default when a record is fetched from the ingestion database. To help optimize the system performance, the data is only loaded on demand.

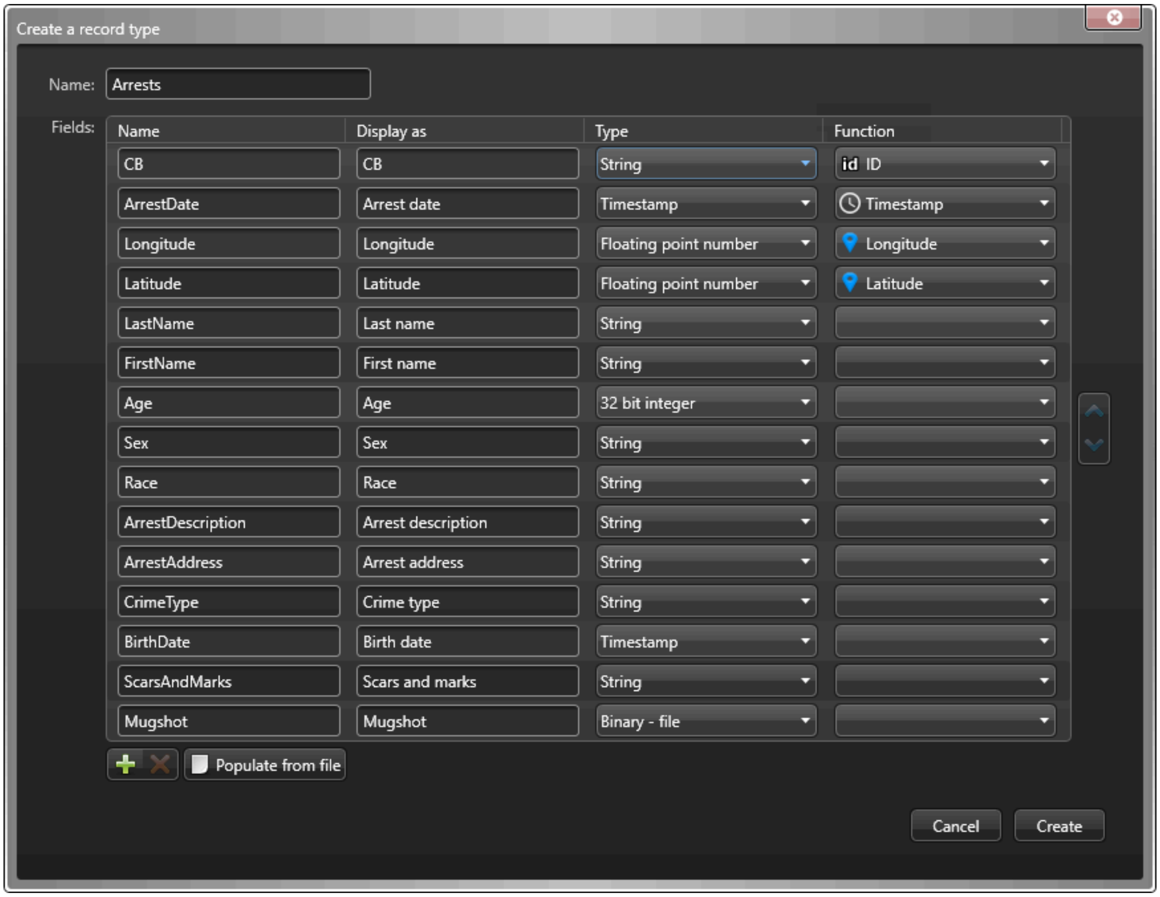
- **Function:** Fields that have a specific function in the record are indexed for faster access. A given function can only be assigned to one field. The following functions are predefined:
  - **ID:** Designates a field as the primary key. Each value from that field must be unique within the record type. It is the only function that must be assigned to a field. All other functions are optional.
  - **Timestamp:** Designates a timestamp field for time correlation. There can be many timestamp fields in a record type, but only one can be assigned the *Timestamp* function.
  - **Latitude, Longitude:** These two functions must be assigned together. The *Latitude* and *Longitude* fields must correspond to a geographical location that can be used to position the data on a map and for geofencing.
  - **Location:** This function is equivalent to the *Latitude* and *Longitude* functions. They are mutually exclusive. A field assigned to the *Location* function must contain a string in the format `{"Latitude": n.nnnn, "Longitude": n.nnnn}`.

5 Review all fields definitions and click **Create**.

To populate the field list from a data file:

1 Click **Populate from file**, select a data file, and click **Open**.

The field list is automatically populated with the fields deduced from the data file.



Name: Arrests

Fields:

Name	Display as	Type	Function
CB	CB	String	id ID
ArrestDate	Arrest date	Timestamp	Timestamp
Longitude	Longitude	Floating point number	Longitude
Latitude	Latitude	Floating point number	Latitude
LastName	Last name	String	
FirstName	First name	String	
Age	Age	32 bit integer	
Sex	Sex	String	
Race	Race	String	
ArrestDescription	Arrest description	String	
ArrestAddress	Arrest address	String	
CrimeType	Crime type	String	
BirthDate	Birth date	Timestamp	
ScarsAndMarks	Scars and marks	String	
Mugshot	Mugshot	Binary - file	

2 Check the **Type** and **Function** of each field and fix any mistakes.

CAUTION: The system can generate the field list quickly, but some data types might be recognized incorrectly. The *Binary - file* data type can be mistaken for a string, and a timestamp can be mistaken for an integer or a string. Pay attention to the functions; they are more error-prone from automatic field population.

3. Go through the **Display as** column and enter more user-friendly display names.

   By default, the display names are copied from the field names.
4. Review the list and add or delete fields as needed.

   CAUTION: If you change the number of fields or their sequence, you might not be able to import data from the file you used to create the field list.
5. When you are finished, click **Create**.

The suggested presentation of the data is displayed.

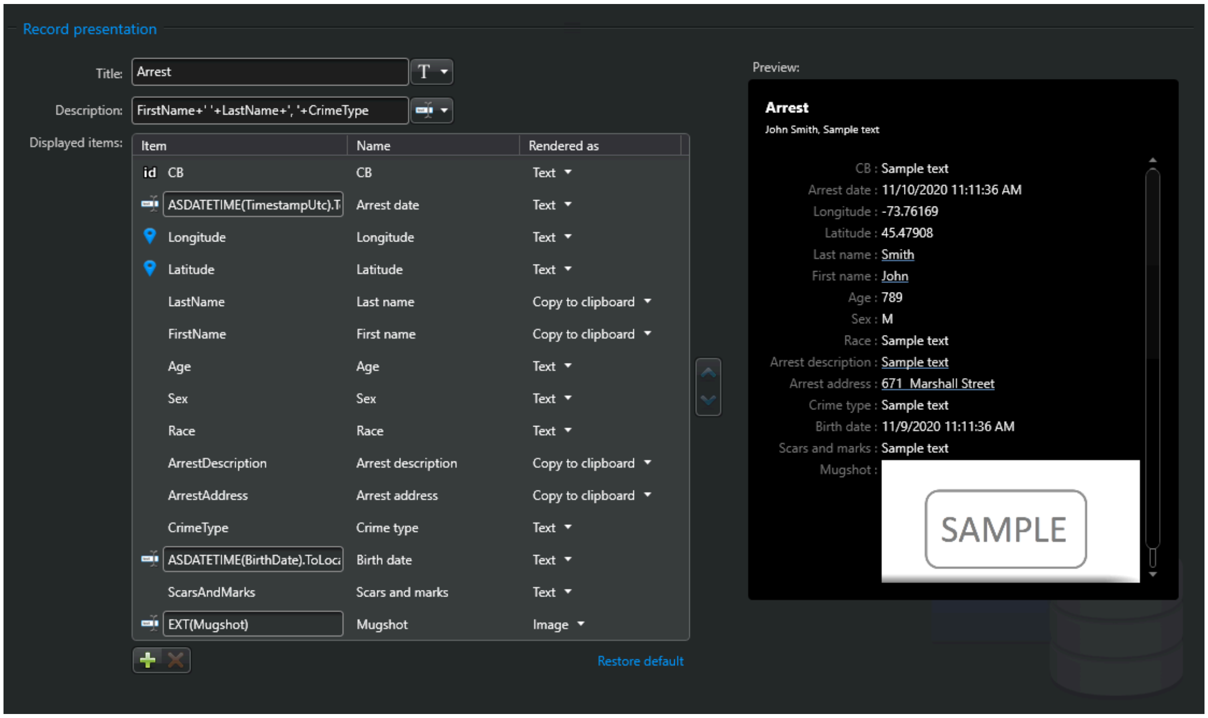
Configuring the record display properties

You can configure how the fields in your record type are presented when a record is displayed in a tile or in the information bubble when you click a record on a map.

What you should know

After you define your record format, a default presentation is suggested. The **Displayed items** list should not be confused with the field list defined for your record type. The former is a list of items to display in the information bubble used to show a specific data record. Each displayed item can be a field from your record type or a custom expression.

A preview of the information bubble is shown to the right of the displayed item list.



Record presentation

Title: Arrest

Description: FirstName+' '+LastName+', '+CrimeType

Displayed items:

Item	Name	Rendered as
id CB	CB	Text
ASDATETIME(TimestampUtc).T	Arrest date	Text
Longitude	Longitude	Text
Latitude	Latitude	Text
LastName	Last name	Copy to clipboard
FirstName	First name	Copy to clipboard
Age	Age	Text
Sex	Sex	Text
Race	Race	Text
ArrestDescription	Arrest description	Copy to clipboard
ArrestAddress	Arrest address	Copy to clipboard
CrimeType	Crime type	Text
ASDATETIME(BirthDate).ToLoc	Birth date	Text
ScarsAndMarks	Scars and marks	Text
EXT(Mugshot)	Mugshot	Image

Restore default

Preview:

Arrest

John Smith, Sample text

CB : Sample text
Arrest date : 11/10/2020 11:11:36 AM
Longitude : -73.76169
Latitude : 45.47908
Last name : Smith
First name : John
Age : 789
Sex : M
Race : Sample text
Arrest description : Sample text
Arrest address : 671 Marshall Street
Crime type : Sample text
Birth date : 11/9/2020 11:11:36 AM
Scars and marks : Sample text
Mugshot :

To configure the display properties of your record type:

1 In the *Record presentation* section, specify what you want to show as the **Title** and **Description** of the information bubble.

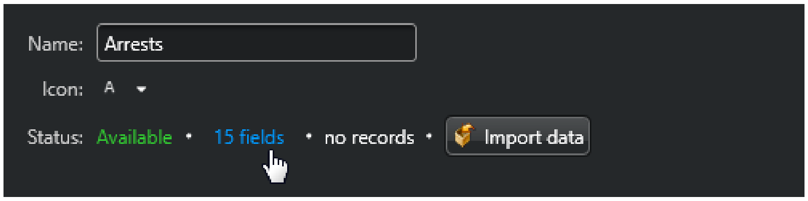
For each property, specify what you want to present as one of the following:

- A plain text
- A field from your record type
- A C# Eval Expression

  For example: FirstName+' '+LastName+', '+CrimeType.

Field names are case-sensitive. If your expression is not resolved in the preview, check the spelling of the field names.

TIP: To view the actual fields of your record type, at the top of the page, in the **Status** row, click the blue link.



Name: Arrests

Icon: A

Status: Available • 15 fields • no records •

2 For each item in the list, specify the following:

- **Item:** Item to display. It is either a field or a custom expression.

  By default, timestamps are converted to strings using the expression ASDATETIME(*{FieldName}*).ToLocalTime().ToString(), which is equivalent to converting the timestamp to your local time zone and then displaying it using your Windows regional settings. The field must first be converted to a *DateTime* with the function ASDATETIME() because timestamps are stored in various formats, and this function converts them all to a common type for display formatting.
- **Name:** Label of the displayed item.
- **Rendered as:** Display format of the item. Select one of the following:
  - **Text:** Displays the item as text.
  - **Image:** Displays the item as an image.
  - **Copy to clipboard:** Displays the item as text with a blue underline. Clicking on the text copies it to the clipboard.
  - **Link:** Displays the item as a hyperlink. Clicking on the hyperlink opens a web page at the desired address.
  - **Entity:** Displays the item as an entity: an icon followed by a name. The icon represents the type and the status of the entity. The item must contain a Security Center entity GUID. Clicking the entity name displays the entity in a tile.
  - **Barcode:** Displays the item as a QR barcode.
  - **Play a sound:** Displays the item as a **Play** button. Clicking the button plays the sound.
  - **Geocoding:** If the item contains a latitude and longitude pair, displays the item as a street address. If the item contains a street address, displays the item as a latitude and longitude pair. This works only if **Geocoding** is enabled on at least one of your map providers.

    TIP: If your record type contains separate latitude and longitude fields, you can combine them into a single item with the expression Latitude+', '+Longitude, and use geocoding to convert it to a street address.

3 Click ➕ to add a new item to the list.

An item can be a field or a custom expression.

4 Select an item and click ✖ to remove it from the list.

5 Validate your choices of display format in the *Preview* window.

6 (Optional) Click **Restore default** to restore the default displayed item list.

After you finish

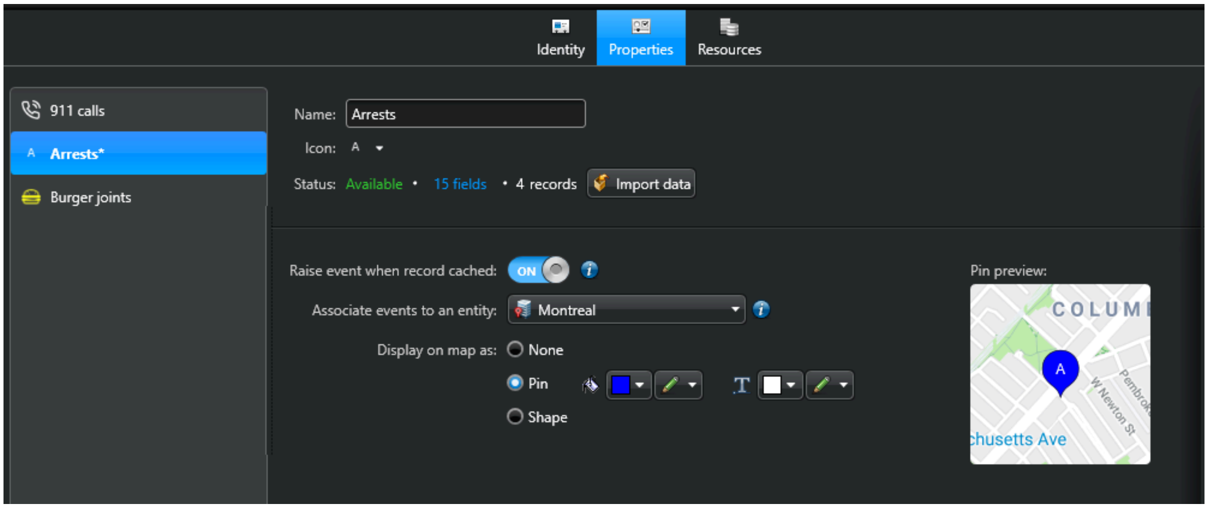
If your record type is georeferenced, configure it as a map object.

Configuring records for map display

If your record type has latitude and longitude fields, you can display its records on maps. A record can be represented as a pin or as a polygon on the map.

What you should know

The default representation of a record on a map is a blue pin identified by the first letter of the record type name. You can change the color of the pin and the image displayed over it. You can also represent a record as a colored shape. Clicking a map object representing a data record opens its information bubble.



Name: Arrests

Icon: A

Status: Available • 15 fields • 4 records

Raise event when record cached: ON

Associate events to an entity: Montreal

Display on map as: ○ None ● Pin ○ Shape

To use the ingested records as map objects:

1. On the *Properties* page of the Record Caching Service role, click the record type you want to configure.
2. Click the pull-down arrow beside *Icon*, and select one of the following:
   - **Select image**: Select an image to display inside the 32 x 40 pixel pin. A PNG image with transparent background works best.
   - **Use expression**: Enter a C# Eval Expression that resolves as a path to an image file. You can use this method to change the pin icon dynamically based on a field value.
   - **Clear**: Restore the default display.

3 (Optional) Turn on the **Raise event when record cached** option to raise the *Record updated* event when new record of this record type is ingested, meaning saved to the *record cache*.

Record caching occurs when you add a record on a map or import multiple records from a flat file. For more information, see "Adding records on maps" in the *Security Center User Guide*.

For the system to raise and event when a record is cached, the following conditions must be met:

- The record type must contain a field assigned to the *Timestamp* function.
- The record type must contain a field assigned to the *Location* function, or a pair of fields assigned to the *Latitude* and *Longitude* functions.
- The record type must be associated to a georeferenced map. The area entity associated to the map is used as the source entity of the event.

NOTE: For a data ingestion event to be displayed on the map when it occurs, at least one *geofence* must be defined on the map.

To add a geofence, add an area entity represented by a polygon to the map. When a new record is ingested, the system checks whether it is found within the boundaries of an area on the map. If it is, a second *Record updated* event is raised, and the area in which the ingested data is found is used as the source entity of that event.

4 Select the appearance of the map object.

- **None:** Do not show the records on maps.
- **Pin:** Show the records as pins. You can choose the background and foreground colors of the pin.
- **Shape:** Show the records as polygons. The polygon must be defined as a Well-Known-Text (WKT) object.

  You can specify the shape as any of the following:

  - A record field containing a WKT object.
  - A static WKT object. You can use Wicket or a similar tool to generate the WKT object.
  - A C# Eval Expression that resolves as a WKT object.

  NOTE: The WKT object is only used for drawing purpose. It does not determine the location of the record on the map. The *Location* field does. Only the location of the record is used for geofencing.

5 To set a color, do one of the following:

- Click **Constant** (✎), and then click the color picker and select a static color.
- Click **Properties** () and select a field containing a color code. We support the most common color codes, from friendly names, such as "Red", "Green", and "Blue", to 6-char and 8-char hexadecimal code codes. For example, "#FF0000FF" for blue.
- Click **Custom expression** () and enter a C# Eval Expression that resolves to a color code.

Related Topics

Adding areas to your maps on page 338

Importing external data from flat files

You can import the records contained in a flat file into Security Center through a *record type*.

Before you begin

- Create a record type that matches the format used in your data file.
- An administrator must grant you the privilege associated with the record type through which you want to import data.

What you should know

The Record Caching Service accepts the following file types:

- **JSON:** JavaScript Object Notation.
- **BSON:** Binary JSON.
- **CSV:** Comma-separated values.
- **TSV:** Tab-separated values.
- **SSV:** Semi-colon-separated values.
- **GPX:** GPS Exchange Format.
- **KML, KMZ:** Keyhole Markup Language.

IMPORTANT: Note the following requirements:

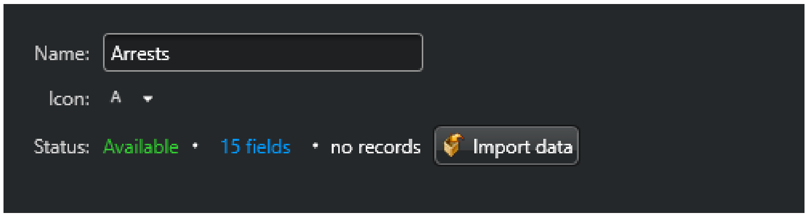
- The first row of CSV, TSV, and SSV files is ignored. It is assumed to be a header row.
- With JSON files, the names and types of the fields defined in your record type must match the names and types of the fields found in the data file. The order of the fields is not important.
- With all other types of files, the order and type of the fields defined in your record type must match the order and types of the fields found in the data file. The field names are not important.

To import external data from a flat file:

1 Open the *System* task and click the **Roles** view.

2 Select the Record Caching Service role that manages the record type you want to import data from, and click the **Properties** tab.

3 Select the record type that matches the format of the data file you want to import and click **Import data**.



Name: Arrests

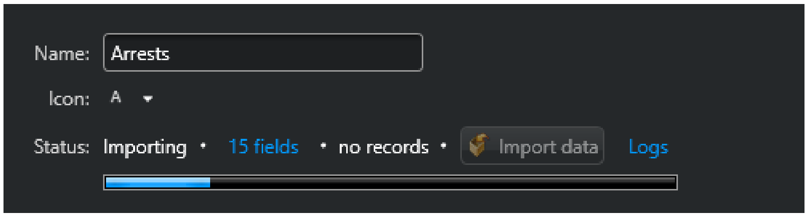
Icon: A

Status: Available • 15 fields • no records

A file browser opens.

4 Select the file you want to import and click **Open**.

A progress bar is shown. Depending on the size of your data file, this might take a while.



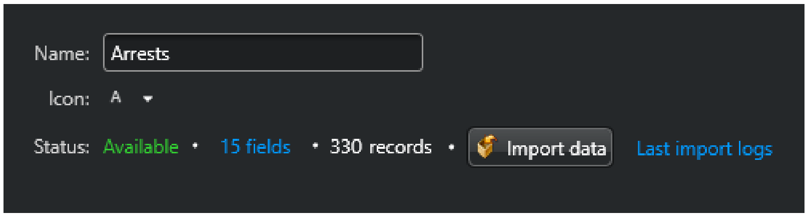
Name: Arrests

Icon: A

Status: Importing • 15 fields • no records

5 Click **Logs** to view the status of the current import operation.

After the import is complete, the total number of records in your record type is updated.



Name: Arrests

Icon: A ▾

Status: Available • 15 fields • 330 records • Import data Last import logs

6 Click **Last import logs** to view your last import operation logs.

The logs are replaced at every new import operation.

7 If your record type is configured to raise events on ingestion, open Security Desk and do one of the following:

- Open the *Monitoring* task to view the events corresponding to the ingested data items.

  If your record type is georeferenced, switch to map view to view the events on a map.
- Open the *Maps* task to view the events that fall within the areas (geofences) defined on the map.
- Open the *Unified report* task to query the ingested data using specific criteria.

For more information, see "Investigating record types" in the *Security Center User Guide*.

12

Federation™

This section includes the following topics:

About the Federation™ feature

The Federation™ feature joins multiple, independent Genetec™ IP security systems into a single virtual system. With this feature, users on the central Security Center system can view and control entities that belong to remote systems.

For a list of Security Center and Omnicast™ versions you can federate in this release, see the *Security Center Release Notes.*

For a list of available federated events, refer to the *Properties* page of the corresponding Federation™ role in Config Tool.

Related Topics

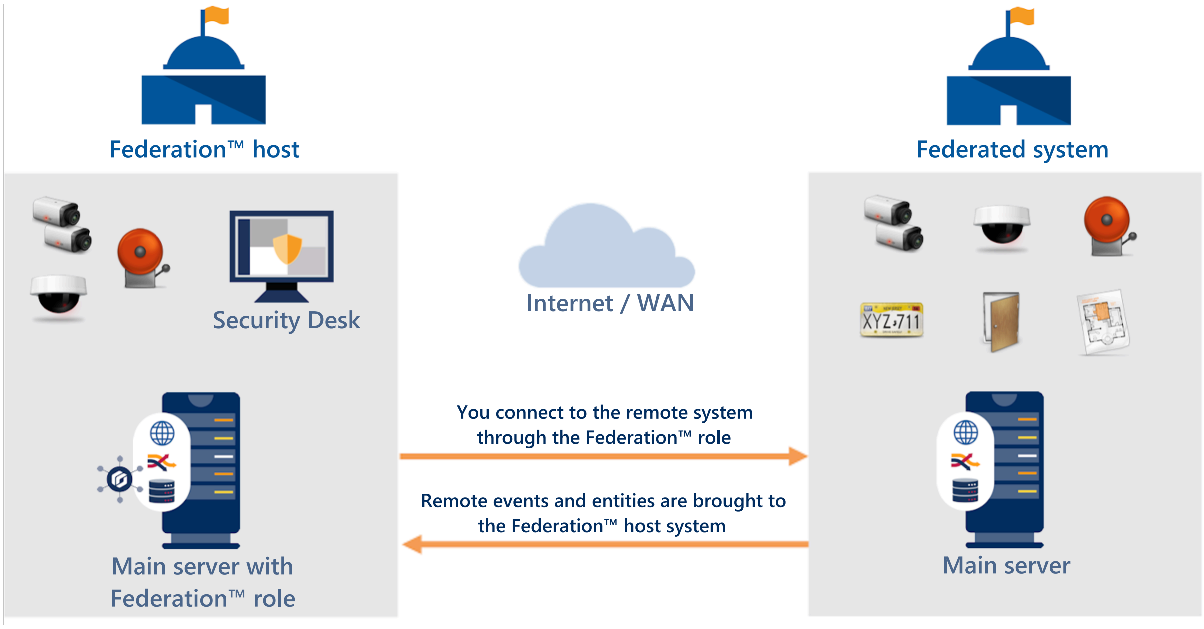
Differences between Federation™ and GCM on page 895

What is Security Center Federation™?

With Security Center Federation™, you can connect multiple Security Center systems into a single virtual system. Users on the central Security Center system can access entities that belong to the remote systems.

How Security Center Federation™ works

You view, monitor, and control remote entities from a central system called the *Federation™ host*. On the Federation™ host system, you create a Security Center Federation™ role for each independent system that you want to federate. The role connects the remote system to the Federation™ host.


Federation™ host
Federated system
Security Desk
Internet / WAN
XYZ·711
You connect to the remote system through the Federation™ role
Remote events and entities are brought to the Federation™ host system
Main server with Federation™ role
Main server

Security Center Federation™ in a hosted system

When the Security Center Federation™ role runs in a hosted system in the cloud, we recommend using *reverse tunneling*. For more information on running the Federation™ host in the cloud, see "Setting up a Security Center Federation™ in a hosted system" topic in the *Cloud-Hosted Security Center SaaS Edition Deployment Guide*.

What is Omnicast Federation?

With Omnicast™ Federation™, you can connect multiple Omnicast 4.x systems into a single virtual system. Users on the central Security Center system can access entities that belong to the remote systems.

NOTE: In Security Center 5.11.3.0 and later, Omnicast Federation is not supported and the role is in a permanent warning state.

How Omnicast Federation works

You view, monitor, and control remote entities from a central system called the *Federation™ host*. On the Federation host system, you create an Omnicast Federation role for each independent Omnicast 4.x system that you want to federate. The role connects the remote system to the Federation host.

NOTE: Omnicast 4.8 has reached End of Life. For more information, see the Genetec™ Product Lifecycle page.

Limitations with Omnicast Federation

Federating an Omnicast system has the following limitations:

- Some playback capabilities are not supported on federated cameras. Smooth reverse playback is not available and the rewind speed is limited to -10x, -20x, -40x, and -100x.
- Camera sequences are federated, but they behave as a single camera on the Federation host. This means that the users on the Federation host cannot unpack nor stop the camera cycling on camera sequences () federated from Omnicast.
- Sites () are federated as areas ( ) in Security Center.
- Sites with a Map (URL) property ( ) are federated as areas ( ) with a web page tile plugin attached.

About federated entities

A federated entity is any entity that is imported from an independent system through one of the Federation™ roles.

Federated entities do not belong to your local system but you can view and manipulate them in the Federation™ host system. Starting in Security Center 5.8 GA, you can also change the native settings of federated entities using the *Remote configuration* task.

In Config Tool, federated entities have a yellow arrow superimposed on their entity icon (for example, here is a federated alarm entity:). In Security Desk, the yellow arrow is not displayed on federated entities.

What entities are federated in Security Center

The following entities and related events can be federated from a remote system:

Component	Entities
Video	• Cameras • Camera sequences • Virtual cameras (Omnicast™ Federation™ only)
Access control	• Access control units • Doors (Security Center Federation™ only) • Elevators (Security Center Federation™ only) • Cardholders (Security Center Federation™ only) • Cardholder groups • Visitors (Security Center Federation™ only) • Credentials (Security Center Federation™ only) • Intrusion detection units • Intrusion detection areas
ALPR	• ALPR units • Genetec Patroller™ units
General	• Alarms • Areas • Cash registers • Networks • Maps • Zones • Output behaviors • Custom events • Records and *Record updated* events **Limitation:** ArcGIS maps are only federated in version 5.7 and later. If you federate an older system (5.6 and earlier) that federates a system with an ArcGIS map, you cannot see the ArcGIS map in your system.

What you can do with federated entities in Security Desk

You can perform the following operations on federated entities in Security Desk:

- View live or playback video from federated cameras.
- Add bookmarks, start and stop recording, and export video from federated cameras.
- Control federated PTZ cameras, taking into account the user level of the local users on the Federation™ host, when conflicts arise between federating users.
- Send specific commands to federated cameras, such as arm and disarm a camera for video analytics.
- Switch cameras on CCTV matrices using *virtual cameras* federated from Omnicast 4.x.
- View, start and stop cycling, pack and unpack federated camera sequences.
- Restrict users from viewing a segment or entire video capture by blocking the camera.
- Receive, acknowledge, snooze, forward, start and stop cycling, pack and unpack federated alarms.
- View and control federated tile plugins.
- Unlock federated doors of an area.
- Temporarily override the schedule of a federated door.
- Set a federated door in maintenance mode.
- Shunt a federated door's reader and inputs.
- Change a federated area's minimum security clearance on threat level.
- Sound and silence reader buzzers.
- Monitor federated input and output states on maps. Fast changing output states, such as blinking, might not be displayed properly.
- Monitor federated devices in the *System status* task.
- Monitor the people count in federated areas. For more information, see About people counting through Federation™ on page 274.
- Sending federated output behaviors to federated outputs, if both belong to the same system.
- Arm and disarm federated intrusion detection areas.
- Arm and disarm federated zones.
- View federated records and record types in *Unified report* task.

What you can configure with federated entities

You can make the following changes to federated entities on the Federation™ host:

- Assign logical IDs to federated entities. The logical ID is a local attribute associated with the federated entity to identify it uniquely within the Federation™.
- Assign local entity names to federated entities. The original entity names remain visible in Config Tool for troubleshooting purposes.
- Update the custom fields associated to federated entities. Custom fields are local to the Federation™ host.
- Choose what events you want to receive from the federated system. Based on these events, you can define *event-to-actions* for federated entities. The actions can either be run on the Federation™ host or on the federated system.
- View their activity and audit trail reports in the *report* pane.
- Control the visibility of the federated entities to your local users using partitions.
- Configure visual tracking for cameras federated from Omnicast systems.
- Use federated entities to configure local entities, such as attaching federated cameras to local entities, or using them to define local alarms and camera sequences.
- Assign local cameras to federated doors to display camera feeds in Security Desk. This relationship remains local; the camera is not shared with the federated system.

Limitations of federated entities

You cannot do the following with federated entities:

- You cannot view the custom fields defined on the remote system. Custom fields are not federated.
- Actions performed on federated entities, such as arming a zone or adding a bookmark to a camera, are not logged in the activity trails of the federated system.

  NOTE: There is one exception to this limitation. *Export video* actions are logged in both activity trails. On the Federation™ host, the user who performed the activity is logged as the *initiator*. On the federated system, the *initiator* is the Federation™ user, and the user who performed the activity on the Federation™ host is logged as the *original initiator*. Remote activity logging only works if the federated system is running Security Center 5.7 or later.
- You cannot add records to federated record types on maps.
- Visitors are only federated so that people counting can work for federated areas. In the *Visitor management* task, federated visitor cannot be checked in, checked out, deleted, or modified, except for adding credentials. Visitors on systems earlier than 5.10.2.0 cannot be federated.

  NOTE: If you do not want to see in the *Visitor management* task all federated visitors that are still checked in, you can move the visitors to partitions that are not synchronized through Federation™.

Exceptions for federated alarms

Not all alarm properties are federated. Most properties pertaining to the alarm display in Security Desk must be configured locally on the Federation™ host.

The exceptions for federated alarms are the following:

- The alarm schedule follows the original configuration of the remote system. Because schedule entities are not federated, the default schedule *Always* is shown instead.
- Alarm priority:
  - Omnicast: Original value is not federated. You can configure it (default=1) locally on the Federation™ host.
  - Security Center: Original value is federated and cannot be modified.
- Reactivation threshold is an inherent property of the alarm and cannot be modified.
- Entity cycling is a local property to the Federation™ host. You can change its setting without affecting the federated system.
- Automatic acknowledgment is an inherent property of the alarm and cannot be modified.
- Create an incident on acknowledgment is a local property to the Federation™ host. You can change its setting without affecting the federated system.
- Automatic video recording is an inherent property of the alarm and cannot be modified.
- Protect recorded video is an inherent property of the alarm and cannot be modified.
- Video display is a local property to the Federation™ host. You can change its setting without affecting the federated system.
- Alarm procedure (URL):
  - Omnicast: Original value is not federated. You can configure it locally on the Federation™ host.
  - Security Center: Original value is federated and cannot be modified.
- Entities that are associated to the federated alarm (cameras, doors, and so on) are inherent properties of the alarm and cannot be modified.
- Alarm recipients must always be configured locally for the Federation™ host.

Caution about federated record types

The Federation™ host creates a privilege for each federated record type, just as it does for local record types. The privilege is named after the record type. If a federated record type has the same name as a local record type, it would be impossible to differentiate which privilege is for the local record type and which privilege is for the federated record type.

Related Topics

Custom card formats on page 882

Importing security groups from an Active Directory on page 481

About people counting through Federation™

You can monitor the people count and track federated cardholders and visitors in federated areas, using various tasks, reports, and maps.

The following options related to people counting are supported:

- The **Clear all** and **Remove from area** buttons in the *People counting* task and maps.
- The *Reset area people count* action for event-to-actions.

You can view people count for federated areas in the following tasks:

- *People counting*
- *System status*
- *Area presence*
- *Maps* and any other task that can display maps

Requirements

This feature requires Security Center 5.10.2.0 and later. The people count state of systems earlier than 5.10.2.0 is not reported through the Security Center Federation™ role.

Example: Federated visitor activity cannot be properly tracked from a 5.10.0.0 Security Desk connected to a 5.10.2.0 system.

The following user privileges are required to view the people count and use the *People counting* task:

- Task privileges > Operation > People counting
- Action privileges > Areas > Modify people count

How it works

People count and visitor information is sent through the Security Center Federation™ role. Federated areas and local areas of each system do not communicate. This means that a federated cardholder can simultaneously be in a federated area at site B and in a local area at site A because the cardholder is not removed from one area when they badge at the other.

Setting up a Security Center Federation™

To federate one remote Security Center system using Security Center Federation™, a user account on the remote system and a Federation™ role must be created and configured for the Federation™ host.

What you should know

This is a 2-step process, with one part carried out on the federated system and the other part on the Federation™ host.

To set up a Security Center Federation™:

1. The federated system administrator creates and configures the Federation™ user.
2. The Federation host administrator creates and configures the Federation™ role.

Related Topics

Requirements for large Federation™ systems on page 284

Using default Security Desk settings to view federated cameras on page 280

Configuring the Media Router role on page 597

Creating and configuring a Security Center Federation™ user

To allow an external Security Center system to remotely access your system and the entities that belong to it, you must first create a local user account for the Security Center Federation™ host.

To create and configure a Security Center Federation™ user:

1. Create the Federation™ user.

   NOTE: Give the Federation™ user a descriptive name. For example, instead of using *federation_1*, use *PoliceDepartment* or *CompanyHeadquarters*. That way, if multiple hosts federate your system, it would be easy for you to tell which Federation™ host is connected to your system.
2. Configure the Federation™ user.
3. Assign the necessary privileges.

   NOTE: The rights and privileges of the Federation™ user determine what the users on the Federation™ host can see and do on the federated system. The Federation™ user must have the application privilege *Federation*™. Any other access rights and privileges depend on what you want to let the Federation™ user do on your system. The Federation™ user should not be a member of the Administrators group, as it increases the security risks if ever the associated credentials are compromised. This could lead to a malicious user taking control of your system. Instead, you should only grant the privileges that the Federation™ host requires to perform their operations.

After you finish

Provide the Security Center Federation™ host with the credentials created for the Federation™ user. The Federation™ host will use the credentials to create the Federation™ role and remotely connect to your system.

Related Topics

Creating users on page 433

Configuring user settings on page 434

Assigning privileges to users on page 441

Creating and configuring a Security Center Federation™ role

To connect to a remote Security Center system using Security Center Federation™, you must create and configure a Security Center Federation™ role on your system, using the credentials for your Federation user.

Before you begin

Ensure you have the username and password of the Federation™ user, created for you by the administrator of the system you want to federate. The rights and privileges of the Federation™ user determine what the users on your system can see and do on the federated system. The Federation™ user must have the application privilege *Federation*™ and any other privilege you need to perform your task.

To set up a Security Center Federation™:

1 Open the *System* task and click the **Roles** view.

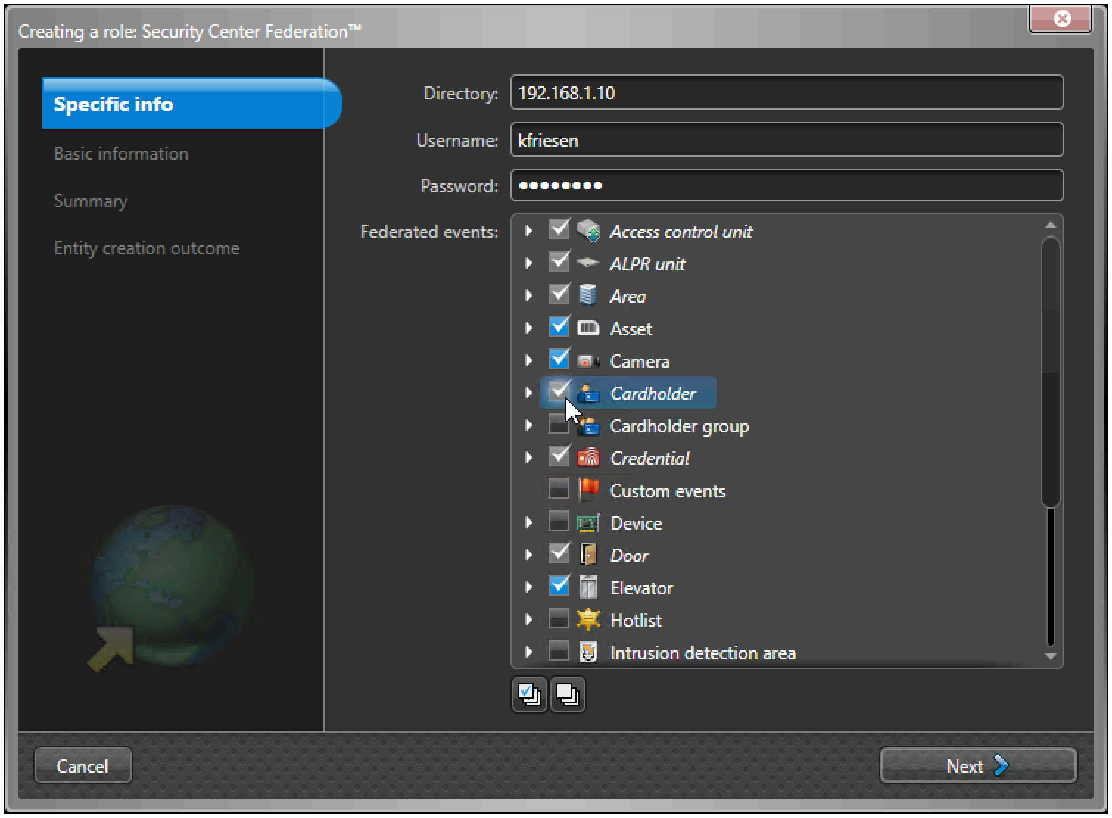
2 Click **Add an entity** (➕), and click **Security Center Federation**™.

3 In the **Directory** field, enter the name or IP address of the remote Security Center Directory.

4 Enter the username and password for the Federation™ user, that the Federation™ role is going to use to log on to the remote Security Center system.

BEST PRACTICE: Give the Federation™ user a descriptive name. For example, instead of using *federation_1*, use *PoliceDepartment* or *Headquarter*. That way, if multiple hosts federate the same system, it's easy for the federated system to tell which Federation™ host is connected to their system. Ensure that **Use secure communication** (on by default) is enabled in the Media Router on both systems. This will ensure a secure communication and will allow *Live/Playback streaming requested from Federation* to be logged in the *Activity trails* report, because they cannot be logged if **Use secure communication** is disabled. This applies to 5.11.1.0 or higher.

5 In the *Federated events* section, select the events that you want to receive from the federated system, and click **Next**.



Directory: 192.168.1.10
Username: kfriesen
Password: ••••••••
Federated events:
- ☑ *Access control unit*
- ☑ *ALPR unit*
- ☑ *Area*
- ☑ Asset
- ☑ Camera
- ☑ *Cardholder*
- □ Cardholder group
- ☑ *Credential*
- □ Custom events
- □ Device
- ☑ *Door*
- ☑ Elevator
- □ Hotlist
- □ Intrusion detection area

6 On the *Basic information* page, enter a name and description for the role.

7 Select a **Partition** this role is a member of, and click **Next**.

All federated entities are created in the partition you select. Only users that are part of the partition can view or modify those entities.

8 Click **Next** > **Create** > **Close**.

9 Select the new Federation™ role (🌐), and click the **Properties** tab.

The connection status should say **Synchronizing entities**, or **Connected**.

10 Decide what happens if the connection between the Security Center Federation™ role and the federated Security Center Directory is interrupted by configuring the following options:

- **Resilient connection:** When this option is turned on (default=OFF), the Federation™ role attempts to reconnect to the federated Security Center Directory server after a connection interruption. After a specified period of attempting to reconnect, the connection is considered lost and the role goes into a warning state.

  NOTE: Activating Resilient connection is highly recommended for remote systems that might have an unstable connection to the cloud.
- **Reconnection timeout:** Specify the number of seconds that the Federation™ role attempts to reconnect to the Directory before the connection is considered lost.

11 Configure the additional options for Security Center Federation™:

- **Forward Directory reports:** When this option is turned on (default=OFF), you can view user activities (viewing cameras, activating the PTZ, and so on) and configuration changes performed at the federated site from the *Activity trails* and *Audit trails* reports on the Federation™ host, as long as the Federation™ user has the privileges and access rights to view them. You can also view the federated units in the *Hardware inventory* task.

  IMPORTANT: Forward Directory reports is only supported with 5.8 systems and higher (including federations). This means that if your federated system is 5.7 and lower, the Forward Directory reports option is grayed out and not available.
- **Default live stream:** Default video stream used for viewing live video from federated Security Center cameras (default=**Remote**).

  If your workstation does not require specific video stream settings for Federation™, you can use the default stream settings from Security Desk instead.
- **Enable playback requests:** When this option is turned on, users can view playback video from federated Security Center cameras.
- **Federate alarms:** When this option is turned on, alarms are received from the federated Security Center system.
- **Federate custom icons:** When this option is turned on, federated entities share custom icons with the Federation™ host. This means that entity icons in the Federation™ host appear identical to the federated system. It can take a few minutes to synchronize the custom icons.

12 Click **Apply**.

13 If necessary, change the default multicast addresses used by the Media Router for local and federated streams.

After you finish

In the *Area view* task, expand the Security Center Federation™ role (🌐) and make sure all the federated entities were imported by the role.

The entity hierarchy corresponds to the area view on the federated remote system.

Related Topics

Changing entities' icons on page 78

Setting up an Omnicast Federation

To federate one remote Omnicast™ system using Omnicast Federation™, you must create and configure an Omnicast Federation role.

Before you begin

Install the Omnicast Compatibility Pack corresponding to the version of the Omnicast system that you plan to federate on the following servers and workstations:

- On the server where the Federation role is to be hosted.
- On the client workstation where Config Tool is running.
- On all secondary servers that you plan to assign to the Federation role.
- On all Security Desk workstations viewing the federated cameras.

What you should know

- Omnicast 4.8 has reached End of Life. For more information, see the Genetec™ Product Lifecycle page.
- In Security Center 5.11.3.0 and later, Omnicast Federation is not supported and the role is in a permanent warning state.

To set up an Omnicast Federation:

1 Open the *System* task and click the **Roles** view.

2 Click **Add an entity** (➕), and click **Omnicast Federation**.

3 In the **Directory** field, enter the name of the Omnicast Gateway connecting you to the remote Omnicast system.

4 Enter the username and password that the Federation role is going to use to log on to the remote Omnicast system.

The rights and privileges of that user determine what the users on the Federation host can see and do on the federated system.

5 From the **Version** list, select the version of the remote Omnicast system, and click **Next**.

This drop-down list only shows the Omnicast versions for which a compatibility pack is installed.

6 In the **Federated events** section, select the events that you want to receive from the federated system, and click **Next**.

Events are necessary to monitor the federated entities in Security Desk and to configure event-to-actions for the federated entities.

7 On the *Basic information* page, enter a name and description for the role.

8 Select a **Partition** this role is a member of, and click **Next**.

All federated entities are created in the partition that you select. Only users that are part of the partition can view or modify those entities.

9 Click **Next** > **Create** > **Close**.

10 Select the new Federation role (●), and click the **Properties** tab.

The connection status should say **Synchronizing entities**, or **Connected**.

11 Configure the options for Omnicast Federation:

- **Default live stream:** Default video stream used for viewing live video from federated Omnicast cameras (default=**Remote**).

If your workstation does not require specific video stream settings for Federation™, you can use the default stream settings from Security Desk instead.

- **Enable playback requests:** When this option is turned on, users can view playback video from federated Omnicast cameras.
- **Federate alarms:** When this option is turned on, alarms are received from the federated Omnicast system.

12 Click **Apply**.

After you finish

In the *Area view* task, expand the Omnicast Federation role () and make sure all the federated entities were imported by the role.

The entity hierarchy corresponds to the area view on the federated remote system.

Related Topics

Requirements for large Federation™ systems on page 284

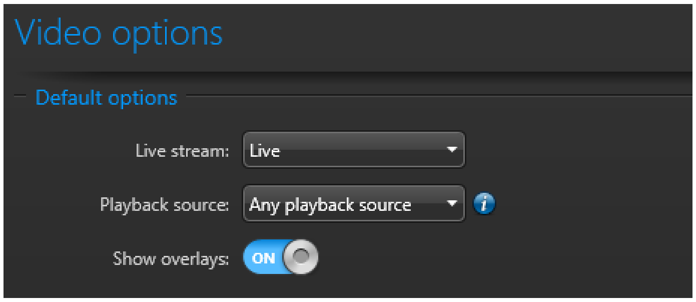
Using default Security Desk settings to view federated cameras on page 280

Using default Security Desk settings to view federated cameras

When requesting live video from federated cameras, you can configure a workstation to use the default video stream settings from Security Desk instead of using the settings from the Federation™ role.

What you should know

When users request live video from a local camera, the default stream settings are taken from the video options in Security Desk (default=**Live**).



Video options

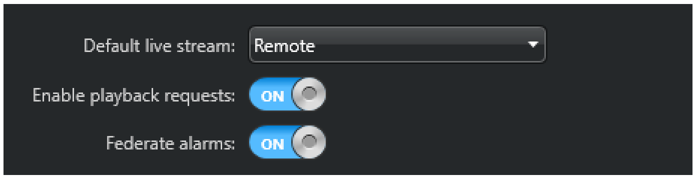
Default options

Live stream: Live

Playback source: Any playback source

Show overlays: ON

When users request live video from a federated camera, the default stream settings are taken from the properties of the Federation™ role (default=**Remote**). The remote stream is used because federated cameras are often used in a low bandwidth segment of the network.



Default live stream: Remote

Enable playback requests: ON

Federate alarms: ON

To overwrite the Federation™ role settings with the Security Desk settings for federated cameras:

1 On the workstation where you want to change the default behavior, back up the *GeneralSettings.gconfig* file by copying it to another folder.

The file is found in the Security Center installation folder (*C:\Program Files (x86)\Genetec Security Center 5.11\ConfigurationFiles*).

CAUTION: Only modify a *.gconfig* file if you are sure that the changes are valid. Incorrect code in a *.gconfig* file can cause issues on your system or cause your system to go offline.

2 Open the *GeneralSettings.gconfig* in a text editor and add the following line of code in the `<configuration>` section:

```
<streamUsage bypassFederationDefaultStream="true"/>
```

3 Save your changes and restart Security Desk.

Configuring federated entities

You can configure federated entities like local entities using the *Remote configuration* task.

What you should know

- You can only configure entities federated from remote systems running Security Center 5.8 GA and later from the Federation™ host.
- You must have the *Remote configuration* privilege to use the *Remote configuration* task.
- You must have Security Center Client that corresponds to the version of the remote system installed on the computer running the *Remote configuration* task.
- You cannot update the software components of the federated system from the *Remote configuration* task.

To configure a federated entity:

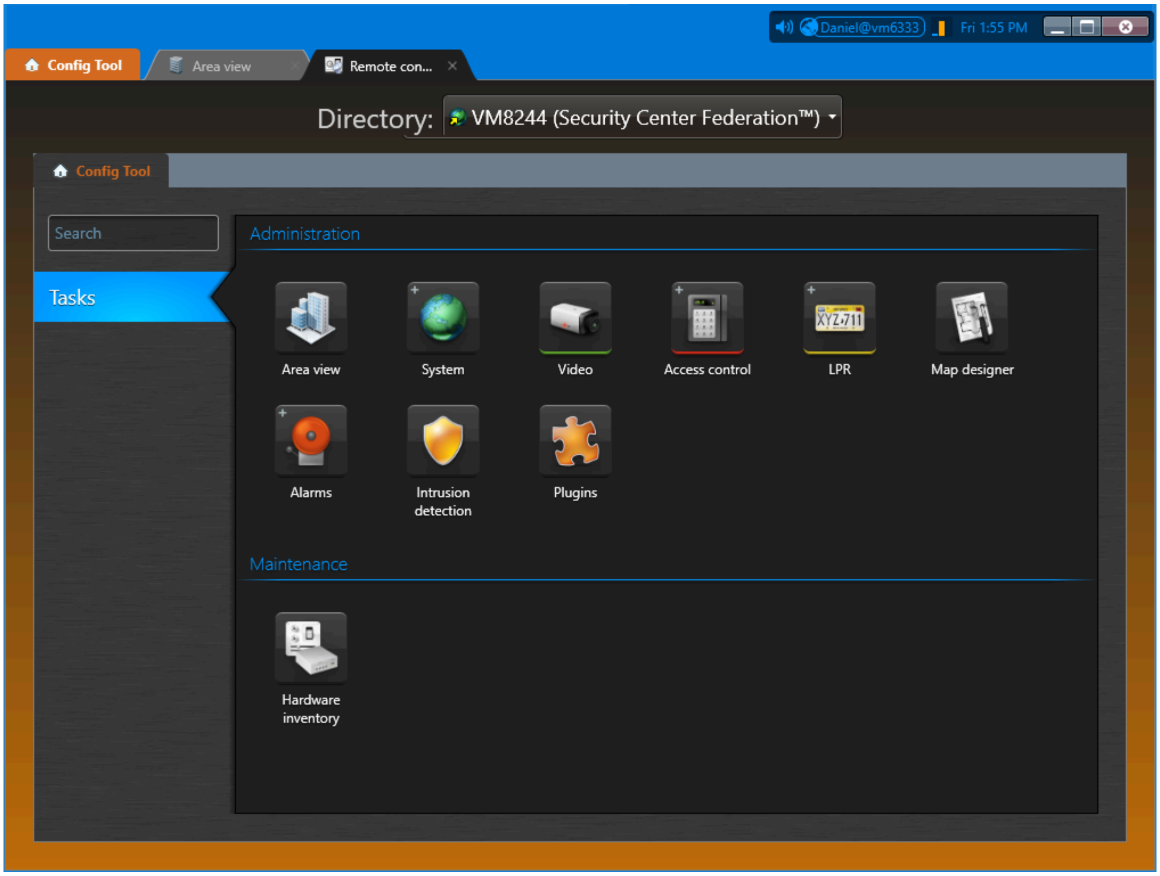
1 Do one of the following:

- From the *Area view* task, right-click a federated entity and click **Configure entity** ().

  The *Remote configuration* task opens automatically on the configuration pages of the selected entity.

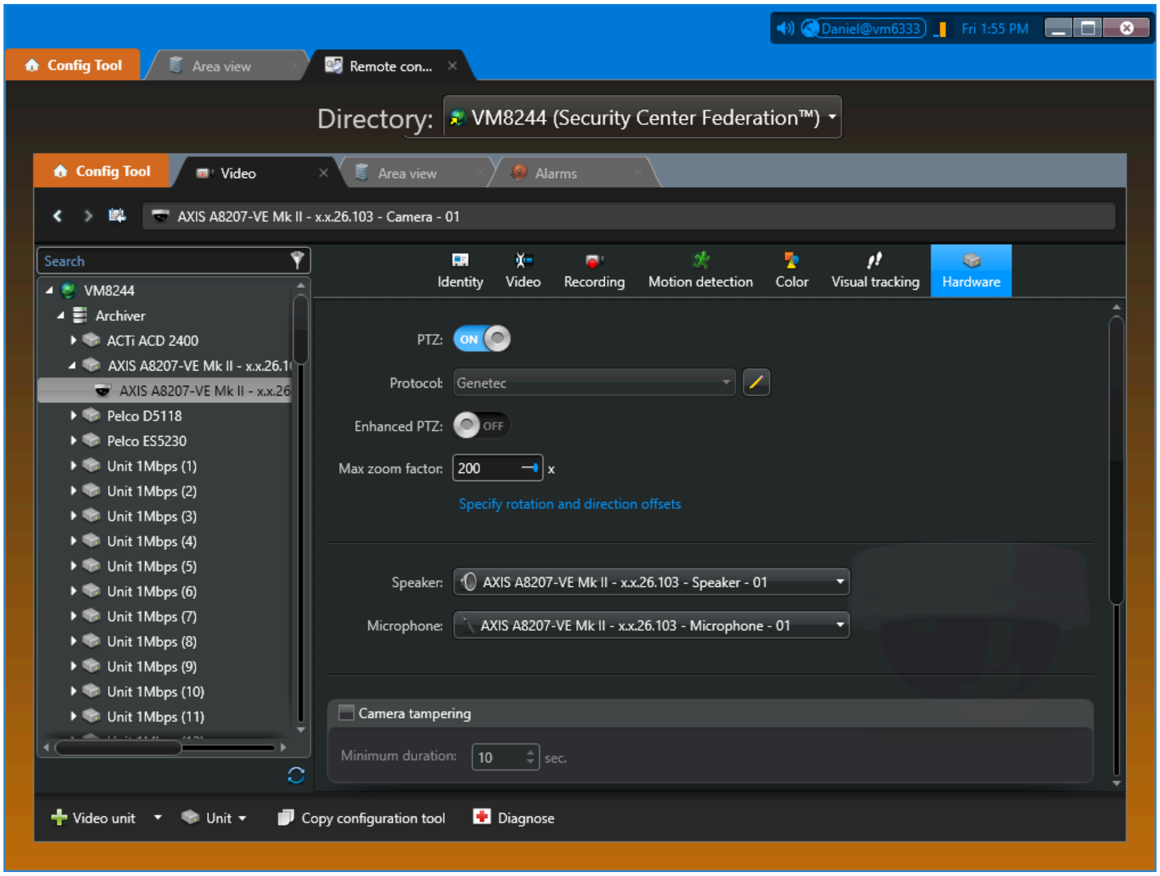
  If the *Remote configuration* task was connected to different federated system, you are asked if you want to save the open tasks. Click **Save** if you want the open tasks to be automatically loaded the next time you log on with this user.
- From the Config Tool home page, open the *Remote configuration* task and select the federated Directory () you want to connect to.

A remote Config Tool session opens inside the task workspace on the federated remote system.



Directory: VM8244 (Security Center Federation™)

The remote Config Tool works exactly like your local Config Tool. The tasks you can open and the entities you can view and modify depend on the access rights and privileges granted to the Federation™ user on the remote system.



Directory: VM8244 (Security Center Federation™)

PTZ: ON

Protocol: Genetec

Enhanced PTZ: OFF

Max zoom factor: 200 x

Speaker: AXIS A8207-VE Mk II - x.x.26.103 - Speaker - 01

Microphone: AXIS A8207-VE Mk II - x.x.26.103 - Microphone - 01

□ Camera tampering

Minimum duration: 10 sec.

2 To connect to a different remote system, click the **Directory** drop-down list at the top of the task workspace, and select another federated Directory (🌐).

Requirements for large Federation™ systems

On a large scale deployment, Security Center can federate thousands of independent remote systems. However, there are hardware and software limitations you must consider.

The number of Federation™ roles you can host on a single server depends on the following:

- Type of Federation™ roles you are hosting.
- Number of Federation™ roles you are hosting.
- Type of computer running the Genetec™ Server service. For the minimum, recommended, and high-performance requirements for client workstations, see the *Security Center System Requirements*.

Federation™ role groups

When a large number of Federation™ roles are hosted on the same server, they must be divided into multiple *role groups*. All roles belonging to the same role group are executed by the same process on the same machine. There is a limit to the number of roles a single process can handle.

The following table helps determine how many role groups you need on your server.

NOTE: These calculations assume that each federated system (Omnicast™ or Security Center system) has 150 cameras or doors.

Role type	Number of Federation™ roles supported on a single server		
	Single role group (Any hardware profile)	**Multiple role groups(Low and Medium capacity hardware profiles)**	**Multiple role groups (High capacity hardware profile)**
Omnicast™ Federation™	40	Contact Genetec™ Technical Assistance.	100
Security Center Federation™	100	Contact Genetec Technical Assistance.	500

If a single role group can have up to 40 Omnicast Federation™ roles, a high capacity computer hosting 100 Omnicast Federation™ roles requires three separate role groups. A high capacity computer hosting 500 Security Center Federation™ roles requires five separate role groups.

Example

You want to federate 250 Omnicastsites, using one Omnicast Federation™ role per site. You can divide your sites as follows:

- **Server A:** 40 Omnicast sites (*role group 1*) + 40 Omnicast sites (*role group 2*) + 20 Omnicast sites (*role group 3*) = 100 Omnicast sites.
- **Server B:** 40 Omnicast sites (*role group 1*) + 40 Omnicast sites (*role group 2*) + 20 Omnicast sites (*role group 3*) = 100 Omnicast sites.
- **Server C:** 40 Omnicast sites (*role group 1*) + 10 Omnicast sites (*role group 2*) = 50 Omnicast sites.

Adding Federation™ role groups

If you need to host a large number of Federation™ roles on the same server, you must configure a Federation™ role group.

Before you begin

Determine how many role groups you require for your deployment.

To add a Federation™ role group:

1. Open the *System* task, and click the **Role view**.
2. Select the Federation™ role entity to configure (Security Center or Omnicast™), and click the **Identity** tab.
3. In the **Name** field, type Ctrl+Shift+A.
   The **Advanced settings** section appears at the bottom of the tab.
4. Change the **Role group** name if necessary.
5. Click **Apply**.

13

Maps

This section includes the following topics:

How to work with maps in Security Center

Maps in Security Center enhance situational awareness and system security by enabling users to view and navigate your facilities in real time. They also facilitate the management of cameras, doors, and other entities.

To use maps in Security Center, you must have Plan Manager enabled in your license. To work with your maps in Security Desk, you can use either the *Maps* task, which is dedicated to working with maps, or the generic *Monitoring* task.

NOTE: The Map Manager role replaced the Plan Manager role in Security Center 5.4 GA.

With maps, you can do the following:

- Pan and zoom.
- Navigate through different maps.
- Span a single map across multiple monitors.
- Manage your Security Center entities, such as cameras, doors, zones, and so on.
- Monitor and respond to alarms and events in real time.
- Add local and federated entities.
- Show and hide information about *map objects.*
- View information related to map objects in a text bubble.
- Find entities on maps and see what other entities are nearby.
- Mark points of interest, such as fire exits, first aid kits, and so on.
- Monitor and control cameras, doors, intrusion detection areas, and zones.
- Monitor moving objects, such as patrol vehicles.
- View license plate reads and hits from fixed ALPR cameras.
- Monitor the state of input pins (active, inactive).
- Control the behavior of output relays.
- Run macros.

Configuring the Map Manager role

The Map Manager is the central role that manages all mapping resources in Security Center, including imported map files, external map providers, and KML objects. It acts as the map server for all client applications that require maps and as the *record provider* for all Security Center entities placed on georeferenced maps. The Map Manager role replaced the Plan Manager role in Security Center 5.4 GA. You must configure this role before you can start using maps on your system.

What you should know

The *Map Manager* role is created by default during installation of Security Center, and is assigned to the main server.

To configure the Map Manager role:

1 From the Config Tool home page, open the *System* task, and click the **Roles** view.

2 Select the Map Manager role, and click the **Properties** tab.

3 In the *Map providers* section, connect the Map Manager to third-party map providers.

A map provider is a *Geographic Information System (GIS)* used to create geographic maps. Most of them require a license to use. These systems can be offline or online. The following map providers are supported:

- **BeNomad:** An offline GIS that must be installed on all Security Center client machines.
- **Esri:** An online GIS based on the ArcGIS Runtime SDK for .NET.
- **Bing:** *Bing map*, *Bing hybrid map*, and *Bing satellite map* are online map providers offered by Microsoft.
- **Google:** *Google map*, *Google terrain map*, and *Google satellite map* are online map providers offered by Google.
- **Custom *:** A Tile Map Service (TMS) server, such as one provided by the OpenStreetMap Foundation, can be added as an online map provider.
- **WMS:** A Web Map Service (WMS) server can be added as an online map provider.

The list of map providers also serves as a geocoding priority list. This means that the map provider at the top of the list is the first to be tried as the geocoding provider. If this provider cannot return a result, the next provider in the list is tried.

4 (Optional) In the *Map layers* section, import the KML objects you want to show on your maps.

5 Set the **Cache location** for your maps.

The cache is a folder where the map tiles are stored. When you create maps from images files, the role generates a set of small images, called *map tiles*, for each zoom level at which you need to view the map. The larger the map scale, the more map tiles the role must generate. The default folder is *C:\ProgramData \Security Center\Maps*.

BEST PRACTICE: If you are setting up role failover, set the cache to a location that all servers assigned to the role can reach. If the role cannot reach the configured cache location, it regenerates the map tiles from source file stored in the Directory database, and saves them to the default cache location.

6 In the **Default map** list, select the default map for your system.

The system default map, also known as the global default map, is the map initially loaded for all users when opening the *Maps* task. The global default map can be overridden both at the user group and user levels, where a default map can be configured for each user and group. You can only set the global default map after creating your first map.

7 After all client applications have been upgraded to Security Center 5.9 or later, switch **Backward compatibility OFF**.

Backward compatibility is not required by new installations and is disabled by default. On systems upgraded from Security Center 5.8 or earlier, **Backward compatibility** is automatically switched **ON** to allow client applications that have not been upgraded to work normally.

8 Click **Apply**.

9 If your Security Center license supports *Basic record fusion*, configure the map objects you want to use as *record types*.

   a) Click the **Record fusion** tab.

   b) From the *Use map locations for* list, select the object types you want to use for location correlation.

      The selected object types are registered with the *Record Fusion Service* as record types and can be viewed using the *Records* investigation task. All map objects registered as record types can be filtered on their *Location*, *Name*, *Description*, and *Entity* attributes. For more information, see "Investigating record types" in the *Security Center User Guide*.

   c) In the **Maps** list, add the maps that must be examined by correlation requests.

      You must select at least one map.

   d) Click **Apply**.

Installing the BeNomad mapping solution

If your Security Center license includes BeNomad, the offline maps must be installed before you can use BeNomad to provide map and reverse geocoding information.

Before you begin

After your Security Center license is created, you will receive an email with a *.zip* file containing the BeNomad maps for your geographic location, and a unique *.glic* file containing your BeNomad license information. You need both files to install BeNomad.

What you should know

BeNomad must be installed on all Security Center client machines.

To install BeNomad:

1. Unzip the contents of the BeNomad *.zip* file to your client machine.

   A folder called *BeNomad* is created.
2. Copy the *BeNomad* folder to the main program folder where Security Center is installed.

   The default location of this folder is: *C:\Program Files (x86)\Genetec Security Center 5.11*.
3. Copy the *.glic* license file to the *BeNomad* folder on the client machine.

   The BeNomad map provider is enabled when you start Config Tool.

Connecting Map Manager to a Bing or Google map provider

Before you can create maps based on Microsoft Bing Maps or Google Maps data, you must set up a map provider for the map type you want to use.

Before you begin

Acquire a valid Bing Maps or Google Maps license, and know your license key.

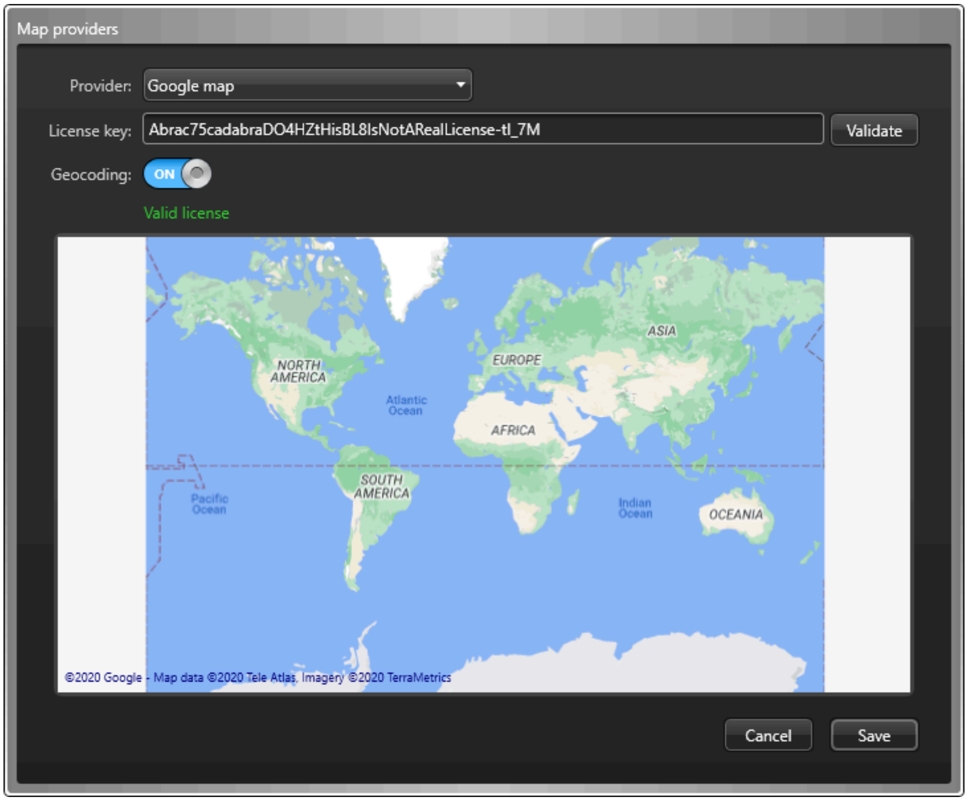
To connect the Map Manager to Bing Maps or Google Maps:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the Map Manager role, and click the **Properties** tab.
3. In the *Map providers* section, click **Add an item** (✚).
4. In the *Map providers* dialog box, select one of the following map types from the **Provider** drop-down list:
   - **Bing map:** General-purpose map.
   - **Bing satellite Map:** Satellite map without labels.
   - **Bing hybrid Map:** Satellite map with labels.
   - **Google map:** General-purpose map.
   - **Google terrain map:** Labeled topographic map with 3D terrain.
   - **Google satellite Map:** Satellite map without labels.

   A preview of the selected map is displayed.
5. In the **License key** field, type the license key and click **Validate**.
   If you entered a correct license key, *Valid license* is shown below the **License key** field.

6 If your license includes geocoding services, turn the **Geocoding** option on.

With this feature enabled, Map Manager can convert a pair of latitude and longitude into a street address and vice versa. You can also search for a street address from the *Maps* task in Security Desk and zoom in to that address on the map.



Map providers

Provider: Google map

License key: Abrac75cadabraDO4HZtHisBL8IsNotARealLicense-tl_7M

Geocoding: ON

Valid license

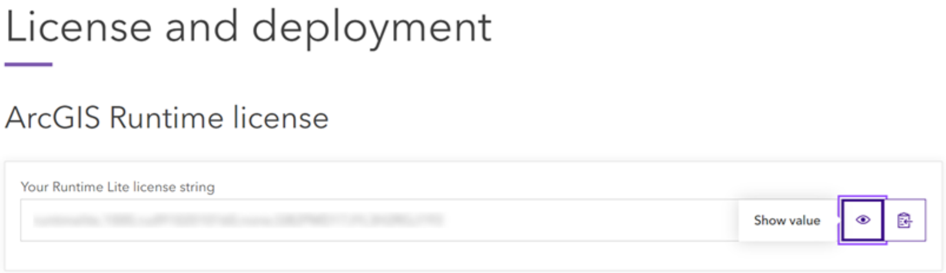
7 Click **Save** > **Apply**.

Connecting Map Manager to the Esri ArcGIS map provider

Before you can create maps using the Esri map provider, you must you must acquire a valid ArcGIS Runtime license and connect the Map Manager to an ArcGIS server.

Before you begin

- Acquire a valid ArcGIS Runtime license using the ArcGIS Runtime License Generator.



License and deployment

ArcGIS Runtime license

Your Runtime Lite license string

For more information about ArcGIS Runtime licenses, see Licensing your ArcGIS Runtime App.

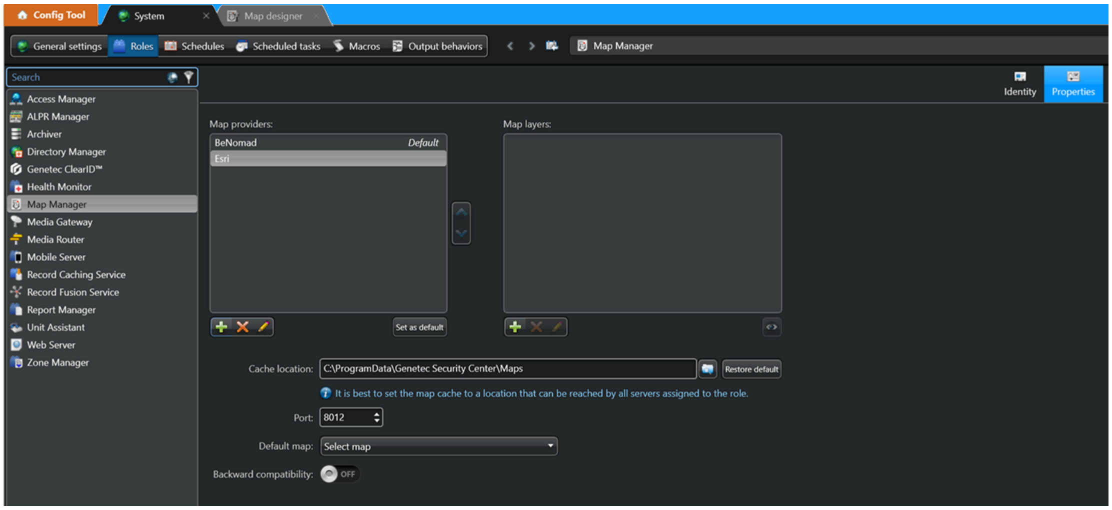
To connect Map Manager to an Esri map provider:

1 From the Config Tool home page, open the *System* task, and click the **Roles** view.

2 Select the Map Manager role, and click the **Properties** tab.

3 In the *Map providers* section, click **Add an item** (➕).

4 In the *Map providers* dialog box, select **Esri** from the **Provider** drop-down list.



Map providers:

BeNomad	*Default*
Esri	

Cache location: C:\ProgramData\Genetec Security Center\Maps

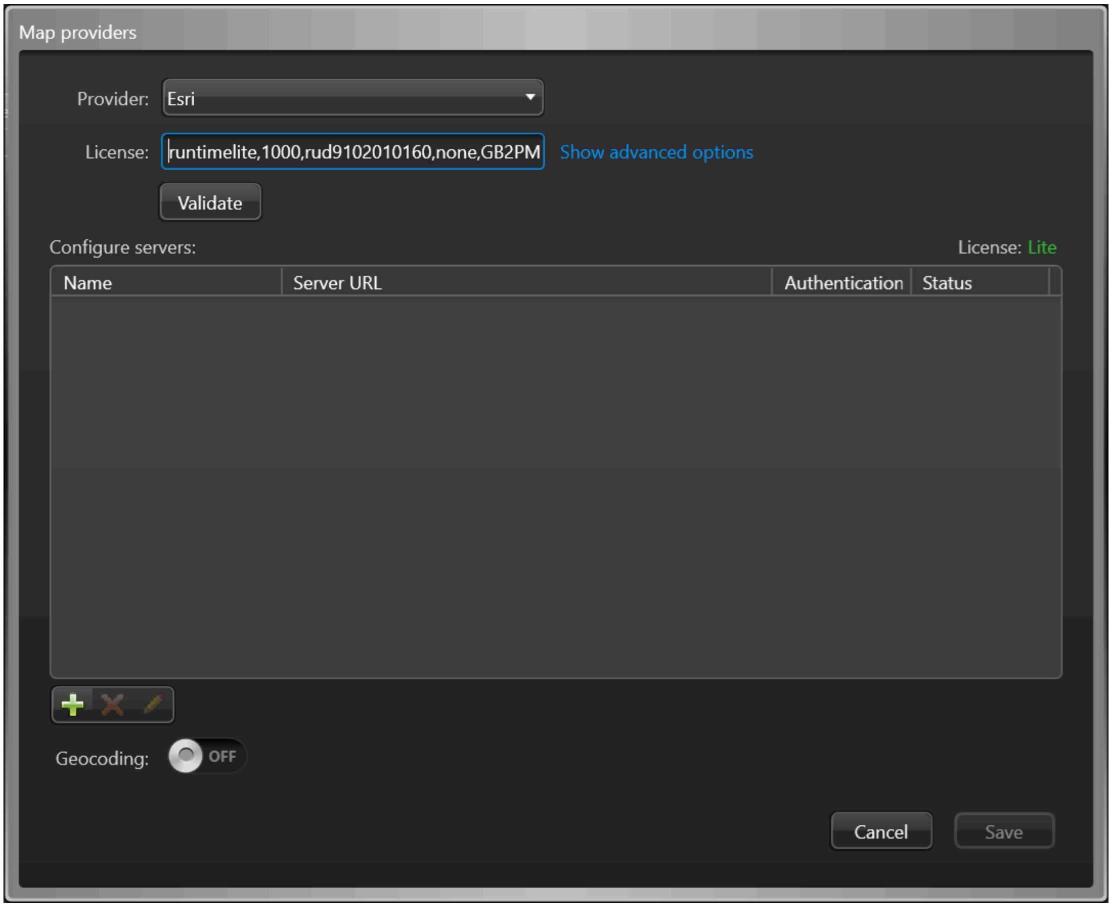
It is best to set the map cache to a location that can be reached by all servers assigned to the role.

Port: 8012

Default map: Select map

Backward compatibility: OFF

5 In the **License** field, enter your ArcGIS license code.



Map providers

Provider: Esri

License: runtimelite,1000,rud9102010160,none,GB2PM

Configure servers:

License: Lite

Name	Server URL	Authentication	Status

Geocoding: OFF

NOTE: The **LITE** license is the free version and all the functionality required from Esri. There is no need for the **Basic** or **Standard licensing**.

6 Click **Validate**.

If you entered the correct information, the license status changes to **Valid**.

7 Add an Esri ArcGIS server:

a) In the *Map providers* dialog box, click **Add an item** (➕) under *Configure servers*.

b) In the *Add server* dialog box, enter the **Name** of the ArcGIS server.

c) In the **Server URL** field, enter the URL of the ArcGIS server.

Use one of the following URL formats, depending on the type of server you are using:

- Web portal server: *https://<PortalName>.maps.arcgis.com/sharing/rest*
- Online map server: *http://services.arcgisonline.com/arcgis/rest/services/<MapName>/MapServer*
- Online or on-premise server: *http://<ServerName>:<PortNumber>/arcgis/rest/services*

d) If the server requires authentication, enable **Use authentication** and enter your credentials.

e) If the server offers token-based authentication, enable **Use token authentication** to exchange user credentials for a token that is used to authenticate all future requests for secured content on the server.

f) Click **Add**.

8 As needed, add additional ArcGIS servers to view more layers on your map.

9 If your license includes geocoding services, turn the **Geocoding** option on.

If you are using your own geocoding service, enter its specific address in the **URL** field.

With this feature enabled, Map Manager can convert a pair of latitude and longitude into a street address and vice versa. You can also search for a street address from the *Maps* task in Security Desk and zoom in to that address on the map.

10 Click **Save** > **Apply**.

Connecting Map Manager to a WMS map provider

Before you can create maps that use layers from a WMS server, you must set up a map provider and select the layers to use.

What you should know

The Web Map Service (WMS) standard separates maps into one or more layers of georeferenced information. When connecting the Map Manager to a WMS server, layers can be enabled or disabled to control what the map displays.

Map Manager supports the WMS protocol version 1.3.0 and 1.1.1.

IMPORTANT: The Map Manager requires WMS maps to use EPSG:4326. Use the Esri ArcGIS map provider for all nonstandard projections.

To connect the Map Manager role to a WMS server:

1 From the Config Tool home page, open the *System* task, and click the **Roles** view.

2 Select the Map Manager role, and click the **Properties** tab.

3 In the *Map providers* section, click **Add an item** (➕).

4 In the *Map providers* dialog box, select **WMS** from the **Provider** drop-down list.

5 In the **Name** field, type a name for the map provider.

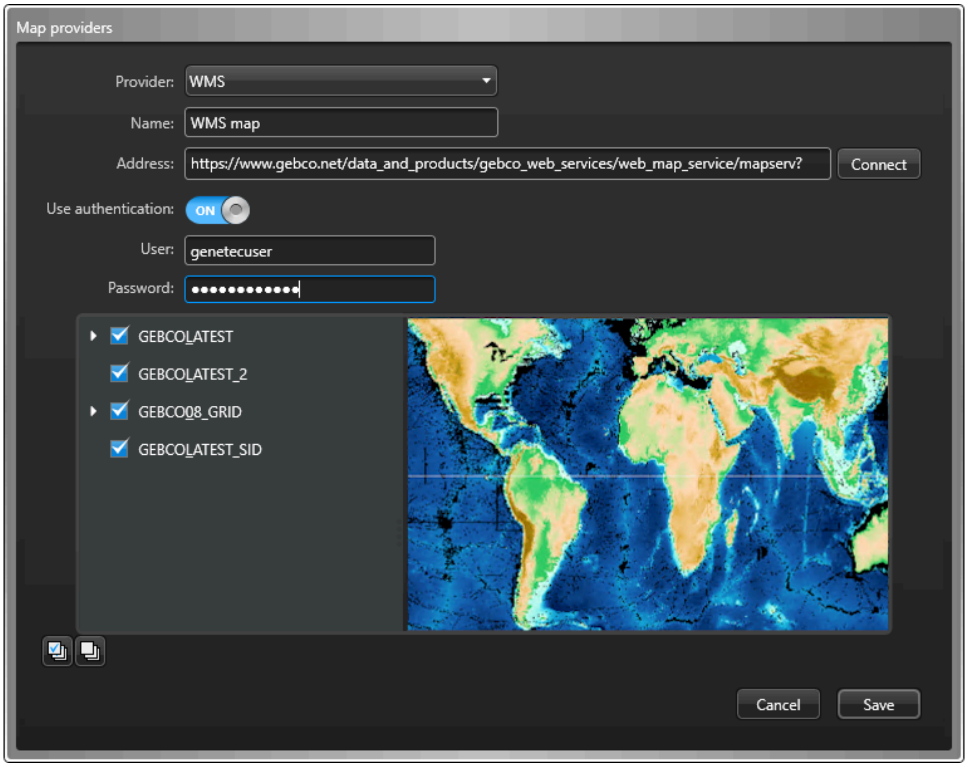
6 In the **Address** field, type the base URL of the map server.

   If the server requires authentication, turn **Use authentication** on and enter the username and password.

   Server capabilities are discovered automatically.

7 Click **Connect**.

If you entered a valid URL, a preview of the selected map and a list of available layers is displayed. All layers are selected by default.



Map providers

Provider: WMS

Name: WMS map

Address: https://www.gebco.net/data_and_products/gebco_web_services/web_map_service/mapserv?

Use authentication: ON

User: genetecuser

Password: ●●●●●●●●●●●●

☑ GEBCO_LATEST

☑ GEBCO_LATEST_2

☑ GEBCO08_GRID

☑ GEBCO_LATEST_SID

8 If required, deselect any layers that are not needed.

9 Click **Save** > **Apply**.

Connecting Map Manager to a TMS map provider

Before you can create maps based on OpenStreetMap or other tile data, you must set up a custom map provider and connect Map Manager to a GIS that supports a specific URL format.

What you should know

Map Manager supports Tile Map Service (TMS) servers, like those provided by the OpenStreetMap Foundation, that deliver content on URLs with a zoom factor, X position, and Y position. The format and supported elements are described in the URL format for web tile servers on page 299. When using a TMS server, you can define the boundaries and scale of the tiled map that you need.

To connect Map Manager to a TMS server:

1 From the Config Tool home page, open the *System* task, and click the **Roles** view.

2 Select the Map Manager role, and click the **Properties** tab.

3 In the **Map providers** section, click **Add an item** (➕).

4 In the *Map providers* dialog box, select **Custom *** from the **Provider** list.

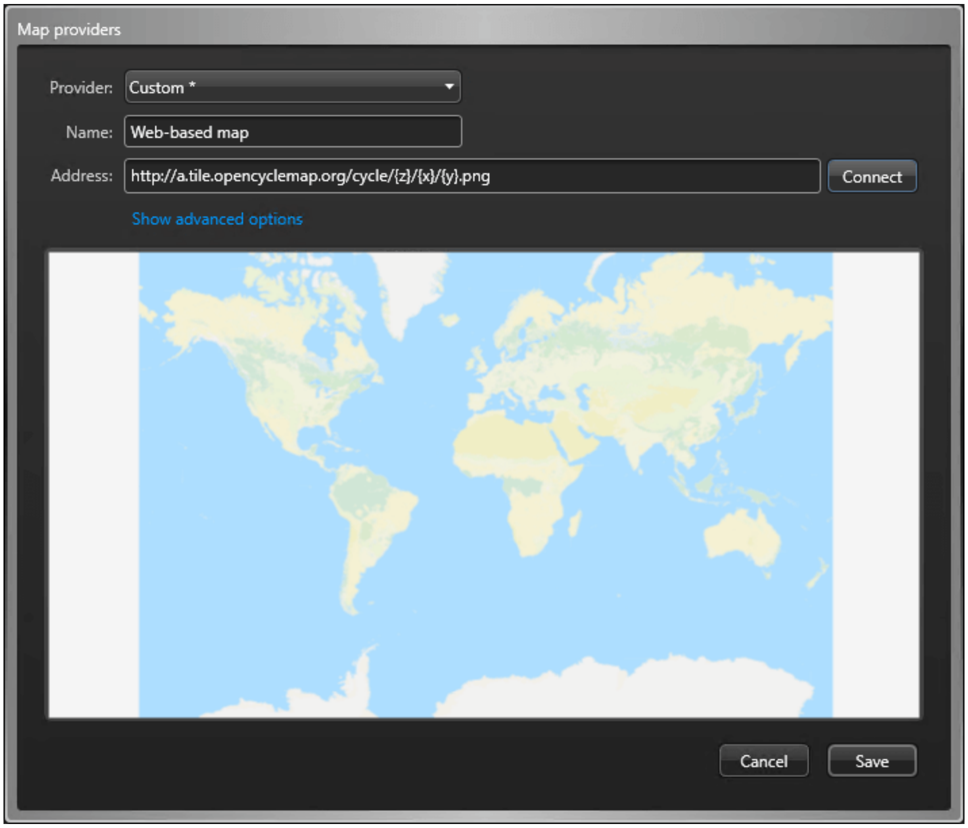
5 In the **Name** field, type a name for the map provider.

6 In the **Address** field, type the URL of the TMS server.

7 If required, click **Show advanced options** and configure the following:

- Set the **Maximum zoom level** supported by the map to a level between 1 - 25. The default is 17.
- If the server requires authentication, turn **Use authentication** on and enter the username and password.

8 Click **Connect**.
If you entered a valid URL, the map appears.



Map providers

Provider: Custom *

Name: Web-based map

Address: http://a.tile.opencyclemap.org/cycle/{z}/{x}/{y}.png

9 Click **Save** > **Apply**.

URL format for web tile servers

To connect Map Manager to a web tile server, the server URL must adhere to the supported format.

URL format for web tile servers

The Map Manager supports the following URL format for web tile servers:

```
http://<Server>/tile/<Version>/<Layer>/<Style>/{z}/{x}/{y}.<FileType>
```

The URL components are as follows:

URL element	Description	Mandatory
Server	The root URL of the Web Map Tile Service (WMTS) resource.	Yes
Version	The version of the WMTS standard: for example, 1.0.0.	
Layer	The map layer.	
Style	The style of the map layer, usually default.	

URL element	Description	Mandatory
{z}/{x}/{y}	The zoom factor {z}, X position {x}, and Y position {y} variables that are part of the WMTS standard. These values are calculated automatically when you view the map in Security Center.	Yes
FileType	The format of the file, usually JPEG or PNG format.	Yes

For a list of supported values, see the *capabilities document* of the server.

Example

```
http://sampleserver6.arcgisonline.com/arcgis/rest/services/WorldTimeZones/
MapServer/WMTS/tile/1.0.0/WorldTimeZones/default/default028mm/{z}/{y}/{x}.png
```

URL format for OpenStreetMap

If you are connecting Map Manager to a web tile server provided by the OpenStreetMap Foundation, use the following URL format:

```
http://<Server>/{z}/{x}/{y}.<FileType>
```

Where the Server is the URL of the OpenStreetMap server and FileType is the format of the file.

Example

```
http://a.tile.opencyclemap.org/cycle/{z}/{x}/{y}.png
```

Creating maps

A map in Security Center is a two-dimensional diagram that helps you visualize the physical locations of your security equipment in a geographical area or a building space. You create maps using the *Map designer* task.

Before you begin

All maps must be attached to an area in Security Center. The area and its map form a single entity. It is best practice to define your area hierarchy before attaching the maps.

What you should know

A map is composed of a static background image with various information layered on top, called *map objects*. Security Desk users can control the amount of information they see on a map by showing or hiding any of these layers (map objects).

Maps can be created from the *Area view* task or the *Map designer* task. Creating a map from the *Area view* automatically attaches that map to the selected area.

To create a map from the *Area view*:

1. From the Config Tool home page, open the *Area view* task.
2. In the entity tree, select an area for the map.
3. Click the **Identity** tab, and click **Create map**.
   The *Map designer* task opens.
4. Select one of the following methods to create your map background.
   - Import the map background from an image file.
   - Connect to a map provider.
5. Configure the default map view and other presets.
6. Configure the default information to display when someone opens this map.
7. Click **Apply**.

After you finish

Add map objects to your map.

Related Topics

Overview of the Map designer task on page 321

Configuring map presets

You can save frequently used map views as map presets so other users can quickly access them when needed.

What you should know

A map preset is a saved map view. Every map has at least one preset, called the *default view*, that is displayed when a user opens the map. When a user selects a map preset, Security Desk fits the map view inside the map window by adjusting the zoom level, if possible.

Maps can be locked to the *default view*. When locked, users are prevented from repositioning the map by panning, zooming, or using presets.

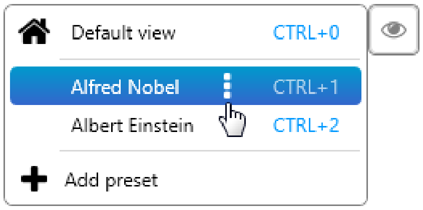
To configure a map view:

1 In the *Map designer* task, position the map in the required *map view*.

- Click and drag to reposition the map.
- Use the mouse wheel or the overlaid + and − buttons to zoom in and out.

2 Click **Select preset** (👁).

The following menu opens:



3 Do one of the following:

- Click **Add preset** (+) to save your map view as a new preset.
- Click ⋮ to override, rename, or delete an existing map preset.

  NOTE: Users can be prevented from repositioning the map by locking their display to the *default view*.

  After setting the *default view*, lock the map in the *Map designer* task by selecting **Map** > **Lock Display** and one of the following:

  - **None:** No lock applied to map.
  - **Zoom:** Users cannot zoom in or out of default view, but can still navigate around the map.
  - **Pan and zoom:** Users cannot zoom in or out of default view, nor navigate around the map.

4 In the *Map designer* toolbar, click **Save** (💾).

To revert your changes, click **Cancel** (↺) instead.

Your changes are immediately available to Security Desk users.

Configuring default information to display on maps

You can configure which information appears by default when opening maps.

What you should know

Security Desk users can always set which layers they want to see on their maps, regardless of what layers are displayed by default.

To configure the layers to show by default on a map:

1 In the *Map designer* menu, click **Map** > **Layers**.

A dialog box that lists all available layers for your map opens.

2 Select the layers that you want to show by default.

You can show or hide multiple layers on the map, such as the following:

- Door
- Camera
- ALPR unit
- Alarm
- Custom entity
- Entity name

3 Select the **Hide empty layers** option to show only the layers that have map objects on the current map.

4 To sort the layers, select a layer, and then use the up (▲) and down (▼) arrows.

5 In the *Map designer* toolbar, click **Save** (💾).

Adjusting the opacity of the information displayed on maps

To avoid obstructing valuable information on the map, you can adjust the opacity of a map layer. For example, a layer that displays weather patterns might block the view of a street name or point of interest on the map.

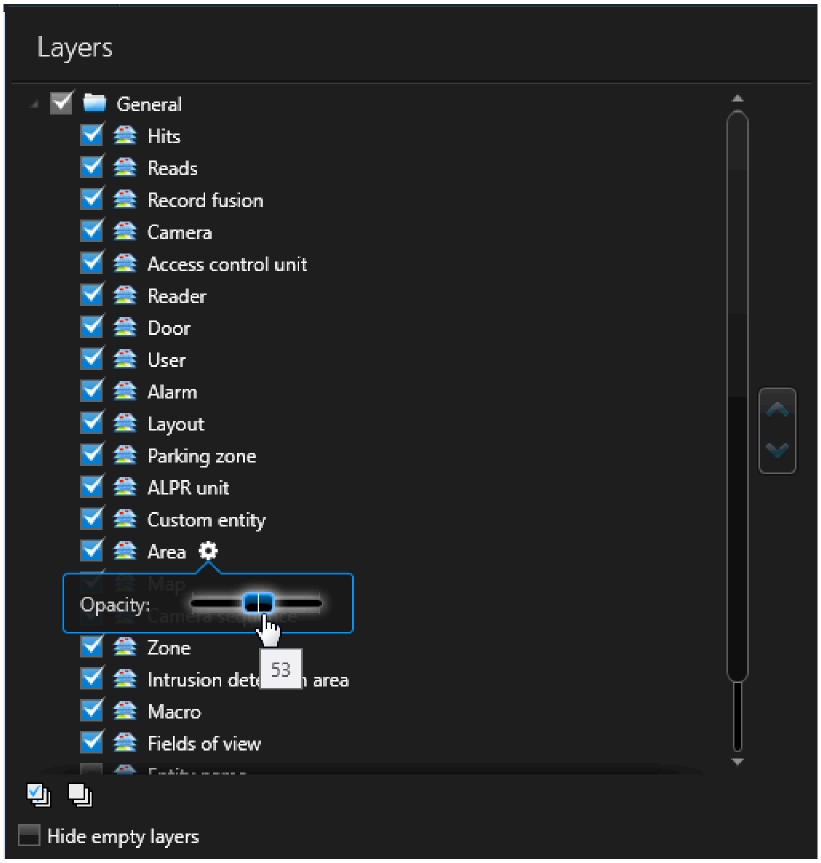
What you should know

Security Desk users cannot change the opacity of a map layer because it can only be done from Config Tool.

To adjust the opacity of map layers:

1 In the *Map designer* menu, click **Map** > **Layers**.
A dialog box that lists all available layers for your map opens.

2 Point to the layer you want to change, and click the cogwheel (⚙).



3 In the widget that opens, drag the **Opacity** slider until you get the desired effect on the map.

4 Repeat with other layers if necessary.

5 In the *Map designer* toolbar, click **Save** (💾).

Configuring map objects that move

To represent objects that move on maps, you can configure an Esri map layer to refresh at regular interval.

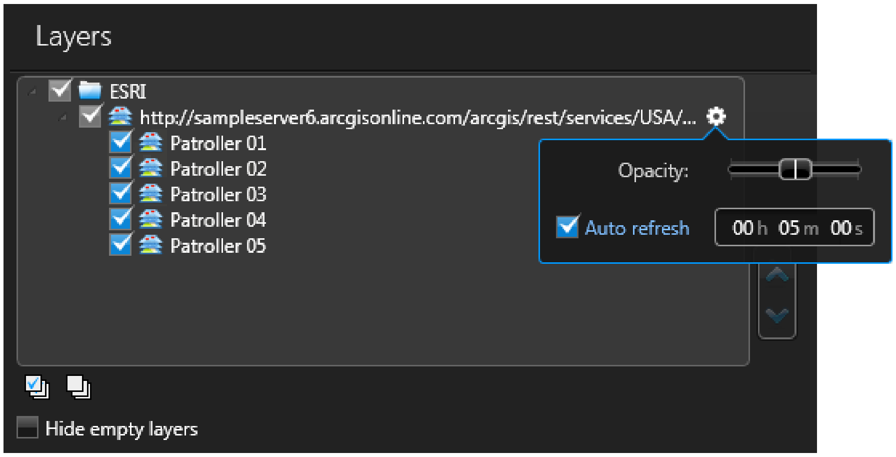
What you should know

If you have an Esri object that gets updated in real time, you can set the corresponding map layer to refresh at regular intervals, so that those updates are applied. For example, if you have an Esri object that tracks a vehicle position in real time, you can set the map layer to refresh every 5 minutes to show the movement of this vehicle in Security Desk.

To configure a moving map object:

1 In the *Map designer* menu, click **Map** > **Layers**.
A dialog box that lists all available layers for your map opens.

2 Point to the layer you want to change and click the cogwheel (⚙).



Layers

☑ ESRI
☑ http://sampleserver6.arcgisonline.com/arcgis/rest/services/USA/...
☑ Patroller 01
☑ Patroller 02
☑ Patroller 03
☑ Patroller 04
☑ Patroller 05

Opacity:
☑ Auto refresh 00 h 05 m 00 s

□ Hide empty layers

3 In the widget that opens, select **Auto refresh** and then set the refresh rate.

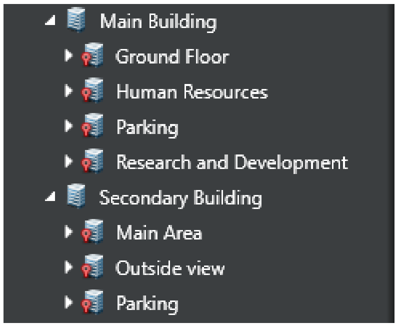
4 In the *Map designer* toolbar, click **Save** (💾).

Configuring maps as floors of a building

To navigate between maps quickly, you can designate two or more maps as floors of the same building.

Before you begin

Organize your area view into one or more buildings, each with mapped sub-areas that represent floors.



- Main Building
  - Ground Floor
  - Human Resources
  - Parking
  - Research and Development
- Secondary Building
  - Main Area
  - Outside view
  - Parking

What you should know

Using the *Map designer*, you can configure maps as floors of a building. With floor maps, you can quickly navigate a building using controls overlaid on these maps.

Each floor is linked to all other floors in the same building. You can navigate between floor maps by pressing the button for the floor you want to see. If an area is included in multiple buildings, like a shared parking lot, then the floor controls can be used to navigate between buildings.

If the floor maps are georeferenced, the map view stays on the same part of the map when navigating between floors. Press and hold the Ctrl key while changing floors to restore the default view.

To configure floors:

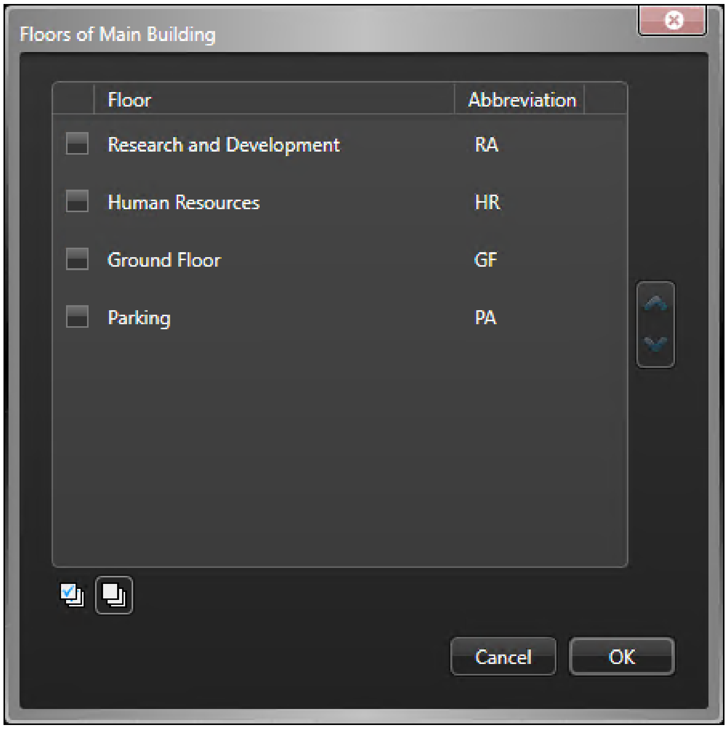
1 From the Config Tool homepage, open the *Map designer* task.

2 Open a floor map by selecting one of the recent maps or clicking **Browse all maps**.

NOTE: The areas attached to connected floor maps must have the same parent.

3 Open the *Floors* dialog box in one of the following ways:

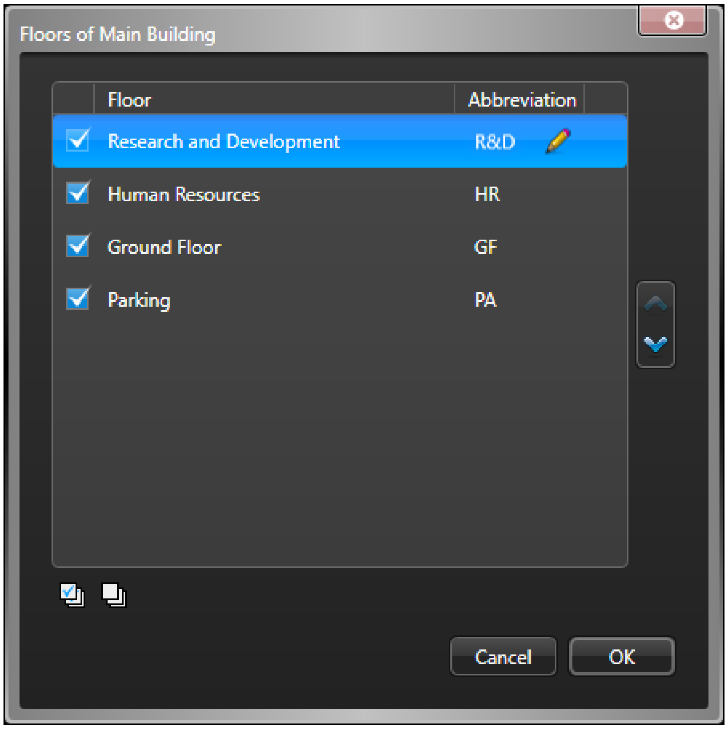
- Click **Map** > **Floors**.
- In the *Map designer* toolbar, click the **Floors** () button.
- Click the overlaid **Edit floors** () button.



Floors of Main Building

	Floor	Abbreviation
□	Research and Development	RA
□	Human Resources	HR
□	Ground Floor	GF
□	Parking	PA

4 Select two or more check boxes to designate maps as floors of the parent area. Each floor has a configurable abbreviation to represent the map on the floor controls.

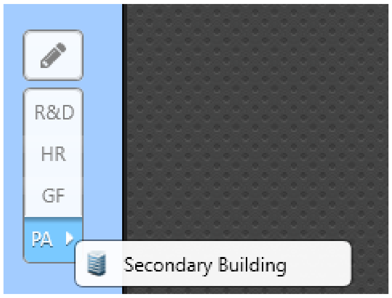


Floor	Abbreviation
☑ Research and Development	R&D
☑ Human Resources	HR
☑ Ground Floor	GF
☑ Parking	PA

5 If needed, use the arrows (▲▼) to reorder the floors. Floors are presented in this order in the floor controls.

6 Click **OK**.

The floor controls are overlaid in the bottom-right corner of the map in Config Tool and Security Desk.



NOTE: The **Edit floors** (✎) button is only available in Config Tool.

Creating maps from image files

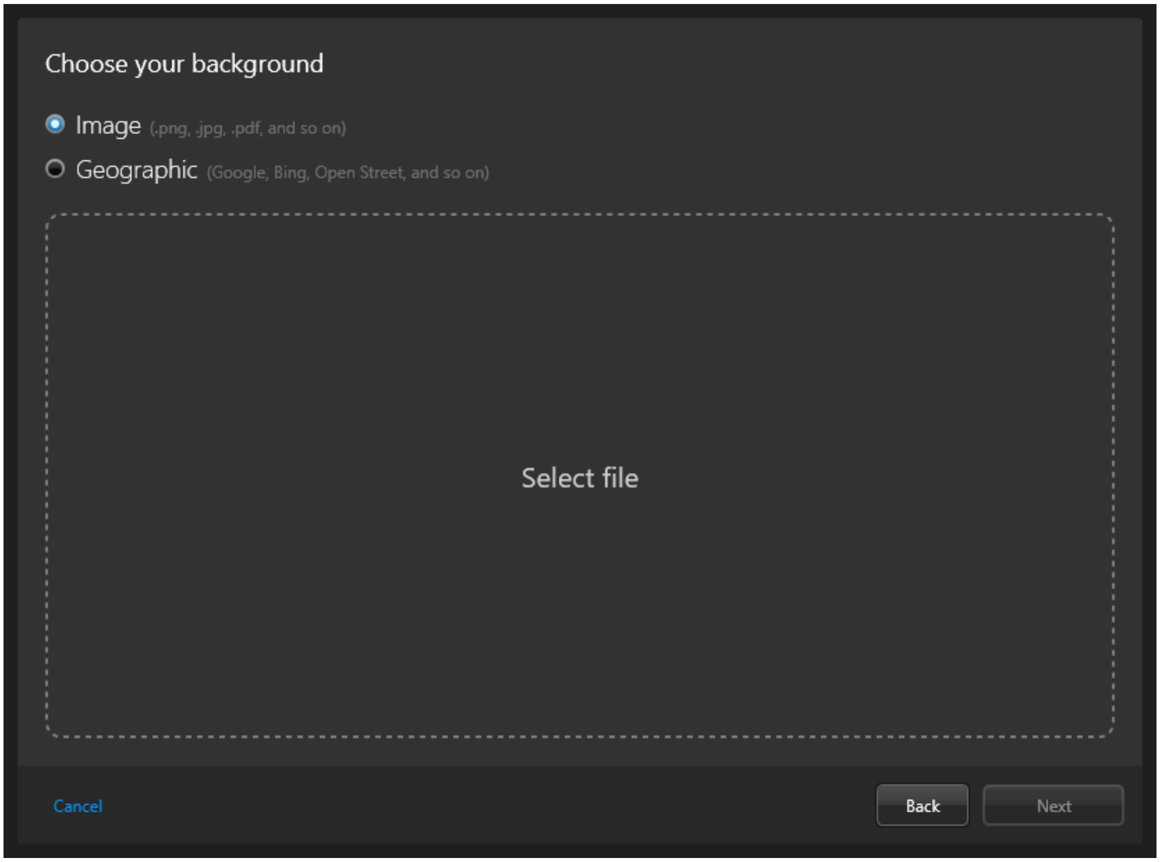
You can create personalized maps of your site and floor plans of your buildings, by importing their background image from image files.

What you should know

All maps must be attached to an *area* or a *parking zone*.

To create a map from an image file:

1. From the Config Tool homepage, open the *Map designer* task.
2. Click **Create**.
3. In the entity tree, select an area or a parking zone to attach your map to, or click **New area**.
4. (Optional) Select the icon to represent your area with a map (Default =).
5. Click **Next**.
6. For the type of map background, select the **Image** option, and click **Select file**.



Choose your background

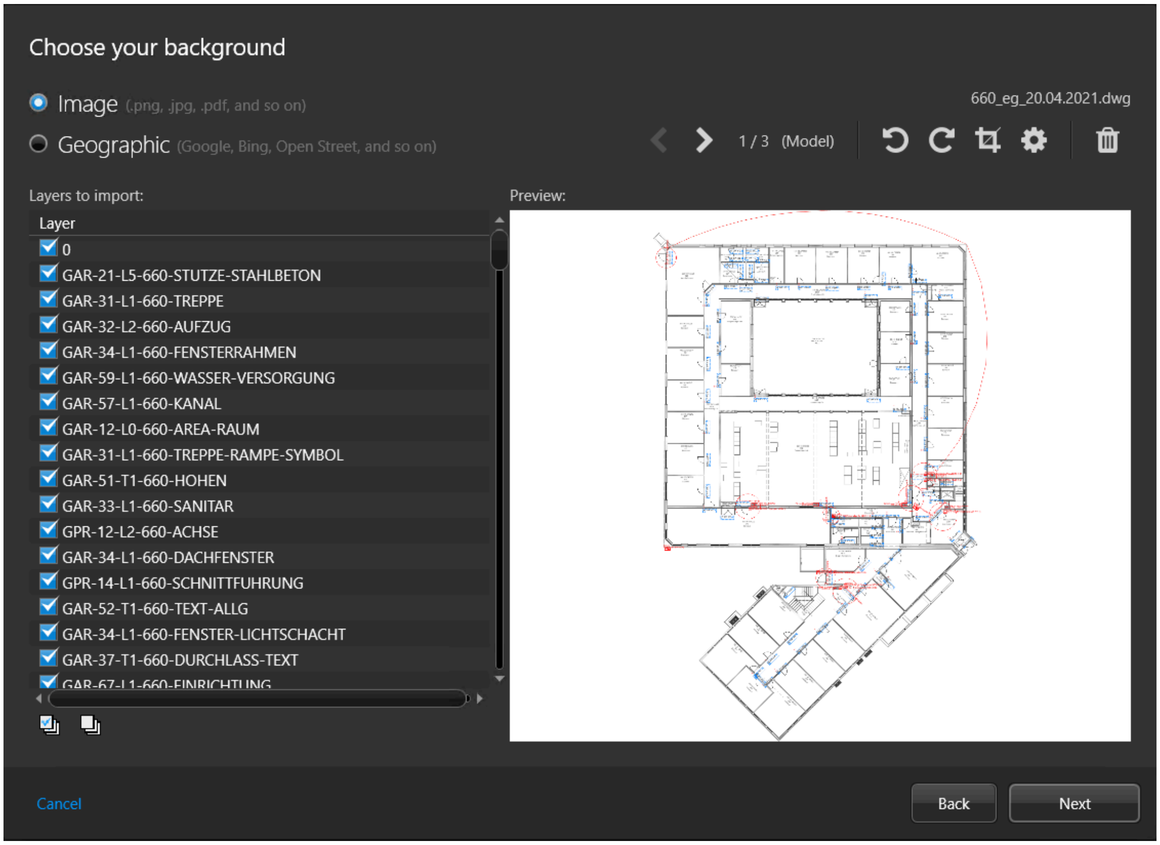
● Image (.png, .jpg, .pdf, and so on)

○ Geographic (Google, Bing, Open Street, and so on)

7 In the file browser, select a file and click **Open**.

NOTE: Image files, PDF files, and AutoCAD (DXF and DWG) files are supported.

The selected image is shown in the preview window.



Choose your background

● Image (.png, .jpg, .pdf, and so on)

○ Geographic (Google, Bing, Open Street, and so on)

660_eg_20.04.2021.dwg

1 / 3 (Model)

Layers to import:

Layer
☑ 0
☑ GAR-21-L5-660-STUTZE-STAHLBETON
☑ GAR-31-L1-660-TREPPE
☑ GAR-32-L2-660-AUFZUG
☑ GAR-34-L1-660-FENSTERRAHMEN
☑ GAR-59-L1-660-WASSER-VERSORGUNG
☑ GAR-57-L1-660-KANAL
☑ GAR-12-L0-660-AREA-RAUM
☑ GAR-31-L1-660-TREPPE-RAMPE-SYMBOL
☑ GAR-51-T1-660-HOHEN
☑ GAR-33-L1-660-SANITAR
☑ GPR-12-L2-660-ACHSE
☑ GAR-34-L1-660-DACHFENSTER
☑ GPR-14-L1-660-SCHNITTFUHRUNG
☑ GAR-52-T1-660-TEXT-ALLG
☑ GAR-34-L1-660-FENSTER-LICHTSCHACHT
☑ GAR-37-T1-660-DURCHLASS-TEXT
☑ GAR-67-L1-660-EINRICHTUNG

8 If necessary, select which layers or page to import, and then rotate and crop the image.

NOTE: The wizard does not create one map per layout. Do so manually.

9 Click **Advanced settings** (⚙), and set the following options:

- **Resolution:** The resolution of the image.
- **Background:** The background color of the image.

10 Click **Next**.

11 (Optional) If you are creating the map from an AutoCAD file, import map objects from the AutoCAD file.

12 Click **Next**.

13 Set your map scale using one of the following options:

NOTE: Instead of setting the map scale, you can georeference the map.

- **Room:** Floor plan for a small area such as a cafeteria or an auditorium.
- **Building:** Floor plan for a large area such as a building floor, a stadium, or a warehouse.
- **Campus:** Site map for an airport, a mall, or a university campus.
- **City:** City map. For example: Montreal, New York, Paris, London, Tokyo.

14 Click **Create** to generate the map.

The created map is displayed in the Map designer workspace.

15 If required, set a specific scale for the imported map image.

16 Configure the default map view and other presets.

17 Configure the default information to display when someone opens this map.

18 In the *Map designer* toolbar, click **Save** (💾).

After you finish

Add map objects to your map.

Importing map objects from AutoCAD

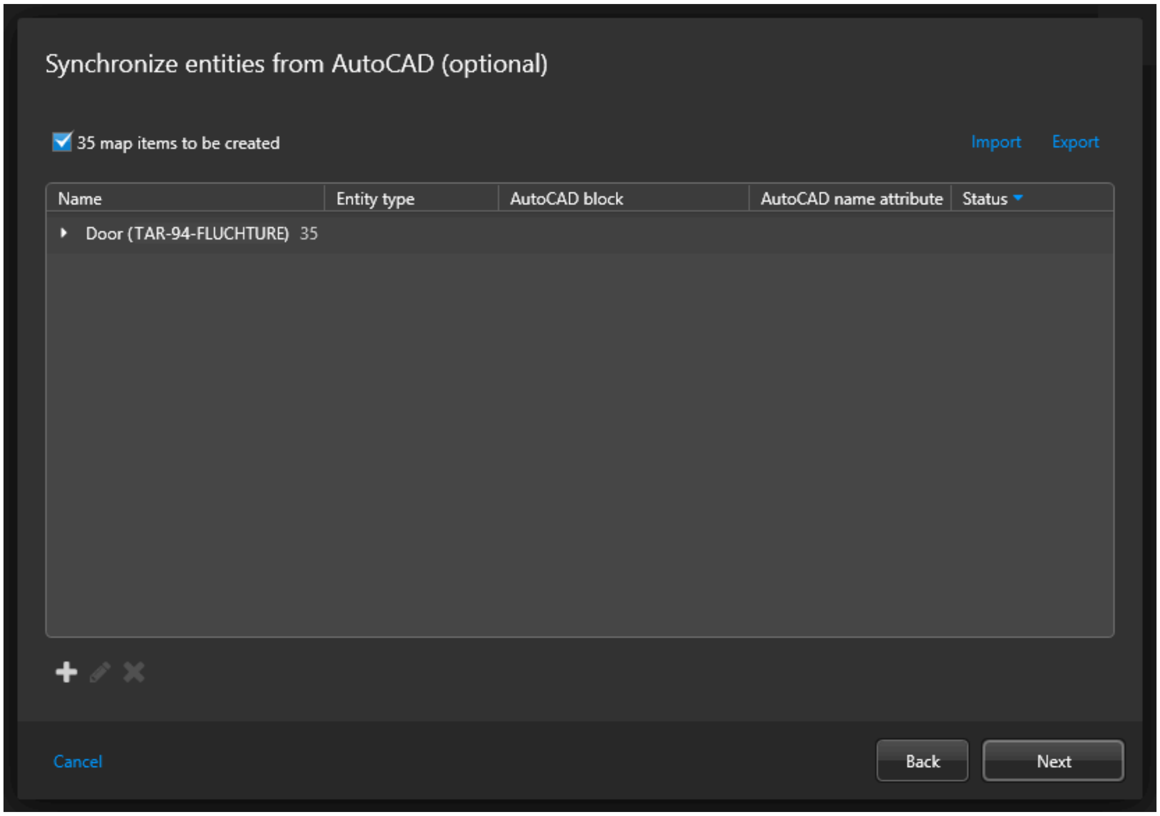
When you create a map from an AutoCAD file, you can import the AutoCAD blocks as map objects by associating them to existing Security Center entities.

Before you begin

- Ensure that the AutoCAD blocks that you want to import as *map objects* have matching Security Center entities.

To import AutoCAD blocks as map objects:

1 After the *Choose your background* step of the map creation wizard, you can import AutoCAD blocks as map objects by associating block definitions with Security Center entity types.



Synchronize entities from AutoCAD (optional)

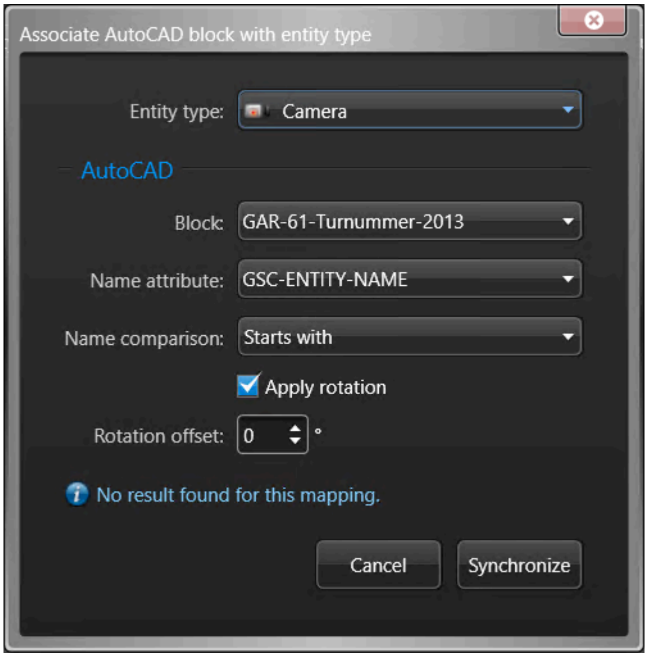
☑ 35 map items to be created

Name	Entity type	AutoCAD block	AutoCAD name attribute	Status
Door (TAR-94-FLUCHTURE) 35				

If you have synchronized entities from AutoCAD before, and the same block definitions exist in your current file, the same mapping would be loaded by default. You can edit the synchronization settings, import previously saved settings from an XML file, or define new ones.

2 If this is the first time you create a map from AutoCAD, click **Add** (✚).

3 In the dialog box that opens, associate an AutoCAD block with an entity type.



Associate AutoCAD block with entity type

Entity type: Camera

AutoCAD

Block: GAR-61-Turnummer-2013

Name attribute: GSC-ENTITY-NAME

Name comparison: Starts with

☑ Apply rotation

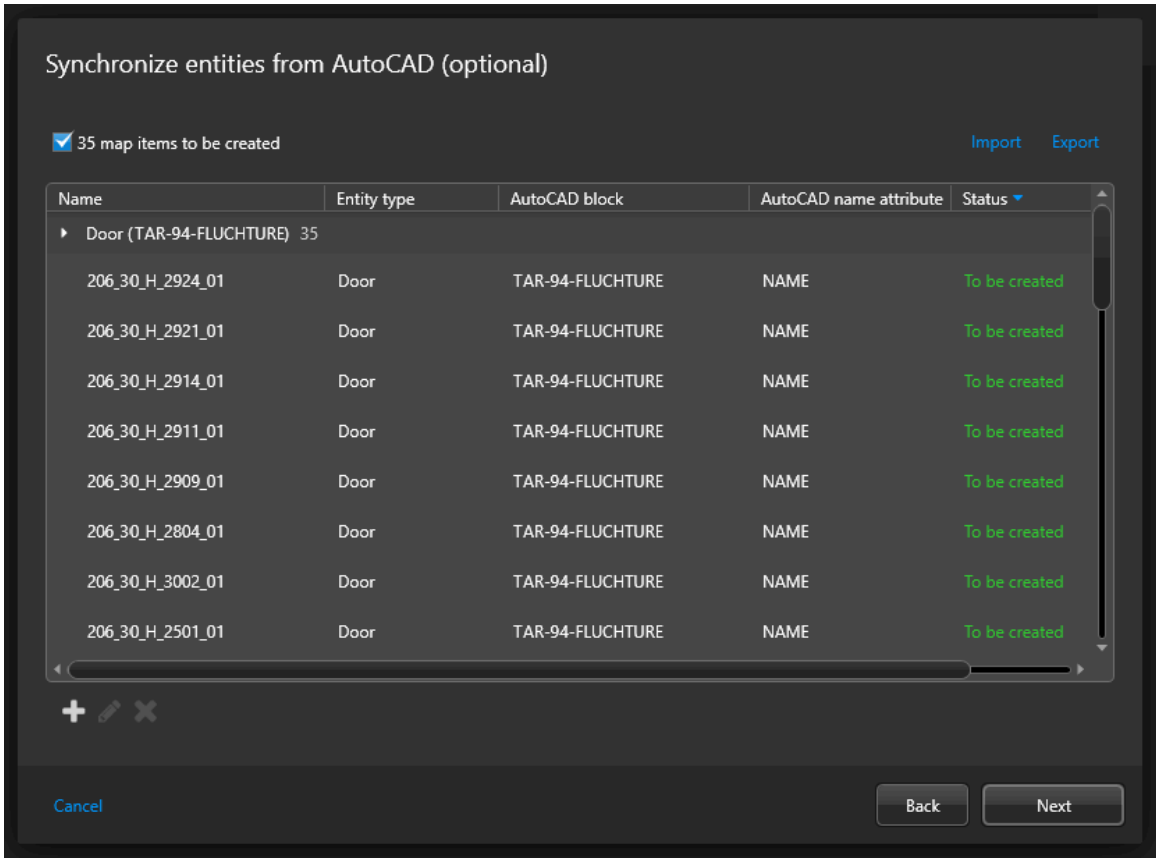
Rotation offset: 0 °

No result found for this mapping.

- **Entity type:** Security Center entity type behind the map objects you want to import.
- **Block:** Block definition to be associated to the selected entity type.
- **Name attribute:** Block attribute that holds the block instance name that must match the entity name.
- **Name comparison:** Search for entity names by **Exact match** or **Starts with**.
- **Apply rotation:** Apply a rotation offset to match the mapping of icons from the AutoCAD file to the icons in Config Tool.
- **Rotation offset:** Degree of rotation offset applied to a mapping.

4 Click **Synchronize**.

The matches found in the AutoCAD file are listed.



Synchronize entities from AutoCAD (optional)

☑ 35 map items to be created

Name	Entity type	AutoCAD block	AutoCAD name attribute	Status
Door (TAR-94-FLUCHTURE) 35				
206_30_H_2924_01	Door	TAR-94-FLUCHTURE	NAME	To be created
206_30_H_2921_01	Door	TAR-94-FLUCHTURE	NAME	To be created
206_30_H_2914_01	Door	TAR-94-FLUCHTURE	NAME	To be created
206_30_H_2911_01	Door	TAR-94-FLUCHTURE	NAME	To be created
206_30_H_2909_01	Door	TAR-94-FLUCHTURE	NAME	To be created
206_30_H_2804_01	Door	TAR-94-FLUCHTURE	NAME	To be created
206_30_H_3002_01	Door	TAR-94-FLUCHTURE	NAME	To be created
206_30_H_2501_01	Door	TAR-94-FLUCHTURE	NAME	To be created

5 If there are block instances you do not wish to import, select them in the list and click **Remove** (✖).

6 If necessary, associate more AutoCAD blocks with Security Center entity types.

7 Export your synchronization settings to an XML file for reuse.

a) Click **Export**.

b) In the file browser that opens, enter a file name and click **Save**.

An XML file that captures the AutoCAD blocks to Security Center entity type synchronization settings is created. You can reuse those settings the next time you create an AutoCAD map with the same block definitions.

8 Click **Next**.

After you finish

Resume your map creation process.

Related Topics

Updating map objects imported from AutoCAD on page 331

Adding map objects to your maps on page 336

Importing map objects from AutoCAD to geographic maps on page 317

Setting the scale of an imported map image

To ensure that the map scale matches the field of view distance defined for cameras on the map, you can set the scale of the imported map image after the map is created.

Before you begin

- Create a map from an image file.
- Add a camera to the map.
- Know the exact distance between two points that appear on the map.

What you should know

As an alternative to setting the scale of the map, you can georeference the map.
NOTE: Map scaling and georeferencing cannot be set at the same time.

To set the scale of an imported map image:

1 Open the *Map designer* task and select the map that you want to scale.

2 Click **Map** > **Edit scale**.

3 From the **Scale** list, select **Specific scale.**

4 From the drop-down list at the top of the screen, select the units to use for the measurement (for example, meters or feet) and define the number of units to match your known measurement.

5 Click **Draw line**.

6 Click and drag your mouse across the map to draw the line.

7 Move the endpoints of the line until they match the two known points of your measurement.

8 In the *Map designer* toolbar, click **Save** (💾).
The camera field of view and the map zoom level automatically adjust to the scale that you defined.

Related Topics

Adding cameras to your maps on page 343
Georeferencing a map image on page 314

Replacing image map background

You can change the background of an image map to update the map while preserving map objects.

Before you begin

- Create a map from an image file.

What you should know

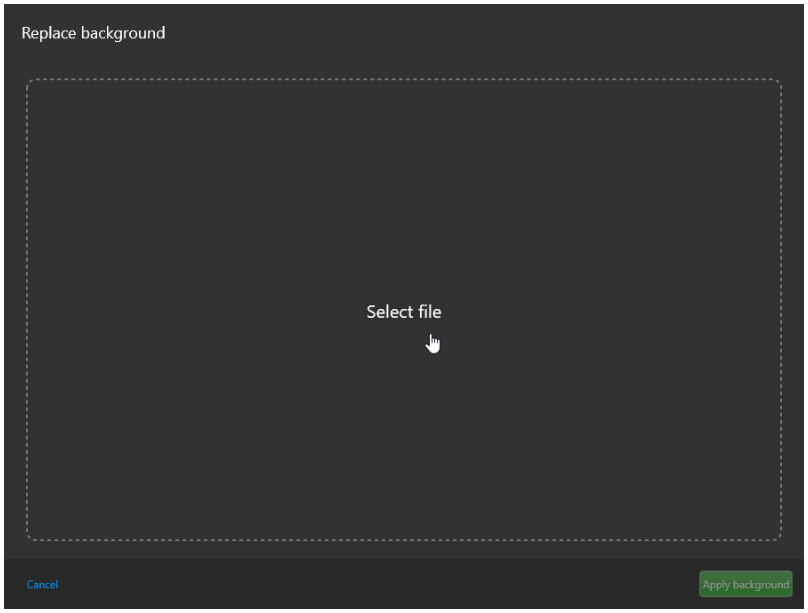
Replacing the background of a map lets you keep any map objects placed on the map. The map objects might need to be moved back into place on the map after the background replacement is complete.

To replace the background of an image map:

1 Open the *Map designer* task and select the map that you want change.

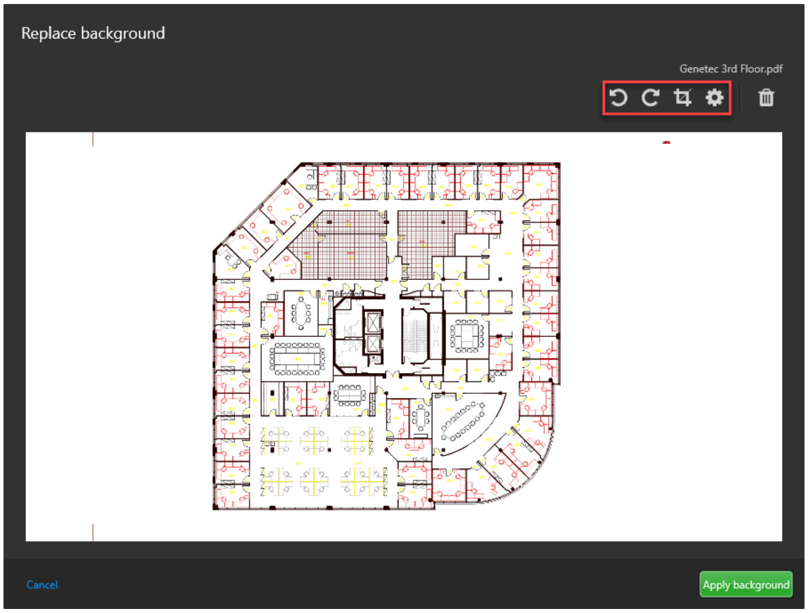
2 Click **Map** > **Replace background**.

3 Drag the replacement image into the dashed area or click **Select file**.



4 In File Explorer, navigate to the desired replacement image, select it, and click **Open**.

5 (Optional) Adjust the background image with the **Rotate left** , **Rotate right**, **Crop**, and or **Advanced settings** buttons.



6 Click **Apply background**.

Map background is replaced.

Georeferencing a map image

To ensure that all imported maps respect the same scale, you can georeference each map by adding at least three markers with geographic coordinates to the map.

Before you begin

Create a map from an image file.

What you should know

IMPORTANT: Georeferencing a map removes all objects that were previously added to the map. Objects need to be added again after you georeference the map.

To georeference a map image:

1 Open the *Map Designer* task and select the map that you want to georeference.

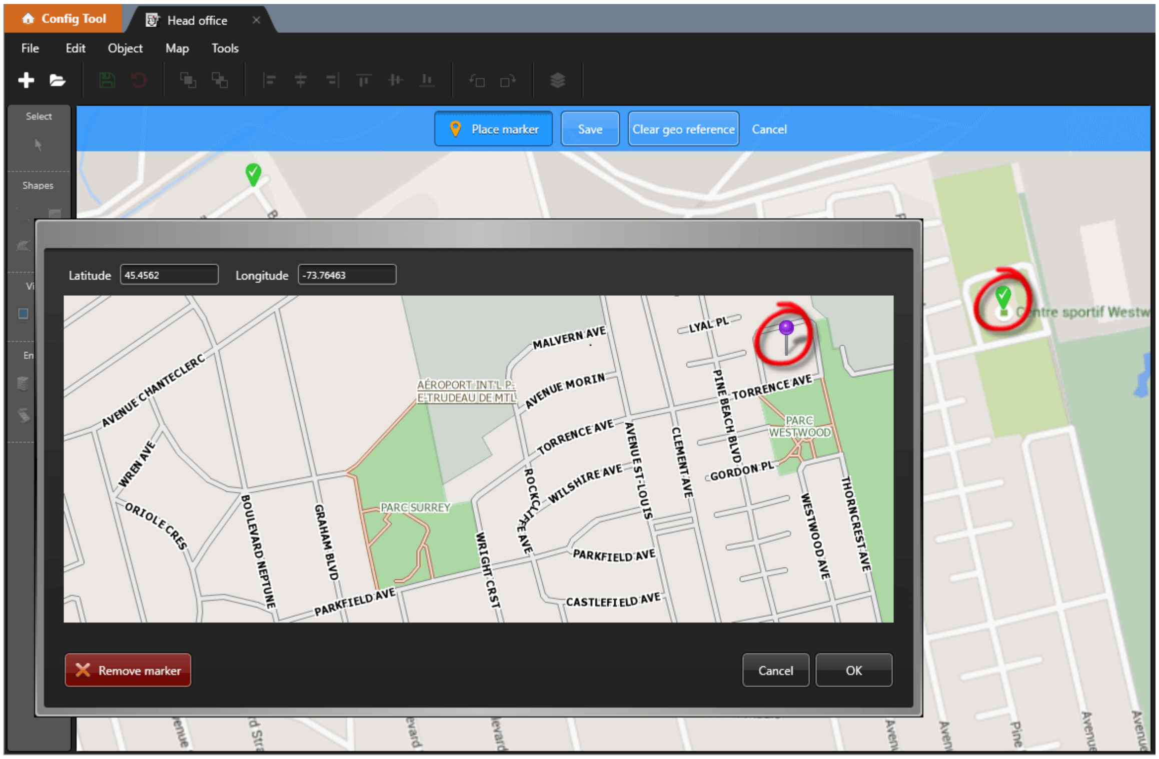
2 Click **Map** > **Calibrate georeferencing**.

3 Click **Place marker** and click a location on the map.

A window opens with a second map.

4 Zoom in and click the same location as the marker that you set in the previous step.

NOTE: If you already know the exact coordinates of the location, you can enter the latitude and longitude in the provided fields.



Latitude 45.4562 Longitude -73.76463

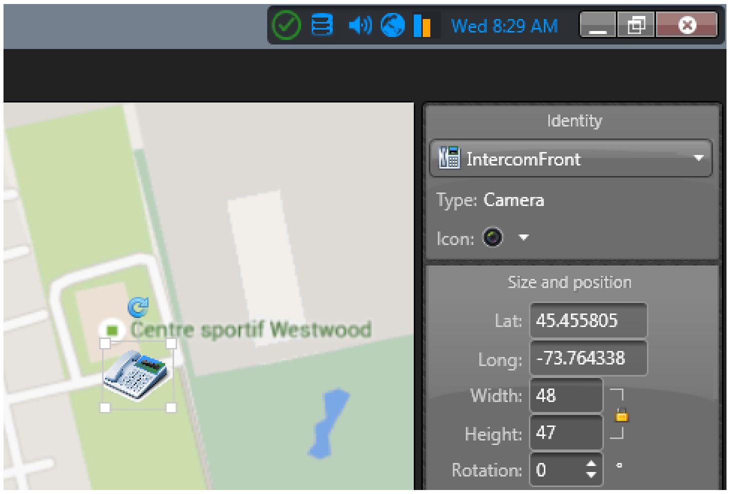
5 To accept the pin position, click **OK**.

6 Repeat the same process until you have georeferenced at least three positions.

TIP: Adding additional markers increases the georeferencing accuracy.

7 In the *Map designer* toolbar, click **Save** (💾).

8 To verify that georeferencing is enabled on the map, add an object to the map.
If the *Size and position* widget shows the latitude and longitude of the object, the map is georeferenced.



Related Topics

Setting the scale of an imported map image on page 312
Adding cameras to your maps on page 343

Creating maps by connecting to a GIS

You can create detailed road maps and large area maps by connecting to a third-party GIS vendor, also known as a map provider.

Before you begin

You must connect your *Map Manager* role to at least one external map provider.

For example, you can connect the Map Manager role to the Esri ArcGIS map provider or connect the Map Manager role to a TMS map provider.

What you should know

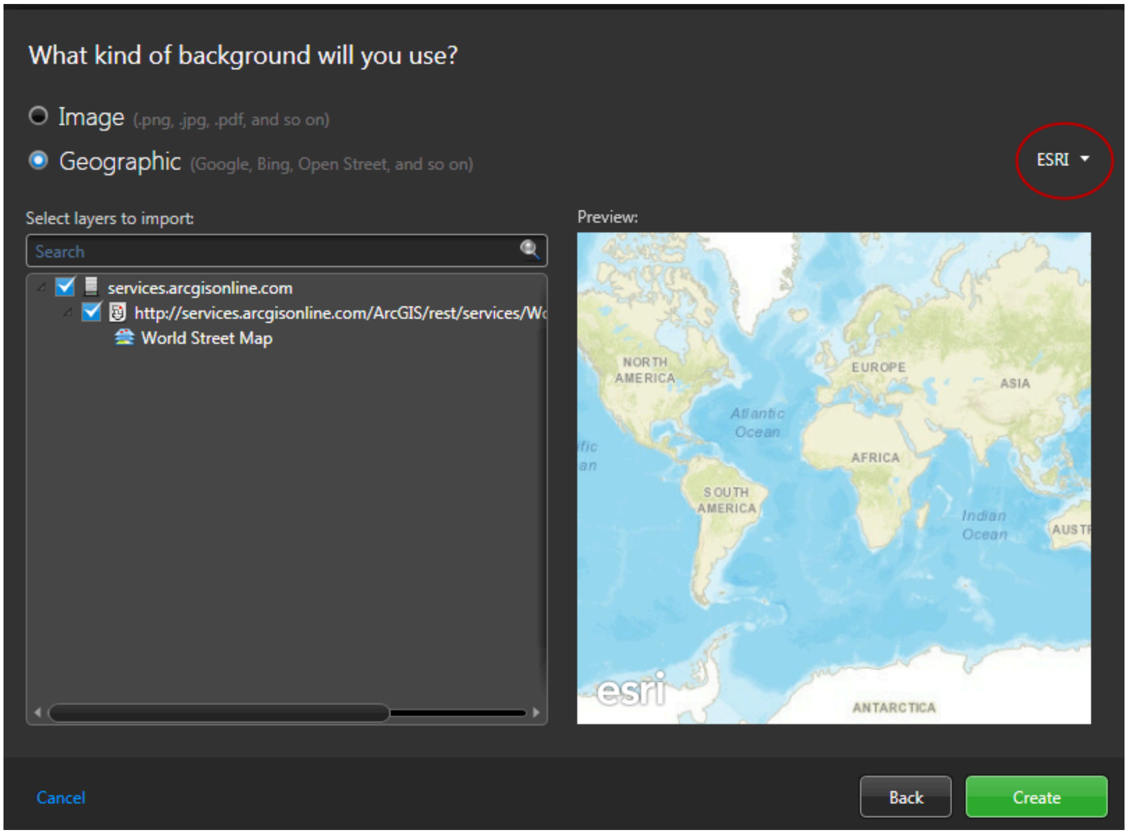
All maps must be attached to an area.

IMPORTANT: Combining data from multiple map providers is not supported. Only one provider can be used to create a map.

To create a map by connecting to a map provider:

1. From the Config Tool homepage, open the *Map designer* task.
2. Click **Create**.
3. From the area tree, select the area you want to attach your map to, or click **New area** to create a new one.
4. (Optional) Select the icon to represent your area with a map (Default = 🏢).
5. Click **Next**.
6. For the type of map background, select the **Geographic** option.

7 Click the drop-down list to the right, and select the desired map provider.
Example: If you connected the Map Manager role to the Esri ArcGIS map provider, select **Esri**.



What kind of background will you use?

○ Image (.png, .jpg, .pdf, and so on)

● Geographic (Google, Bing, Open Street, and so on)

ESRI ▾

Select layers to import:

☑ services.arcgisonline.com
☑ http://services.arcgisonline.com/ArcGIS/rest/services/W
World Street Map

8 Depending on which map provider you selected, you might have to select which maps and layers you want to import.

NOTE: If you import multiple Esri ArcGIS web maps that share the same map layers, you might experience issues with showing, hiding, or sorting map layers. To prevent this issue, only import one Esri web map.

9 Click **Create**.

The created map is displayed in the Map designer workspace.

10 Configure the default map view and other presets.

11 Configure the default information to display when someone opens this map.

12 In the *Map designer* toolbar, click **Save** (💾).

After you finish

Add map objects to your map.

Importing map objects from AutoCAD to geographic maps

You can import map objects from an AutoCAD file to a geographic map if the AutoCAD block definitions have latitude and longitude attributes.

Before you begin

- Create a geographic map.
- Ensure that the AutoCAD blocks you want to import as *map objects* have matching Security Center entities and have latitude and longitude attributes.

What you should know

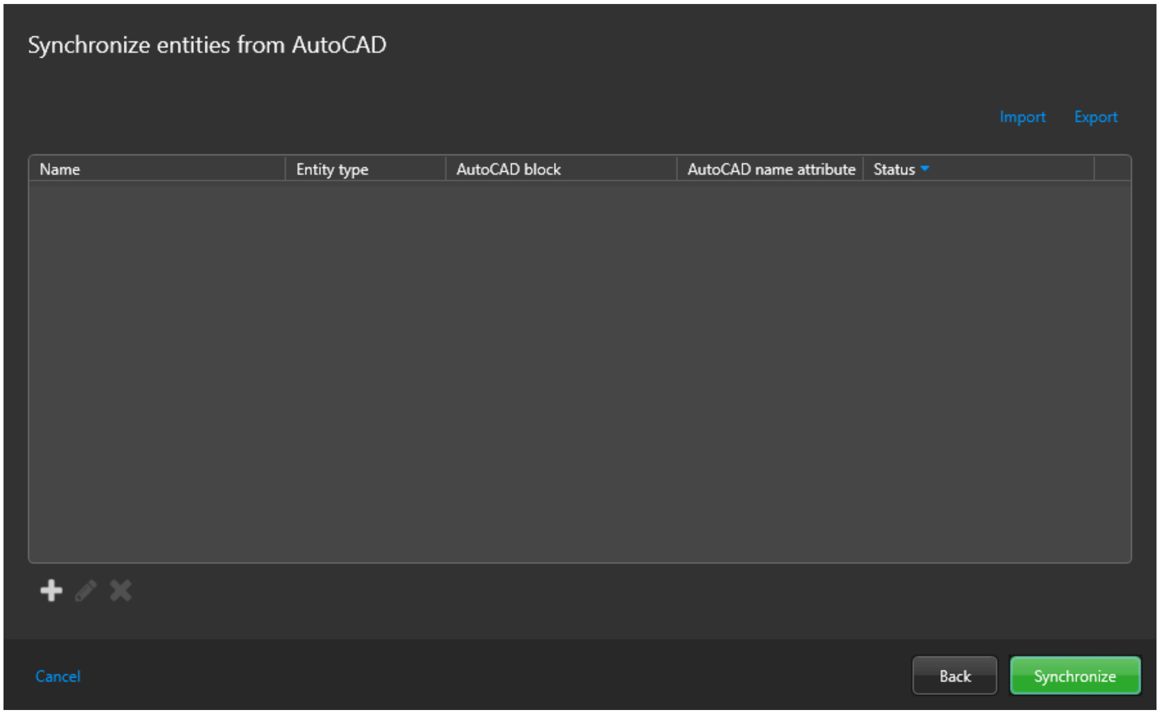
To import map objects from AutoCAD to a geographic map:

1 Open the *Map Designer* task and select the geographic map that you want to update.

2 Click **Map** > **Synchronize entities from AutoCAD**.

3 Click **Select file**, select the AutoCAD file you want to import from, and click **Open**.
A thumbnail of the AutoCAD image is shown.

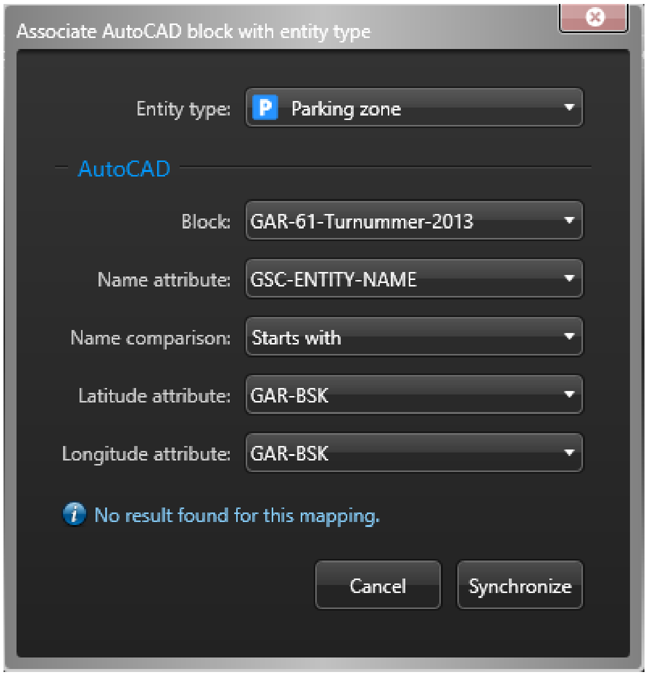
4 Click **Next**.
You are presented with an empty list of AutoCAD blocks to import.



5 If you have saved synchronization settings that you can reuse, click **Import** and select the XML file you saved.
If the selected synchronization file refers to block definitions that are not found in the current AutoCAD file, nothing would be imported.

6 Click **Add** (✚).

7 In the dialog box that opens, associate an AutoCAD block with an entity type.



Associate AutoCAD block with entity type

Entity type: Parking zone

AutoCAD

Block: GAR-61-Turnummer-2013

Name attribute: GSC-ENTITY-NAME

Name comparison: Starts with

Latitude attribute: GAR-BSK

Longitude attribute: GAR-BSK

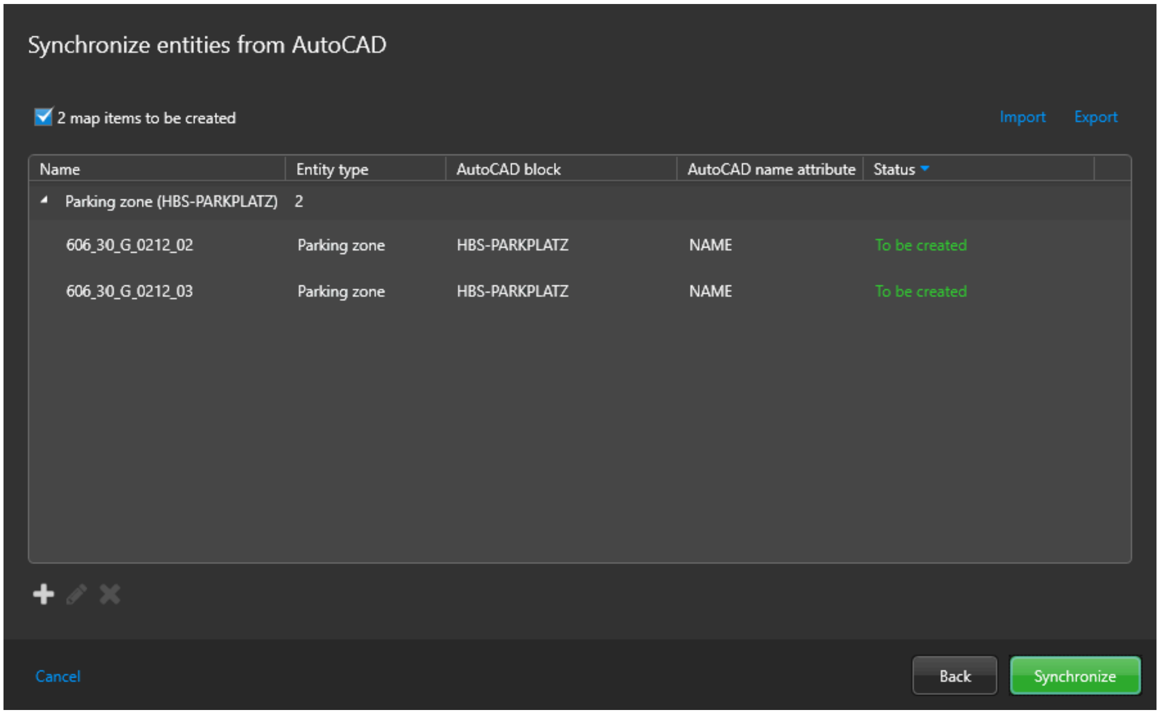
No result found for this mapping.

- **Entity type:** Security Center entity type behind the map objects you want to import.
- **Block:** Block definition to be associated to the selected entity type.
- **Name attribute:** Block attribute that holds the block instance name that must match the entity name.
- **Name comparison:** Search for entity names by **Exact match** or **Starts with**.
- **Latitude attribute:** Block attribute that holds the GPS latitude of the map object.
- **Longitude attribute:** Block attribute that holds the GPS longitude of the map object.

8 If you get a No result found message, change your settings and try again.

9 Click **Synchronize**.

The matches found in the AutoCAD file are listed.



Synchronize entities from AutoCAD

☑ 2 map items to be created

Name	Entity type	AutoCAD block	AutoCAD name attribute	Status
Parking zone (HBS-PARKPLATZ)	2			
606_30_G_0212_02	Parking zone	HBS-PARKPLATZ	NAME	To be created
606_30_G_0212_03	Parking zone	HBS-PARKPLATZ	NAME	To be created

NOTE: If the mapped latitude and longitude block attributes contain invalid values, no entities will be synchronized.

10 If necessary, associate more AutoCAD blocks with Security Center entity types.

11 Export your synchronization settings to an XML file for reuse.

a) Click **Export**.

b) In the file browser that opens, enter a file name and click **Save**.

An XML file that captures the AutoCAD blocks to Security Center entity type synchronization settings is created. You can reuse those settings the next time you create an AutoCAD map with the same block definitions.

12 Click **Synchronize**.

The map objects you imported are displayed on your map.

Related Topics

Updating map objects imported from AutoCAD on page 331

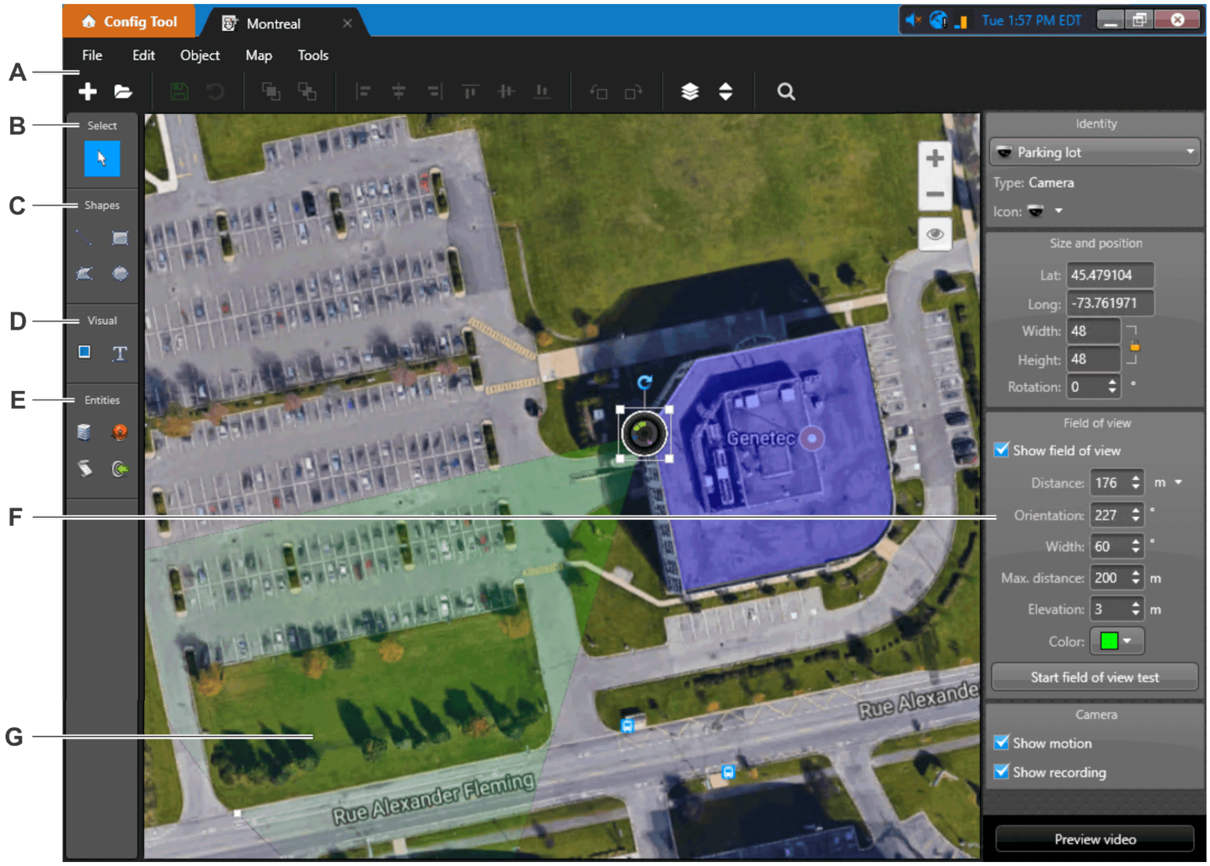
Adding map objects to your maps on page 336

Importing map objects from AutoCAD on page 309

Overview of the Map designer task

Use the Map designer task to create and edit maps that represent physical locations of your equipment to Security Desk users.

A map in Security Center is a two-dimensional diagram that helps you visualize the physical locations of your security equipment in a geographical area or a building space. The following figure shows the *Map designer* task editing a map named "Montreal" in a video monitoring system.



Identity

Parking lot

Type: Camera

Icon:

Size and position

Lat: 45.479104

Long: -73.761971

Width: 48

Height: 48

Rotation: 0 °

Field of view

☑ Show field of view

Distance: 176 m

Orientation: 227 °

Width: 60 °

Max. distance: 200 m

Elevation: 3 m

Color: 🟩

Start field of view test

Camera

☑ Show motion

☑ Show recording

Preview video

A Use the *Map designer* menu and toolbar to create, edit, and delete the maps in your system, as well as arrange and search for *map objects* on your map. On geographic maps, you can also search for addresses and coordinates.

B **Selection tool** (↖): Click a map object to select it. You can also do the following:

- Click and hold the map background to move it.
- Zoom in to an area of the map by holding the Ctrl key, and then clicking and dragging.
- Select multiple map objects with a rectangle, by holding the Alt key, and then clicking and dragging.
- Select all the map objects of the same type that are in view, by holding the Alt key, and then clicking a map object.

C	Draw vector objects: - **Draw line:** Click and drag to draw a single-line segment to represent a wall. - **Draw rectangle:** Click and drag to draw a rectangle. Drag a handle to change its size. You cannot change a rectangle into a different type of polygon. - **Draw polygon:** Click once for each endpoint, and click the first endpoint to close the polygon. Use Shift+click to add or remove a point between two points. Double-click a point to complete the polygon without closing it.
D	Insert images and text: - **Draw ellipse:** Click and drag to draw an ellipse. Drag a handle to change its size. - **Insert image:** Opens a browser for you to select an image file, and click to place it on the map. - **Insert text:** Click to place a text box on the map. Double-click the text box to enter the text. Use the widgets to adjust the appearance of the text.
E	Create map objects representing entities: - **Area view:** Click the area view to create map objects representing areas, intrusion detection areas, cameras, camera sequences, monitoring layouts, doors, ALPR cameras, and zones. - **Alarms:** Click, select, and drag an alarm to the map. - **Macros:** Click, select, and drag a macro to the map. - **I/Os:** Click, select, and drag an input pin, output relay, or a unit to the map. **NOTE:** It is possible to select I/Os federated and local cameras.
F	Use the widgets to configure the selected map object. When multiple map objects are selected, only the common widgets are displayed.
G	Click and drag the FOV to position it on the map.

Supported map objects

Map objects are graphical representations on your maps of Security Center entities or geographical features, such as cities, highways, rivers, and so on. With map objects, you can interact with your system without leaving your map.

Map objects are represented by dynamic icons or colored shapes that you can point to and click. You can configure the appearance of most map objects.

The following map objects are supported:

Map object	Default appearance on maps	Usage and specific actions
Access control unit	• - Access control unit in *Online* state • - Access control unit in *Offline* state • - Access control unit in *Warning* state	• Monitor the state of the access control unit.
Alarm	• - Inactive alarm • - Active alarm • Semi-transparent polygon or ellipse that matches the color of the alarm and flashes if the alarm is active. • A map object linked to an active alarm is flagged with an alarm notification bubble that has the same color as the alarm. • If **Display alarms from linked maps** is enabled in the *Maps* section of the Security Desk options, the number of active alarms on a linked map is shown on the *Maps* task toolbar, floor controls, and links to that map.	• Shows alarms on maps, lets you investigate, acknowledge, snooze, or forward the alarm, and lets you review the alarm procedure. • Useful when no entities attached to the alarm are represented on maps. • Point to the bubble to show more details. • Click the notification bubble to replace it with a tile bubble. • (Inactive) Click to trigger the alarm manually. • (Active) Click to display the alarm in a tile bubble.
ALPR camera	• - Fixed ALPR camera • - ALPR camera is in maintenance mode. • Reads and hits are shown in notification bubbles.	• Monitor the reads and hits from ALPR cameras. • Click to view live video from the associated context camera.
Area	• Map thumbnail (always linked to the map that it represents) • Colored semi-transparent polygon or ellipse (optionally linked to a map)	• Point to show people count or people presence, if enabled. • Remove selected cardholders from the area. • Click to display the area or map in a tile bubble, or to switch to a linked map, if defined.

Map object	Default appearance on maps	Usage and specific actions
Camera	• - Camera is not recording. • - Camera is recording. • - Camera detected motion (with green ripple effect). • - Camera is in maintenance mode. • Fixed cameras are shown with a blue field of view (FOV). • PTZ cameras are shown with a green FOV.	• Monitor alarms and camera events. • Click to view live or playback video in a tile bubble. • If the camera supports position feedback, click and drag the FOV to pan and tilt. • Use the PTZ widget to zoom in and zoom out. • Click the map while holding the Ctrl key to point all available cameras to that location.
Camera sequence	• - Camera sequence	• Display multiple cameras at the same time. • Point PTZ cameras to a specific location. • Double-click the camera sequence to display all the cameras in separate tiles in the *Monitoring* task. If the map is displayed in a tile, it is not replaced if tiles are full. **NOTE:** The **Locate me** right-click command finds individual cameras in the camera sequence, not the camera sequence itself.
Cluster bubble	• 5+ - Three or more map objects, when placed too closely to be visible at a given zoom level, are represented by a blue cluster bubble. The bubble shows a count of the objects inside it. **NOTE:** The count of clustered objects uses the following group sizes: 3, 4, 5, 10, 20, 50, 100, 200, 500. Counts in between these sizes, or larger, are indicated by a plus sign (+).	• Click to zoom in on the map to view the individual map objects.
Custom object	• Custom objects can be added to the map as icons or polygons to add custom behavior to the map.	Examples of custom objects include custom intercom solutions and GPS tracker for mobile units. Contact us for information on Genetec™ Custom Solutions.
Door	• - Door open • - Door closed and no lock is configured • - Door closed and locked • - Door closed and unlocked • - Door forced open • - Door unlocked and in maintenance mode • - Door unsecured • Events are displayed in event notification bubbles. The color of the bubble matches the color assigned to the event.	• Monitor alarms, door states, and events. • Point to the bubble to show more details. • Click the notification bubble to replace it with a tile bubble. • Unlock the door, override the unlock schedule, shunt the reader, and shunt inputs by using the *Door* widget or by right-clicking the door on the map.

Map object	Default appearance on maps	Usage and specific actions
Esri object	• Clickable objects that come with Esri ArcGIS maps. These have a similar function to KML objects.	• Overlays useful information on maps, such as city boundaries, roads, and hydrographic features. • Can represent moving objects, such as patrol vehicles, by refreshing their positions on the map at regular intervals.
Input pin	• 🟢 - Input in *Normal* state • 🔴 - Input in *Active* state • 🟡 - Input in *Trouble (short circuit)* or *Trouble (open circuit)* state • ⚪ - Input in *Unavailable* state • The state colors are configurable, and the icon can be shown or hidden depending on the state. Intrusion inputs with defined types: • - Burglary-type intrusion input • - Door-type intrusion input • - Fence-type intrusion input • - Fire-type intrusion input • - Gas-type intrusion input • - Motion-type intrusion input • - Panic-type intrusion input • - Virtual-type intrusion input • - Window-type intrusion input	• Monitor the input state. • Monitor intrusion detection areas. Inputs used for intrusion detection have other visual indicators: • The *Bypass* state is indicated with an 'X' superimposed on the input icon. With the *Modify intrusion detection unit properties* privilege, you can bypass an input or clear a bypass by right-clicking the input icon and selecting from the context menu. • The *Active alarm* state is indicated by a red, pulsing halo around the input icon. • Left-clicking an intrusion input pin displays a pop-up with the entity name, color-coded status, alarm status, bypass state, parent area, and the alarm sources (virtual inputs only). • The state of an input with a defined type is indicated with a dot superimposed on the lower left corner of the input icon. **NOTE:** You can change the icons of the input types on the *Input definitions* page of the Intrusion Manager role.
Intrusion detection area	• - Intrusion detection area • The different states are: • Disarmed (not ready) • Disarmed (ready to arm) • Arming • Perimeter armed • Master armed • Alarm active • The state colors are configurable, and the icon can be shown or hidden depending on the state.	• Monitor alarms and intrusion detection area state. • Arm or disarm the intrusion detection area from the widget, or by right-clicking the map object. • Trigger, silence, or acknowledge an intrusion alarm from the intrusion detection area widget, or by right-clicking the map object. • Change the *Bypass* state of one or multiple inputs by right-clicking the map object, and right-clicking the inputs.

Map object	Default appearance on maps	Usage and specific actions
KML object	• Can be anything displayed as a clickable transparent layer over a georeferenced map.	• Overlays static features on maps, such as city boundaries, roads, and hydrographic features. • Can represent dynamic information, such as weather conditions and traffic flow, by refreshing the map layer at regular intervals.
Layout	• ▦ - Layout • A map object that is linked to a previously saved monitoring task layout.	• Click to display the monitored cameras as a sequence in a tile bubble. • Double-click to display all the cameras in separate tiles in the *Monitoring* task. If the map is displayed in a tile, it is not replaced if tiles are full.
Macro	• 📜 - Macro	• Execute macros directly from maps. • Override the default execution context on maps. • Click a macro to run it.
Map link	• Map thumbnails, text, icons, images, or colored geometrical shapes.	• Click to switch to the linked map. • Enables map navigation without using the Maps toolbar. • Useful when the map is displayed in the *Monitoring* task. **NOTE:** If **Display alarms from linked maps** is enabled in the map options, the number of active alarms on a linked map is shown on the link to that map.
Mobile user	• 👤 - Mobile user with no picture	• When showing mobile users on maps is enabled, shows mobile users and lets you message them and share entities. • Point to the bubble to show the Security Center username. • Bubble displays the user's picture, if available.

Map object	Default appearance on maps	Usage and specific actions
Output relay	• - Output relay in *Normal* state • - Output relay in *Active* state • - Output relay in *Unknown* state	• Trigger output relays directly from maps. • Click to show a list of behaviors you can trigger. • For intrusion outputs: • With the *Trigger output* privilege, right-click the output icon to change the output state from a context menu. The state can be changed from: • *Normal* to *Active* • *Active* to *Normal* • *Unknown* to either *Normal* or *Active* • Click to display a pop-up with the entity name, state, and assigned output behaviors.
Parking zone	• P - Parking zone marker • Colored semi-transparent polygon (optionally linked to a map)	• Click the marker to display the parking zone occupancy and number of violations in a pop-up. • Click the polygon to jump to the map assigned to the parking zone.
Reader	• - Reader is in *Enabled* (or *Active*) state • - Reader is in *Disabled* (or *Shunted*) state • - Reader is in *Offline* state • - Reader is in *Warning* state • The *Enabled* and *Disabled* state colors are configurable and their state indicator can be shown or hidden.	• Monitor reader states. • Shunt (disable) or activate readers.
Records	• Records are data structured according to a given *record type* and intended to enhance situational awareness or add context to your maps. The display of records on maps is controlled by the *Record Fusion Service*. • A - Default representation with the first letter of the record type name • ☎ - Custom representation with user-selected color and icon • Records can also be represented as colored polygons.	• Click the pin or the polygon to view the record details in an information bubble. • Right-click anywhere on the map and then select **Add new data on map**. A dialog box opens in which you can add a record using a preconfigured record type at the position you clicked. This only works for record types managed by Record Caching Service roles.

Map object	Default appearance on maps	Usage and specific actions
Text, images and geometrical shapes	• Text, icons, images, and colored shapes (polygons and ellipses)	• These can be added to maps to provide additional information, indicate the location of points of interest, or serve as map links or alarms. For example, one usage might be to indicate the location of wall-mounted scanners on a department store floor plan.
Zone	• - Zone • - Virtual zone • - I/O zone • The different states are: *Disarmed*, *Normal*, *Active*, and *Trouble*. • The state colors are configurable, and the icon can be shown or hidden depending on the state.	• Monitor alarms and zone state. • Arm and disarm the zone from the widget.

Best practices for map search

When searching a map for map objects, addresses, or coordinates, there are a few best practices you should take into consideration.

- Searches in Config Tool only list map objects found on the selected map.
- Coordinates and addresses can only be used as search terms on geographic and georeferenced maps.
- Address searches must be written out in full with their street suffix, or entered by ZIP or postal code.

Enabling the AutoCAD import feature

To import AutoCAD blocks as map objects, you must first enable the AutoCAD block import feature.

Before you begin

Contact your representative of Genetec Inc. to enable this feature on your system.

What you should know

In AutoCAD, a block is a collection of geometric shapes that are combined into a single named object that you can use repeatedly. Like Security Center entities, AutoCAD blocks can represent real-world objects such as cameras, doors, readers, and so on.

If you synchronize an AutoCAD block definition with a Security Center entity type, you can import the block instances as map objects during the map creation process, or after the map is created.

To import an AutoCAD block instance, the block instance name must match an existing Security Center entity name. To import AutoCAD blocks to a geographic map, the block definition must have latitude and longitude attributes.

IMPORTANT: To import door readers, the block instance name must follow the format "DoorName (DoorSide)", where *DoorName* is the name of the door entity, and *DoorSide* is the name of the door side where the reader is installed. Door sides are named "In" and "Out" by default in the *Hardware* page of the door.

To enable the AutoCAD block import feature:

1. In a text editor, open the *Lnk.Maps.config* file.

   This file is located in the *ConfigurationFiles* folder of your Security Center installation folder.
2. Add the following code to the <Maps> line:

   ```
   EnableAutoCadImport="True"
   ```
3. Save the *Lnk.Maps.config* file, and then restart Config Tool.

A new command, **Synchronize entities from AutoCAD**, is added to the **Map** menu of the *Map designer* task. The next time you create a map from an AutoCAD file, the step, *Synchronize entities from AutoCAD (optional)*, will follow the step *Choose your background*, in the map creation process.

Related Topics

Importing map objects from AutoCAD on page 309

Importing map objects from AutoCAD to geographic maps on page 317

Updating map objects imported from AutoCAD

If you update the AutoCAD file used to import map objects to your map, you can resynchronize your map with the updated AutoCAD file without having to recreate the map.

What you should know

You can add, move, and delete the map objects imported from an AutoCAD file by resynchronizing the map with the updated AutoCAD file.

To update the map objects imported from AutoCAD:

1 Open the *Map Designer* task and select the map that you want to update.

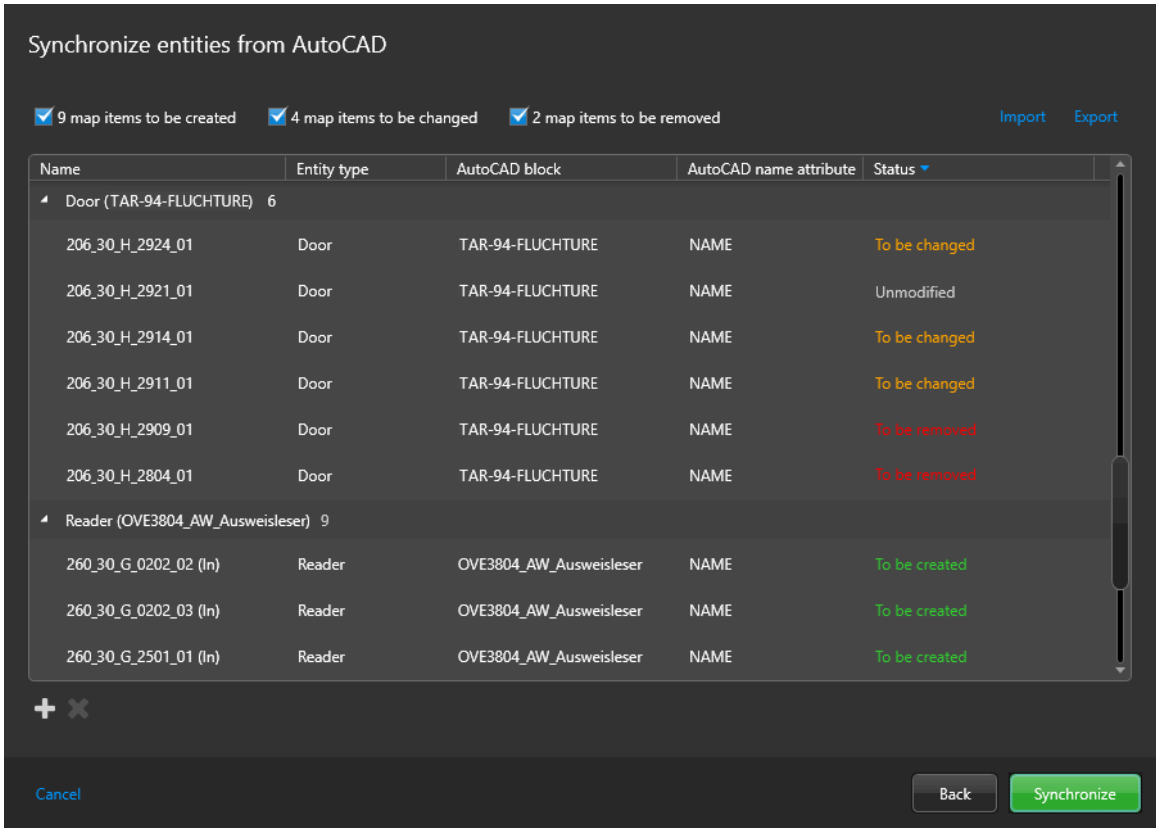
2 Click **Map** > **Synchronize entities from AutoCAD**.

3 Click **Select file**, select the AutoCAD file you want to import from, and click **Open**.

A thumbnail of the AutoCAD image is shown.

4 Click **Next**.

The entities flagged for synchronization are listed. Expand each group to see whether map objects are going to be modified, added, or removed. Clear a group of changes to exclude them from the synchronization.



Synchronize entities from AutoCAD

☑ 9 map items to be created ☑ 4 map items to be changed ☑ 2 map items to be removed

Name	Entity type	AutoCAD block	AutoCAD name attribute	Status
Door (TAR-94-FLUCHTURE) 6				
206_30_H_2924_01	Door	TAR-94-FLUCHTURE	NAME	To be changed
206_30_H_2921_01	Door	TAR-94-FLUCHTURE	NAME	Unmodified
206_30_H_2914_01	Door	TAR-94-FLUCHTURE	NAME	To be changed
206_30_H_2911_01	Door	TAR-94-FLUCHTURE	NAME	To be changed
206_30_H_2909_01	Door	TAR-94-FLUCHTURE	NAME	To be removed
206_30_H_2804_01	Door	TAR-94-FLUCHTURE	NAME	To be removed
Reader (OVE3804_AW_Ausweisleser) 9				
260_30_G_0202_02 (In)	Reader	OVE3804_AW_Ausweisleser	NAME	To be created
260_30_G_0202_03 (In)	Reader	OVE3804_AW_Ausweisleser	NAME	To be created
260_30_G_2501_01 (In)	Reader	OVE3804_AW_Ausweisleser	NAME	To be created

5 (Optional) To change the list of entities you want to synchronize, click **Import**, **Add** (✚), or **Remove** (✖).

6 Click **Synchronize**.

7 If you have entities to be removed in your list, confirm by clicking **Yes**.

The map objects on your map are updated.

Related Topics

Importing map objects from AutoCAD on page 309
Importing map objects from AutoCAD to geographic maps on page 317

Importing map objects from flat files

You can create or update map objects by importing them from a flat file. The new map objects can be automatically linked to Security Center entities by their name or GUID.

Before you begin

Create a geographic map or a georeferenced image map.

What you should know

You can import map objects from the following file types:

- **JSON:** JavaScript Object Notation.
- **BSON:** Binary JSON.
- **CSV:** Comma-separated values.
- **TSV:** Tab-separated values.
- **SSV:** Semi-colon-separated values.
- **GPX:** GPS Exchange Format.
- **KML, KMZ:** Keyhole Markup Language.

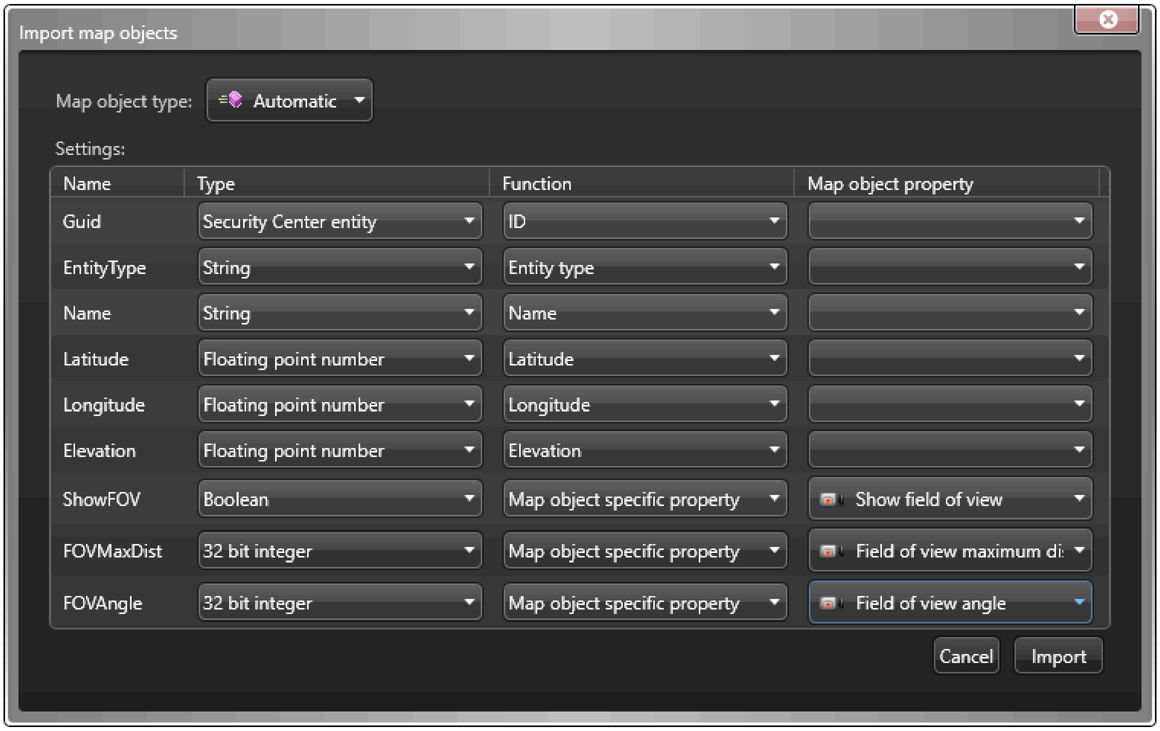
IMPORTANT: For file formats that contain one entry per row, such as XLS and CSV files, the first row must be a header row. This is how the Import tool extracts the field names.

To import map objects from a flat file:

1 From the *Map designer* task, open the map into which you want to import the map objects.

2 Click **File** > **Import** > **Map objects**.

3 In the file browser that opens, select the file you want to import and click **Open**.
The *Import map objects* dialog box opens, listing the property fields read from the file.



Import map objects

Map object type: Automatic

Settings:

Name	Type	Function	Map object property
Guid	Security Center entity	ID	
EntityType	String	Entity type	
Name	String	Name	
Latitude	Floating point number	Latitude	
Longitude	Floating point number	Longitude	
Elevation	Floating point number	Elevation	
ShowFOV	Boolean	Map object specific property	Show field of view
FOVMaxDist	32 bit integer	Map object specific property	Field of view maximum di:
FOVAngle	32 bit integer	Map object specific property	Field of view angle

4 Configure the settings of each field read from the file.

Each field is characterized by the following:

- **Name:** Name of the field read from the file.
- **Type:** Field data type. The possible values are:
  - **String:** An alphanumeric string.
  - **32 bit integer:** An integer in the range -2,147,483,648 to 2,147,483,647.
  - **64 bit integer:** An integer in the range -9.223372x10^{18} to 9.223372x10^{18}
  - **Floating point number:** A floating point number.
  - **Boolean:** A Boolean value expressed as 1 or 0, or a string containing one of the following: "True", "False", "true", "false", "T", or "F".
  - **Security Center entity:** A GUID representing the internal ID of a Security Center entity.
  - **Binary - file:** String containing the path to a file on disk. It can be an image file containing an icon or a Well-Known-Text (WKT) file containing the definition of a polygon.
- **Function:** Standard map object property assigned to that field. If a field is not needed, leave this column blank. The standard map object properties are:
  - **Latitude, Longitude:** These two functions must be assigned together. The *Latitude* and *Longitude* fields define the position of the map object on the map.
  - **Location:** This function is equivalent to the *Latitude* and *Longitude* functions. They are mutually exclusive. A field assigned to the *Location* function must contain a string in the format {"Latitude": n.nnnn, "Longitude": n.nnnn}.
  - **ID:** GUID of the Security Center entity represented by this map object. This function must correspond to the *Security Center entity* data type.
  - **Name:** Name of the Security Center entity represented by this map object.
  - **Entity type:** Type of the Security Center entity represented by this map object. This function must correspond to *String* data type. The value of the field must correspond to one of the Security Center entity type in English. For example, "Camera" for a camera entity, "Door" for a door entity, and so on.
  - **Elevation:** Elevation of the map object. Not all map object types require an elevation.
  - **Map object specific property:** This function is used to define the less common properties that are not shared by all map object types. If you select this function, you must define the map object property in the next column.
- **Map object property:** Specific map object property assigned to that field. If you set the **Function** of the field to *Map object specific property*, you must select a value here. Otherwise, you can leave this column blank.

  Make sure that the selected field **Type** corresponds to the map object property you select. For example, if you select the *Image* property, the data type must be set to *Binary - file*.

5 Click **Map object type** and select how the Import tool is going to determine the map object types.

If you select a specific map object type, such as *Camera* or *Door*, the Import tool expects to find a Security Center entity can be linked to the map object, and the properties that go along with the map object type. If it cannot find an entity in your system that matches the data in a file entry, that entry is skipped. If your file contains map objects of different types, you can use this method to import only one type of map objects and skip all the rest.

If you select **Automatic**, you must have enough information in your file for the Import tool to determine the map object type. This is how the Import tool determines the map object type based on the data found in a file entry:

a. Look for an **ID** field. If there is one, find the entity whose GUID corresponds to this ID.

   If the entity exists, the map object type and name is taken from the entity, and the entity is linked to the map object.

b. If there is no **ID** field, look for a clue in the **Name** field.

   If a single match is found, the map object type and name is taken from the entity, and the entity is linked to the map object.

c. If there is no **Name** field, skip the file entry.

d. If there are multiple entities matching that name, look for a clue in the **Entity type** field.

   If a single match is found, the map object type and name is taken from the entity, and the entity is linked to the map object.

e. If there is no **Entity type** field, look for a clue from the list of map object specific properties.

   For example, the presence of a 📹 **Show field of view** property suggests that we are looking for a camera.

   If a single match is found, the map object type and name is taken from the entity, and the entity is linked to the map object.

f. If the tool determines that the map object is not linked to a Security Center entity, such as an image, a text, or a shape, create the map object as such.

g. If no clue is found, skip the file entry.

NOTE: After the Import tool determined what the map object type is, it only looks at the properties that are relevant to that map object type. All other properties are ignored. If compulsory properties are missing, the file entry is skipped.

6 Click **Import**.

   Depending on the number of entries in your file, the operation might take a while. When the import process completes, the number of map objects added, the number of map objects updated, and the total number of entries found in the file, are indicated in a message box.

7 Click **OK** to accept the changes.

   The map zooms to a level where all the imported map objects can be shown in a single view.

8 Click **Save** (💾).

Adding map objects to your maps

For the maps that you create to be interactive, you must add map objects to the maps.

What you should know

- Map objects are graphical representations on your maps of Security Center entities or geographical features, such as cities, highways, rivers, and so on. With map objects, you can interact with your system without leaving your map.
- If you are creating a map that shares cameras or other entities with another map, you can copy and paste the entities and their configurations from one map to another.

To add a map object to your map:

1. From the Config Tool homepage, open the *Map designer* task.
2. Select a recent map or click **Browse all maps** to open an existing map.

   The selected map fills the *Map designer* workspace.
3. Do one of the following:
   - Add an access control unit.
   - Add an area.
   - Add a door.
   - Add a reader.
   - Add a camera.
   - Add a camera sequence.
   - Add a layout.
   - Add a parking zone.
   - Add a fixed LPR camera.
   - Add an alarm.
   - Add an intrusion detection area.
   - Add a zone.
   - Add an input pin.
   - Add an output relay.
   - Add a KML object.
   - Add a macro.
   - Add a point of interest.

After you finish

View and test your map objects in Security Desk with the *Maps* task.

Related Topics

Overview of the Map designer task on page 321

Importing map objects from AutoCAD on page 309

Importing map objects from AutoCAD to geographic maps on page 317

Adding access control units to your maps

You can add access control units to your maps to allow Security Desk operators to monitor the states of access control units from maps.

Before you begin

- Create the map to which you want to add your access control unit.
- Make sure you have access control units in your system.

To add an access control unit to your map:

1 From the Config Tool homepage, open the *Map designer* task.

2 Select a recent map or click **Browse all maps** to open an existing map.

The selected map fills the *Map designer* workspace.

3 In the toolbar, click **I/Os** (), select the access control unit () you want to add, and drag it to where you want it to be on the map.

The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.

4 In the *Map designer* toolbar, click **Save** ().

Adding areas to your maps

You can add areas to your maps to allow Security Desk operators to use them as map links, monitor people counts, show people presence, or all the above.

Before you begin

Create the map where you want to add your areas.

What you should know

- Areas that have a map attached are represented as map thumbnails by default. The map thumbnails are meant to be used as *map links*.
- Areas that do not have a map attached are represented as tetragons by default. You can change them later into any type of polygon.
- You can also use any icon, image, or geometrical shape to represent areas on the map.

To add an area to your map:

1. Do one of the following:
   - Add an area as a map thumbnail.
   - Add an area for monitoring people counts.
   - Add an area as a custom shape or image.
2. In the *Map designer* toolbar, click **Save** (💾).

Related Topics

Overview of the Map designer task on page 321

Adding areas as map thumbnails to your maps

You can add areas with a map attached, as map thumbnails to a map, and use them as map links.

Before you begin

- Create the map where you want to add your map thumbnails.
- Make sure you have other maps you want to link to from your current map.

To add an area as a map thumbnail to your map:

1. From the Config Tool homepage, open the *Map designer* task.
2. Select a recent map or click **Browse all maps** to open an existing map.
   The selected map fills the *Map designer* workspace.
3. In the toolbar, click **Area view** (🏢), select the map (🏢) you want to link to, and drag it to where you want its thumbnail to be on the current map.
   A large thumbnail of the target map appears on your current map.
4. Resize and position the thumbnail to the location you want, using the mouse.
5. In the *Map designer* toolbar, click **Save** (💾).

Adding areas for people counting to your maps

You can add secured areas to your maps to view people counts on maps.

Before you begin

- Create the map where you want to add your areas to.
- Make sure you have secured areas configured for people counting in your system.

To add an area for people counting to your map:

1. From the Config Tool homepage, open the *Map designer* task.
2. Select a recent map or click **Browse all maps** to open an existing map.

   The selected map fills the *Map designer* workspace.
3. In the toolbar, click **Area view** ( ), select the secured area ( ) you want to add, and drag it to where you want it to be on the map.

   A tetragon appears on the map.
4. Drag the corners of the tetragon to cover the physical space the secured area represents on the map.

   Use Shift+click to add or remove a point between two points.
5. Use the **Color and border** widget to change the display attributes of the map object.

   Select **Block field of view** if the perimeter of the secured area corresponds to actual walls.
6. (Optional) Click **Unassigned** in the **Links** widget to make the map object a *map link*.

   If you add multiple links to the map object, the operator must click three times to get to a link. The first click displays the entity that identifies the map object. The second click displays the choices of links. The third click selects a link.
7. In the *Map designer* toolbar, click **Save** ( ).

Adding text, images, and shapes to your maps

You can add text, images, and shapes to your maps to indicate points of interest, or to represent entities on the map with something other than the standard look. These map objects can also function as map links.

Before you begin

Create a map for your graphical objects.

What you should know

You can assign custom graphical objects to entities normally represented by polygons, such as areas, intrusion detection areas, and zones. You can also assign custom graphical objects to alarms.

To add a text or an image to your map:

1. From the Config Tool homepage, open the *Map designer* task.
2. Select a recent map or click **Browse all maps** to open an existing map.

   The selected map fills the *Map designer* workspace.
3. In the toolbar, click one of the following tools to insert a graphical object:
   - **Draw rectangle:** Click and drag to draw a rectangle. Drag a handle to change its size. You cannot change a rectangle into a different type of polygon.
   - **Draw polygon:** Click once for each endpoint, and click the first endpoint to close the polygon. Use Shift+click to add or remove a point between two points. Double-click a point to complete the polygon without closing it.
   - **Draw ellipse:** Click and drag to draw an ellipse. Drag a handle to change its size.
   - **Insert image:** Opens a browser for you to select an image file, and click to place it on the map.
   - **Insert text:** Click to place a text box on the map. Double-click the text box to enter the text. Use the widgets to adjust the appearance of the text.
4. (Optional) In the **Physical** widget, select **Block field of view** and use the object to block camera FOVs on the map.

   NOTE: The **Block field of view** option is not available for ellipses.
5. (Optional) Click **Unassigned** in the **Identity** widget to assign an entity to your map object.

   Map objects inherit their identity from the entity that they represent. You do not need to assign an entity to the map object if you are only using it to indicate a point of interest. Only map objects assigned to an entity have a name.

   NOTE: Assigning an area with floors to a graphical object automatically created links to those floors. Adding any links manually overrides the automatic links to the floors.
6. (Optional) Click **Unassigned** in the **Links** widget to make the map object a *map link*.

   If you add multiple links to the map object, the operator must click three times to get to a link. The first click displays the entity that identifies the map object. The second click displays the choices of links. The third click selects a link.
7. In the *Map designer* toolbar, click **Save** (💾).

Adding doors to your maps

You can add doors to your maps to allow Security Desk operators to monitor door events, manage alarms, and control door locks and readers from maps.

Before you begin

- Create the map where you want to add your doors.
- Make sure you have door in your Security Center system.

To add a door to your map:

1. From the Config Tool homepage, open the *Map designer* task.
2. Select a recent map or click **Browse all maps** to open an existing map.

   The selected map fills the *Map designer* workspace.
3. In the toolbar, click **Area view** (🏢), select the door you want to add, and drag it to where you want it to be on the map.

   The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.
4. In the *Map designer* toolbar, click **Save** (💾).

Related Topics

Overview of the Map designer task on page 321

Adding readers to your maps

You can add readers to your maps to allow Security Desk operators to monitor and control readers from maps.

Before you begin

- Create the map where you want to add your readers.
- Make sure you have doors configured with readers in your system.

To add a reader to your map:

1 From the Config Tool homepage, open the *Map designer* task.

2 Select a recent map or click **Browse all maps** to open an existing map.

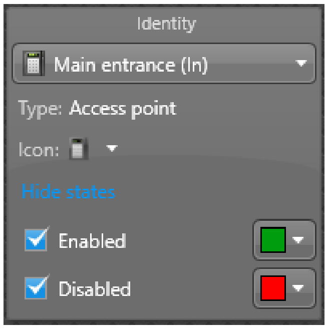
The selected map fills the *Map designer* workspace.

3 In the toolbar, click **Area view** (🏢), select the door (🚪), select the reader (📟) you want to add, and drag it to where you want it to be on the map.

The reader selections are always available whether the devices exist or not. If a device does not exist, the object appears offline (red) on the map.

The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.

4 In the **Identity** widget, click **Show states**, and then assign colors for the different reader states.



Identity

Main entrance (In)

Type: Access point

Icon: 📟

Hide states

☑ Enabled 🟩

☑ Disabled 🟥

NOTE: The system indicates the reader states, *Enabled* (or *Active*) and *Disabled* (or *Shunted*), by a colored dot on the reader icon. If you clear a state selection, the colored dot is hidden, but not the reader icon.

When the reader state changes, the state indicator changes to the color configured for that state, or hides the indicator.

5 In the *Map designer* toolbar, click **Save** (💾).

Related Topics

Overview of the Map designer task on page 321

Adding cameras to your maps

You can add cameras to your maps to allow Security Desk operators to monitor live video and camera events, manage alarms, and control PTZ cameras and recording from maps.

Before you begin

- Create the map where you want to add your cameras.
- Make sure you have cameras in your Security Center system.

What you should know

To create a more realistic effect when the map is displayed in the Maps task or Monitoring task in Security Desk, you can block the field of view of your cameras by drawing walls and other obstacles on your map.

To add a camera to your map:

1 From the Config Tool homepage, open the *Map designer* task.

2 Select a recent map or click **Browse all maps** to open an existing map.

The selected map fills the *Map designer* workspace.

3 In the toolbar, click **Area view** (), select the camera you want to add, and drag it to where you want it to be on the map.

The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.

4 Click **Preview video** to show a live video preview in a tile bubble.

5 Select **Show field of view**, and set the FOV properties.

IMPORTANT: Set the FOV properties even if you do not intend to show the FOV on the map. The orientation, width, and maximum distance of the FOV are necessary for the *Smart click* feature to work properly.

TIP: Alternatively, you can adjust the orientation and the length of the FOV with the mouse.

NOTE: If the map that you are adding the camera to is an imported image file, you must set the scale of the map to give meaning to the distances in the field of view properties. You can do this by georeferencing the map, or by setting the scale of the map.

- **Distance:** Length of the FOV as it appears on the map.
- **Orientation:** Direction the camera is pointing.
- **Width:** Width of the FOV as it appears on the map.
- **Max. distance:** Distance the camera can see. Mainly for *Smart click* calculations.
- **Elevation:** Height of the camera off the ground.

  TIP: Clicking **Start test field of view** shows blind spots created by other objects on the map.
- **Color:** Color of the FOV indicator.

6 Select the camera events that you wish to monitor on the map.

- **Show motion:** Shows the camera icon with a green ripple effect () on *Motion on* event.
- **Show recording:** Shows the camera icon with a red button () when recording is on.

7 In the *Map designer* toolbar, click **Save** ().

Related Topics

Setting the scale of an imported map image on page 312
Georeferencing a map image on page 314
Overview of the Map designer task on page 321
Drawing walls to block the cameras' fields of view on page 344

Drawing walls to block the cameras' fields of view

To create a more realistic effect when the map is displayed in the Maps task or Monitoring task in Security Desk, you can block the field of view of your cameras by drawing walls and other obstacles on your map.

What you should know

Only lines, rectangles, and polygons, can be used to block the field of view (FOV) of cameras. Text, images, and elliptical shapes cannot be used for blocking.

To draw an object to block the FOV of cameras:

1 From the Config Tool homepage, open the *Map designer* task.

2 Select a recent map or click **Browse all maps** to open an existing map.

The selected map fills the *Map designer* workspace.

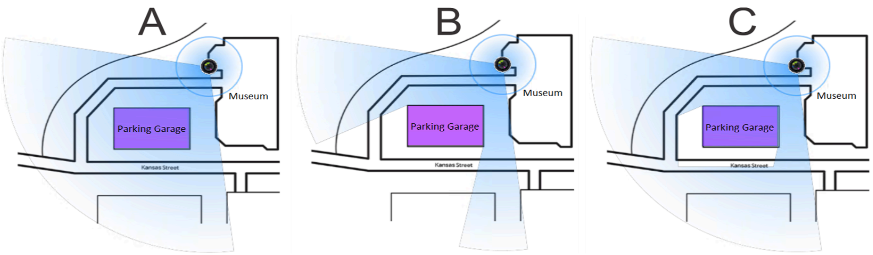
3 In the toolbar, click one of the following tools to insert a graphical object:

- **Draw line:** Click and drag to draw a single-line segment to represent a wall.
- **Draw rectangle:** Click and drag to draw a rectangle. Drag a handle to change its size. You cannot change a rectangle into a different type of polygon.
- **Draw polygon:** Click once for each endpoint, and click the first endpoint to close the polygon. Use Shift+click to add or remove a point between two points. Double-click a point to complete the polygon without closing it.

The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity it represents.

4 From the **Physical** widget, select **Block field of view** and set the **Elevation** of the wall. Using this elevation in conjunction with the elevation that is configured in the camera's **Field of view** widget provide a visual representation on the map of the blind spot created by the wall.

5 Test the blind spot created by the object by selecting the camera and clicking **Start test field of view** in the camera widget.



Example	Configuration
A	**Block field of view** is not selected for the rectangle representing the parking garage.

Example	Configuration
B	**Block field of view** is selected for the rectangle representing the parking garage.
C	**Block field of view** is selected for the rectangle representing the parking garage and the **Elevation** is defined for both the parking garage and the camera.

TIP: To test the coverage of all the cameras, click **Map** > **Show field of view coverage**.

6 In the *Map designer* toolbar, click **Save** (💾).

Related Topics

Adding cameras to your maps on page 343

Adding camera sequences to your maps

To allow Security Desk operators to focus on a point of interest, you can add camera sequences to your maps so that multiple cameras are displayed when you click a single map object.

Before you begin

- Create the map where you want to add your camera sequences.
- Make sure you have camera sequences in your Security Center system.

What you should know

A camera sequence marks a location on the map that requires special attention or close monitoring. You can configure a camera sequence so that when it is displayed, it turns all PTZ cameras that are part of it to a specific location (preset position).

To add a camera sequence to your map:

1. From the Config Tool homepage, open the *Map designer* task.
2. Select a recent map or click **Browse all maps** to open an existing map.

   The selected map fills the *Map designer* workspace.
3. In the toolbar, click **Area view** (), select the camera sequence you want to add, and drag it to where you want it to be on the map.

   The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.
4. In the *Map designer* toolbar, click **Save** ().

Related Topics

Overview of the Map designer task on page 321

Adding layouts to your maps

To allow Security Desk operators to view multiple cameras while focusing on the map, you can add layouts to your maps.

Before you begin

- Create the map where you want to add your *layout*.
- Make sure you have layouts in your Security Center system.

What you should know

On a map, a layout behaves like a camera sequence. When you click a layout on the map, the system displays in sequence, all the cameras associated with the layout in a single tile bubble. You can also double-click a layout on the map to open a *Monitoring* task with that layout.

To add a layout to your map:

1 From the Config Tool homepage, open the *Map designer* task.

2 Select a recent map or click **Browse all maps** to open an existing map.

The selected map fills the *Map designer* workspace.

3 In the toolbar, click **Area view** ( ), select the layout ( ) you want to add, and drag it to where you want it to be on the map.

The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.

4 In the *Map designer* toolbar, click **Save** ( ).

Related Topics

Overview of the Map designer task on page 321

Adding ALPR cameras to your maps

You can add fixed ALPR cameras to your maps to allow Security Desk operators to monitor reads and hits from maps.

Before you begin

- Create the map where you want to add your fixed ALPR cameras.
- Make sure you have fixed ALPR cameras in your Security Center system.

What you should know

To add a fixed ALPR camera to your map:

1 From the Config Tool homepage, open the *Map designer* task.

2 Select a recent map or click **Browse all maps** to open an existing map.

The selected map fills the *Map designer* workspace.

3 In the toolbar, click **Area view** (🏢), select the context camera (📹) attached to the fixed ALPR camera you want to add, and drag it to where you want it to be on the map.

NOTE: If you drag the ALPR unit (▭) or the ALPR camera (📷) onto the map, the system will display ALPR hits and reads instead of the context camera video feed.

The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.

4 In the **ALPR rules** widget, select a hotlist.

5 In the *Map designer* toolbar, click **Save** (💾).

Related Topics

Overview of the Map designer task on page 321

Adding alarms to your maps

You can add alarms to your maps to allow Security Desk operators to monitor and manage alarms from maps.

Before you begin

- Create the map where you want to add your alarms.
- Make sure you have alarms in your Security Center system.

What you should know

There are three ways to add alarms to a map:

- Add a map object, such as a door, that is attached to an alarm.
- Link an alarm to a custom shape on the map.
- Add an alarm object to the map.

During an active alarm, an alarm notification bubble is displayed above the map object associated with the alarm. These notification bubbles show alarms on the map and lets Security Desk operators investigate, acknowledge, snooze, or forward the alarm, and review the alarm procedure.

To add an alarm object to your map:

1 From the Config Tool homepage, open the *Map designer* task.

2 Select a recent map or click **Browse all maps** to open an existing map.
   The selected map fills the *Map designer* workspace.

3 In the toolbar, click **Alarms** (🚨), select the alarm you want to add, and drag it to where you want it to be on the map.
   The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.

4 In the *Map designer* toolbar, click **Save** (💾).

Related Topics

Overview of the Map designer task on page 321

Adding intrusion detection areas to your maps

You can add intrusion detection areas to your maps to allow Security Desk operators to monitor and control intrusion detection areas from maps.

Before you begin

- Create the map where you want to add your intrusion detection areas.
- Make sure you have intrusion detection areas in your system.

To add an intrusion detection area to your map:

1 From the Config Tool homepage, open the *Map designer* task.

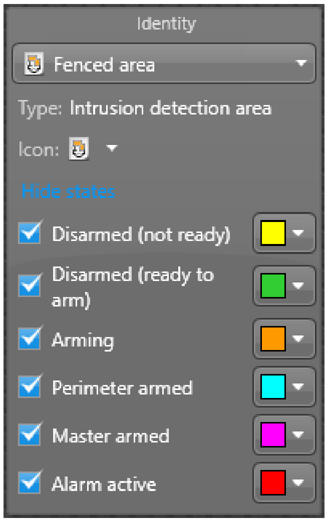
2 Select a recent map or click **Browse all maps** to open an existing map.

The selected map fills the *Map designer* workspace.

3 In the toolbar, click **Area view** ( ), select the intrusion detection area ( ) you want to add, and drag it to where you want it to be on the map.

The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.

4 In the **Identity** widget, click **Show states**, and then assign colors for the different states of the intrusion detection area.



Identity

Fenced area

Type: Intrusion detection area

Icon:

Hide states

☑ Disarmed (not ready) 🟨

☑ Disarmed (ready to arm) 🟩

☑ Arming 🟧

☑ Perimeter armed 🟦

☑ Master armed 🟪

☑ Alarm active 🟥

TIP: To avoid cluttering the map, you can hide the map object when the entity is found in certain states. Clear the states that you want to hide.

When the state of the intrusion detection area changes, the map object changes to the color configured for that state, or is hidden.

5 In the *Map designer* toolbar, click **Save** ( ).

Related Topics

Overview of the Map designer task on page 321

Adding zones to your maps

You can add hardware zones and virtual zones to your maps to allow Security Desk operators to monitor and control zones from maps.

Before you begin

- Create the map where you want to add your zones.
- Make sure you have zones in your system.

To add a zone to your map:

1 From the Config Tool homepage, open the *Map designer* task.

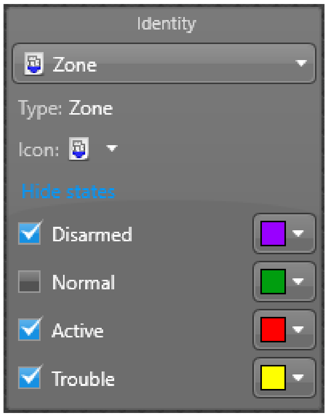
2 Select a recent map or click **Browse all maps** to open an existing map.

The selected map fills the *Map designer* workspace.

3 In the toolbar, click **Area view** (), select the hardware zone (), virtual zone (), or I/O zone () you want to add, and drag it to where you want it to be on the map.

The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.

4 In the **Identity** widget, click **Show states**, and then assign colors for the different zone states.



Identity

Zone

Type: Zone

Icon:

Hide states

☑ Disarmed 🟪

☐ Normal 🟩

☑ Active 🟥

☑ Trouble 🟨

TIP: To avoid cluttering the map, you can hide the map object when the entity is found in certain states. Clear the states that you want to hide.

When the zone state changes, the map object changes to the color configured for that state, or is hidden.

5 In the *Map designer* toolbar, click **Save** ().

Related Topics

Overview of the Map designer task on page 321

Adding input pins to your maps

You can add input pins to your maps to allow Security Desk operators to monitor the states of input pins from maps.

Before you begin

- Create the map where you want to add your input pins.
- Make sure you have input pin in your Security Center system.

To add a input pin to your map:

1 From the Config Tool homepage, open the *Map designer* task.

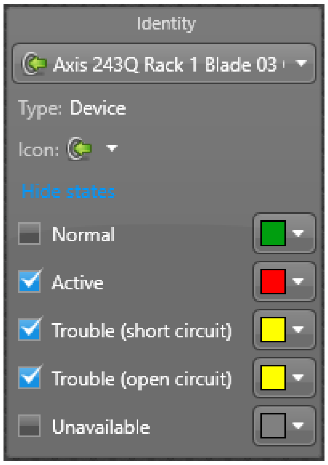
2 Select a recent map or click **Browse all maps** to open an existing map.

The selected map fills the *Map designer* workspace.

3 In the toolbar, click **I/Os** (), select the input pin () you want to add, and drag it to where you want it to be on the map.

The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.

4 In the **Identity** widget, click **Show states**, and then assign colors for the different input states.



Identity

Axis 243Q Rack 1 Blade 03 ▾

Type: Device

Icon: ▾

Hide states

☐ Normal 🟩 ▾

☑ Active 🟥 ▾

☑ Trouble (short circuit) 🟨 ▾

☑ Trouble (open circuit) 🟨 ▾

☐ Unavailable ⬜ ▾

TIP: To avoid cluttering the map, you can hide the map object when the entity is found in certain states. Clear the states that you want to hide.

NOTE: If you use the default input icon (), the map object is shown as a colored LED (●). If you change the icon, then the map object is represented by the icon you selected with a small LED icon superimposed on top.

When the input state changes, the map object changes to the color configured for that state, or is hidden.

5 In the *Map designer* toolbar, click **Save** (💾).

Related Topics

Overview of the Map designer task on page 321

Adding output relays to your maps

You can add output relays to your maps to allow Security Desk operators to trigger output behaviors on output relays from maps.

Before you begin

- Create the map where you want to add your output relays.
- Make sure you have output relay in your Security Center system.

To add an output relay to your map:

1 From the Config Tool homepage, open the *Map designer* task.

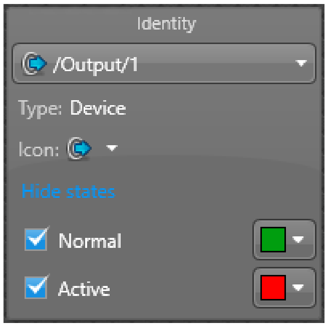
2 Select a recent map or click **Browse all maps** to open an existing map.

The selected map fills the *Map designer* workspace.

3 In the toolbar, click **I/Os** (), select the output relay () you want to add, and drag it to where you want it to be on the map.

The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.

4 In the **Identity** widget, click **Show states**, and then assign colors to the different output relay states.



Identity

/Output/1

Type: Device

Icon:

Hide states

☑ Normal 🟩

☑ Active 🟥

The system indicates the state, *Normal*, *Active*, or *Unknown*, as a color dot over the icon. The color representing the *Unknown* state cannot be changed.

TIP: To avoid cluttering the map, you can hide the map object when the entity is found in certain states. Clear the states that you want to hide.

When the state of the output relay changes, the state indicator changes to the color configured for that state, or the icon is hidden.

5 In the **Output behaviors** widget, click **Add action** (), select an output behavior and give it a name.

You can configure multiple output behaviors. When an operator clicks an output relay on the map, the available output behaviors appear in a menu bubble.

6 In the *Map designer* toolbar, click **Save** ().

Related Topics

Overview of the Map designer task on page 321

Adding KML objects to your maps

You can add geographic features and dynamic information, such as roads and traffic flow, to georeferenced maps. This is done by importing Keyhole Markup Language (KML) objects to the Map Manager role.

Before you begin

Create at least one georeferenced map.

What you should know

Keyhole Markup Language (KML) is a file format used to display geographic data in an Earth browser such as Google Earth and Google Maps. KML files define map objects that represent static features, such as roads and buildings, or dynamic information, such as weather conditions and traffic flow. They can only be used with georeferenced maps.

NOTE: Dynamic KML layers are refreshed on an interval defined in the KML file.

To add KML layers to your georeferenced maps:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the *Map Manager* role, and click the **Properties** tab.
3. Under the *Map layers* section, click **Add an item** (➕).
4. In the *Select layers to import* dialog box, enter the path to a *.kml* or *.kmz* file.

   If the file was loaded successfully, a preview of the KML objects and a list of available layers is displayed. All layers are selected by default.
5. If required, deselect any layers that are not needed.
6. Click **Import**, and then click **Apply**.

After you finish

By default, newly imported KML layers are automatically shown on all georeferenced maps. If the KML information is not required in some maps, you must hide the KML layers in the map configuration.

Adding macros to your maps

You can add macros to your maps to allow Security Desk operators to run macros from maps.

Before you begin

- Create the map where you want to add your macros.
- Make sure you have macro in your Security Center system.

To add a macro to your map:

1. From the Config Tool homepage, open the *Map designer* task.
2. Select a recent map or click **Browse all maps** to open an existing map.

   The selected map fills the *Map designer* workspace.
3. In the toolbar, click **Macros** (📜), select the macro (📜) you want to add, and drag it to where you want it to be on the map.

   The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity that it represents.
4. (Optional) In the **Macro properties** widget, click **Override default context** to set an execution context that is different from the default.

   Click **Clear** to revert to the default execution context.
5. In the *Map designer* toolbar, click **Save** (💾).

Related Topics

Overview of the Map designer task on page 321

About macros on page 223

14

Plugins

This section includes the following topics:

About plugin roles

A plugin role adds optional features to Security Center. A plugin role is created by using the *Plugin* role template. By default, it is represented by an orange puzzle piece in the *Roles* view of the *System* task.

Plugin (🧩) role template

Plugin (with an uppercase, in singular) is the role template that serves to create specific plugin roles.

About creating plugin roles (🧩)

Before you can create a plugin role, the software package specific to that role must be installed on your system. You must also make sure that your Security Center license has a valid *certificate* for the plugin you want to use.

For more information, see the individual *Plugin Guide* for the plugin you are using available for download from the TechDoc Hub. To log on to the Hub, you need a username and password.

About tile plugins

A tile plugin is a software component that runs inside a Security Desk tile. By default, it is represented by a green puzzle piece in the area view.

The tile plugin entity (🧩) represents either a website (🌐) or an interactive *.dll* or *.xaml* file.

When a tile plugin is displayed in Security Desk, you can view and interact with the website or the interactive plugin file. When a tile plugin is attached to an area entity, it is automatically displayed in Security Desk instead of the area icon when the area is dragged to a tile.

Creating tile plugins that link to a website

You can create a tile plugin that links to a web site that contains a map, which you can interact with when the tile plugin is displayed in Security Desk.

What you should know

Make sure that the URL you link the tile plugin can be reached from all Security Desk workstations, or some users might not be able to view the map or other content from the URL.

To create a tile plugin that links to a website:

1 Open the *Area view* task.

2 Click **Add an entity** (➕) > **Tile plugin**.

3 In the *Creating a tile plugin* wizard, enter the entity name and description.

4 If there are partitions in your system, select the partition the tile plugin is a member of, and click **Next**.

Partitions determine which Security Center users have access to this entity. Only users who have been granted access to the partition can see the tile plugin.

5 In the *Tile plugin information* page, select **Website**.

6 Click **Next** > **Close**.

The tile plugin appears in the area view with a website icon (●).

7 Select the tile plugin, and click the **Properties** tab.

8 In the **Web page** option, type a web address.

9 Click **Apply**.

Related Topics

About tile plugins on page 358

Creating tile plugins that link to an executable file

You can create a tile plugin that links to a .dll or .xmal file that contains an executable that you can interact with when the tile plugin is displayed in Security Desk.

Before you begin

The executable file must be created and located on your local computer.

To create a tile plugin that links to an executable file:

1. Open the *Area view* task.
2. Click **Add an entity** (✚) > **Tile plugin**.
3. In the *Creating a tile plugin* wizard, enter the entity name and description.
4. If there are partitions in your system, select the partition the tile plugin is a member of, and click **Next**.

   Partitions determine which Security Center users have access to this entity. Only users who have been granted access to the partition can see the tile plugin.
5. In the *Tile plugin information* page, select **Tile plugin**.
6. In Windows, select the .dll file that the tile plugin will link to, and click **Open**.
7. Click **Next** > **Close**.

   The tile plugin appears in the area view with the default icon (🧩).
8. Select the tile plugin, and click the **Properties** tab.
9. To select another executable file, click **Modify**, and select another .dll file.
10. Click **Apply**.

Related Topics

About tile plugins on page 358

15

Health monitoring

This section includes the following topics:

About the Health Monitor role

The Health Monitor role monitors system entities such as servers, roles, units, and client applications for health issues.

Health events are recorded in a database for the purpose of reporting and statistical analysis. Current system errors are reported in real time in your application's notification tray.

Only one instance of this role is permitted per system. It is created at system installation and cannot be deleted.

From the Heath Monitor role, you can choose which health events to monitor.

Resetting the Health Monitor database

After you initially set up your system, you should reset the health monitoring database to its original state.

What you should know

The process of setting up and configuring a system can generate many health events. It is normal that health errors and warnings are produced during this time. That is why it is important to restore the database to its original, clean state, so the health statistics of your system are reset.

To reset the Health Monitor database to its original state:

1. Open the *System* task and click the **Roles** view.
2. Select the **Health Monitor** role, and click the **Resources** tab.
3. Click **Delete the database** (✖).
4. When prompted if you want to delete this database, click **Delete**.

   The **Database actions** window opens.
5. When you see confirmation that the database has been deleted, click **Clear finished**, and then click **Close**.
6. In the toolbar at the bottom of the workspace, click **Deactivate role** (🚦).
7. Click **Activate role** (🚦).

   After 15-30 seconds, a new *HealthMonitor* database should be created in the Health monitor role's **Resources** tab.

The health errors and warnings generated during the setup are deleted, and all health statistics are reset.

Selecting health events to monitor

You can configure the Health Monitor role to ignore certain health events, and change how it generates some health events.

What you should know

If you want to ignore all health events, deactivate the *Health Monitor* role completely. If you want to temporarily ignore an entity's health events because you are performing maintenance work on it, set it to maintenance mode.

To select which health events to monitor:

1. Open the *System* task and click the **Roles** view.
2. Select the **Health Monitor** role, and click the **Properties** tab.
3. Under **Events to monitor**, select or clear the desired events.

   Most health events come in pairs, such as *Database lost* and *Database recovered*. They can only be selected or ignored together.

   IMPORTANT: Clearing a health event in the monitoring list does not remove it from the *Health history* query filter, but it could make some of the health statistics calculations impossible.
4. Add criteria for generating the events, as follows:

   Criteria are only supported for some events. For example, you can configure the *CPU usage high* health event to only generate on servers whose CPU runs higher than 80% for a period of 10 seconds.

   a) Select the event to modify, and click **Edit** (✏) at the bottom of the list.

   b) In the event **details** window, adjust the values as required, and click **Save**.
5. Click **Apply**.

Related Topics

Viewing system health events on page 374

Event types on page 1410

Configuring predefined reasons for maintenance mode

To facilitate the process of setting an entity in maintenance mode, you can create predefined reasons. You can also assign a color to each reason to help users quickly identify why an entity is in maintenance.

Before you begin

You must have the privilege to modify maintenance mode reasons.

What you should know

With predefined reasons, you can quickly assign a reason for putting an entity in maintenance mode without having to type it out each time. While in maintenance mode, the color assigned to the reason is applied to the User Interface (UI) elements of the entity (icon, label, and the selector) wherever they appear in the application, such as entity trees, tiles, and maps.

To configure a predefined maintenance mode reason:

1. From the Config Tool homepage, open the *System* task, click the *General Settings* view, and then click the *Maintenance mode reasons* page.
2. Click ➕ to open the *Add reason for maintenance mode* dialog box.
3. Give the reason a name.
4. Add a description. This text can be modified when setting the entity in maintenance mode and is shown as a tooltip when hovering over the entity.
5. Assign a color. The UI elements for the entity are highlighted in this color wherever it appears in the application. Choose a basic color from the selection or click **Custom** to create your own.

   NOTE: Use distinct colors so users can easily differentiate between the reasons. Also, it is not recommended to use the following colors because they already have an existing meaning in Security Center:

   - **Red:** Represents an entity that is offline state.
   - **Yellow:** Represents an entity that is in the warning state.
   - **Gray:** Represents an entity that is inactive.
   - **Orange:** Represents the default maintenance mode with no predefined reason specified.
6. Click **OK**.

The predefined reason is created and available as an option when setting an entity in maintenance mode.

Setting entities to maintenance mode

To change the configuration of an entity or perform maintenance on a device without affecting health statistics, you can set the entity to maintenance mode.

Before you begin

You must have the privileges to modify the entities you are working with. Cameras and doors also require a *Maintenance mode* privilege.

What you should know

- When an entity goes offline while it is in maintenance mode, the downtime is considered expected. Expected downtime is not used to calculate the availability of the entity in the *Health statistics* report.

  NOTE: Health events for entities in maintenance mode are reported with *Information* severity.
- You can set the following entities to maintenance mode:
  - Access control units
  - Alarms

    You cannot trigger alarms that are set to maintenance mode through event-to-actions or manually.

    NOTE: Setting an active alarm to maintenance mode does not acknowledge it.
  - ALPR units
  - Cameras
  - Custom entities that support maintenance mode
  - Hardware zones
  - Intrusion detection units
  - Patrol vehicles
  - Roles
  - Video units
- Maintenance mode for doors is called **Unlock for maintenance**.

  Unlock doors for maintenance purposes from the entity tree, and the *Properties* page of the door.

  Unlock for maintenance must be disabled manually by selecting **Disable maintenance mode**.

To set an entity to maintenance mode:

1. Open the appropriate task in Config Tool.
2. In the entity tree view, select the entity or entities, right-click and select **Maintenance** > **Maintenance mode**.
3. In the *Maintenance mode* dialog box, click **Turn ON**.
4. Select how long you want the entity to be maintenance mode for.

   Select one of the following options:
   - **Manually:** Maintenance mode must be manually turned off.
   - **Duration:** Maintenance mode is turned on for the number of days that you select.
   - **Specific end-time:** Maintenance mode is turned on until the date that you select.

   You can modify the duration while the entity is in maintenance mode.
5. Specify the reason that you are setting the entity in maintenance mode:
   - **If predefined reasons were configured:** Select a reason from the drop-down list. In the text box, add a description of the issue or adjust the existing text, if one is provided. This text is shown as a tooltip when hovering over the entity icon.

  NOTE: Every reason is assigned a color. All User Interface (UI) elements for the entity, such as its icon, label, and the selector, are highlighted in the color associated to the reason wherever they appear in the application. This helps users quickly identify why the entity is in maintenance mode. By default, no reason is specified and the entity icon is highlighted in orange.

- **If predefined reasons were not configured:** In the text box, add a description of the issue. This text is shown as a tooltip when hovering over the entity icon.

  NOTE: All User Interface (UI) elements for the entity, such as its icon, label, and the selector, are highlighted in orange.

6 Click **Save**.

The entity is in maintenance mode for the duration that you specified.

While the entity is in maintenance mode, the maintenance mode icon ( ) is displayed over the entity icon in the area view, in tiles, and on maps. All UI elements for the entity are highlighted in the color assigned to the maintenance mode reason. When you hover over these elements, the description for the maintenance mode reason is displayed.

Related Topics

Enabling events for cameras in maintenance mode on page 368

Enabling events for cameras in maintenance mode

By default, Security Center suppresses events from camera and video units while the devices are in *maintenance mode*. If you want related event-to-actions to continue to work when the devices are in maintenance mode, you can turn off the event suppression by modifying the *Archiver.gconfig* file.

What you should know

- When a camera is in maintenance mode, camera events like *Recording started* or *Signal lost* are not generated. When a video unit is in maintenance mode, events associated with the video unit or the cameras connected to the video unit are not generated, like *Unit lost* or*Input state changed*. Related event-to-actions are disabled when events are not generated.
- The *Archiver.gconfig* file has two sections: *ArchiverRole* and *ArchiverAgent*. The settings in the file apply to all the Archiver roles or Archiver agents that are hosted on the server. The maintenance mode setting is modified in the *ArchiverRole* section of the file.

CAUTION: Only modify a *.gconfig* file if you are sure that the changes are valid. Incorrect code in a *.gconfig* file can cause issues on your system or cause your system to go offline.

To enable events for cameras in maintenance mode:

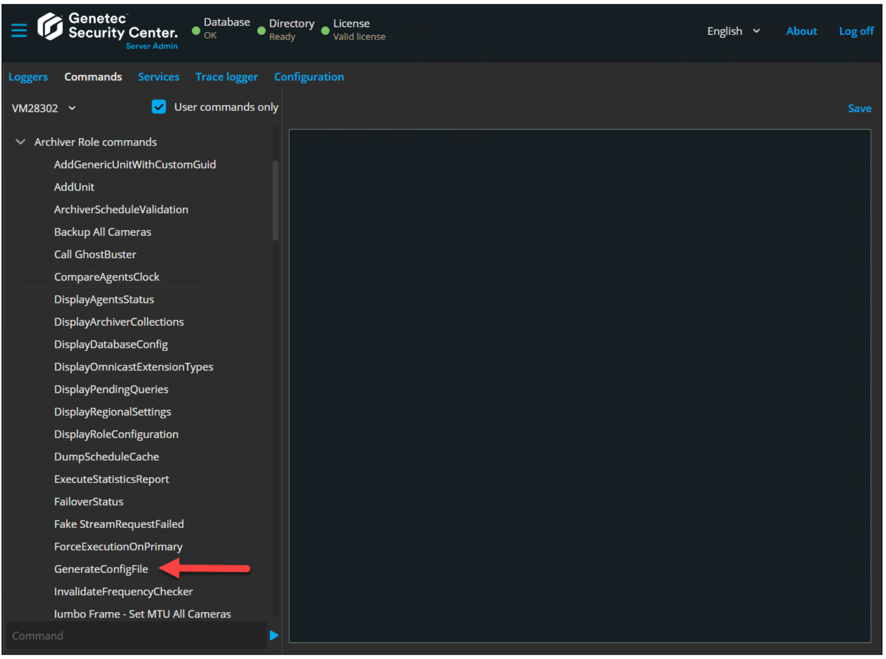
1 On the Archiver server, do one of the following:

- Back up the*Archiver.gconfig* file by copying it to another folder.

  The file is located by default in*C:\Program Files (x86)\Genetec Security Center 5.x\ConfigurationFiles* on a 64-bit computer and in*C:\Program Files\Genetec Security Center 5.x\ConfigurationFiles* on a 32-bit computer.
- If the *Archiver.gconfig* file does not exist, generate it as follows:

  a. Log on to Server Admin and select the server hosting the Archiver role.

  b. Click **Actions** > **Console** > **Commands** > **Archiver Role commands** > **GenerateConfigFile**.



2 Open the*Archiver.gconfig* file and change the `suppressUnitEventsInMaintenanceMode` option to `false`.

```
suppressUnitEventsInMaintenanceMode="false"
```

NOTE: If the *Archiver.gconfig* file already existed on the computer but the options are not listed, it is due to one of the following reasons:

- You have an outdated version of the file. Generate the file using step 1.
- The file was previously generated for the Archiver agent (**Actions** > **Console** > **Commands** > **Archiver Agent commands** > **GenerateConfigFile**), and you are missing the *ArchiverRole* section of the file. Generate the file using step 1.
- If you are using Archiver failover, the Archiver role might be running on a different server. Generate the file on the other server and copy it to this server.

3 Save the file and restart the Archiver role.

4 Repeat the procedure on every server that hosts an Archiver role.

Related Topics

Setting entities to maintenance mode on page 366

Setting Security Desk to maintenance mode

If you expect system downtime, you can set Security Desk to *maintenance mode* so that the health statistics of the application are not affected.

What you should know

Unexpected downtime, the time that an application is unavailable excluding planned maintenance, negatively affects the health statistics for that application. Any downtime while Security Desk is in *maintenance mode* is considered expected downtime, and is not used to calculate application availability.

NOTE: Setting Security Desk to *maintenance mode* does not stop the health events; however, it reports all health events as information only.

To set Security Desk to *maintenance mode*:

1 In Config Tool, open the *System* task, and click the **Roles** view.

2 Select the Health Monitor role, and then click the **Properties** tab.

3 Set **Security Desk maintenance mode** to **ON**, and click **Apply**.

Reviewing system messages

If you receive messages from the system, you can review them from the notification tray, and diagnose the trouble entities.

What you should know

You can receive three types of system messages:

- ✚ Health issues
- ⚠ Warnings
- ℹ Messages

NOTE: System messages are different from health events related to entities. The only system messages that have corresponding health events in the *Health history* report are the health issues. These corresponding health events have the *Error* severity level.

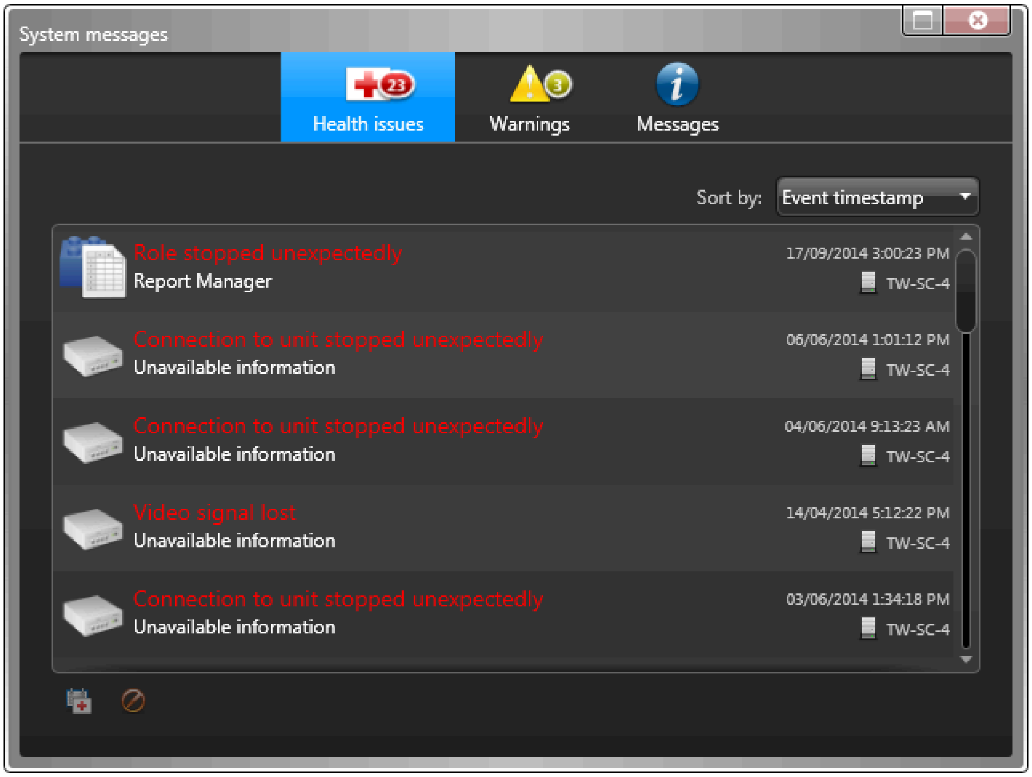
To review system messages:

1 In the notification tray, double-click the **System messages** (✚6) icon.

2 On the *Health issues* () page of the *System messages* dialog box, do one of the following:

- To sort the health issues, from the **Sort by** list, select how to display the health issues. You can sort them alphabetically by health event type, event timestamp, machine (computer name), or source (entity name).
- To open the configuration page of an entity, click the entity.
- To launch the *Health history* task and view system health events, select a health event, and then click **Health history** ().
- To dismiss a health issue, select it, and then click **Dismiss health event** ().

  NOTE: When a health issue is dismissed, it is cleared from the list, and its corresponding health event is no longer considered active. This means that the event is not listed if you generate a *Health history* report with the **Show current health events** filter enabled.
- To update the content displayed on the *Health issues* page, click **Refresh**.



Sort by: Event timestamp

Role stopped unexpectedly
Report Manager
17/09/2014 3:00:23 PM
TW-SC-4

Connection to unit stopped unexpectedly
Unavailable information
06/06/2014 1:01:12 PM
TW-SC-4

Connection to unit stopped unexpectedly
Unavailable information
04/06/2014 9:13:23 AM
TW-SC-4

Video signal lost
Unavailable information
14/04/2014 5:12:22 PM
TW-SC-4

Connection to unit stopped unexpectedly
Unavailable information
03/06/2014 1:34:18 PM
TW-SC-4

3 On the *Warnings* () page, do one of the following:

- To open the configuration page of an entity, click the entity.
- To open the *Diagnosis* window that provides additional details about the warning, click **Details** ().

  From the *Diagnosis* window, you can save the warning as a text file.

4 On the *Messages* () page, select a message, and do one of the following:

- To copy the selected message to the clipboard, click **Copy to clipboard** ().
- To clear a selected message, click **Clear** ().
- To clear all messages, click **Clear all**.

5 Close the *System messages* dialog box.

Related Topics

Viewing system health events on page 374
Troubleshooting: entities on page 90

Viewing system health events

You can view system health events related to selected entities within a specified time range, using the *Health history* report.

What you should know

There are three severity levels of health events:

- ❗ Error
- ⚠ Warning
- ℹ Information

Almost every entity in your system can generate health events. You can choose which health events to monitor by configuring the *Health Monitor* role.

For example, if an entity is experiencing issues, you can search for past health events that have occurred in relation to that entity. If you want to search if there were critical errors that happened in the system during the last week, you can filter you search only for errors, and set a time range.

NOTE: Health events also appear in the notification tray as system messages (6) as they occur in real time.

To view system health events related to an entity:

1. From the homepage, open the *Health history* task.
2. Set up the query filters for your report. Enable one or more of the following filters:
   - **Event timestamp:** Define the time range for the query. You can define the time range for a specific period or a relative period, such as the previous week or the previous month.
   - **Health event:** Name of the health event.
   - **Health severity:**

     Severity level of the health event:

     - ℹ Information
     - ⚠ Warning
     - ❗ Error
   - **Machine:** Select a computer that was having health issues to investigate.
   - **Observer entity:** The entity (role, server, unit, and so on) that reported the event.
   - **Show current health events:** Restrict the search to active health events. Only events that have been active for longer than the specified duration are listed in the report.

     NOTE: Dismissing an event from the *Health history* task or the *System messages* dialog box removes it from the list of active events.
   - **Source entity:** Source entity of the event.
   - **Source group:** Source entity group of the event. Usually a role or a unit.
3. Click **Generate report**.

   The health events of the selected entities are listed in the report pane.

After you finish

To dismiss active health events that have the *Error* severity level, select the event and click **Dismiss health event**. The event is removed from the report and from the *System messages* dialog box. When you regenerate the report, dismissed events are still listed, as long as the **Show current health events** filter is disabled.

Related Topics

Selecting health events to monitor on page 364
Reviewing system messages on page 371

Report pane columns for the Health history task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Health history task.

- **Health event number:** Identification number of the health error.
- **Event timestamp:** Date and time that the event occurred.
- **Severity:** Severity level of the health event:
  - ℹ Information
  - ⚠ Warning
  - ❗ Error
- **Health event:** Name of the health event.
- **Source entity:** Source entity associated to the event.
- **Occurrence count:** Number of times this health event occurred on the selected entity.
- **Entity description:** Description on the *Identity* page of the entity in Config Tool.
- **Description:** Description of the event.
- **Machine:** Computer where the health event occurred.
- **Observer entity:** The entity (role, server, unit, and so on) that reported the event.
- **IP address:** IP address of the unit or computer.

  NOTE: The IP address is not shown for units enrolled with the hostname and units that belong to an ACaaS system.
- **Physical address:** The MAC address of the equipment's network interface.

Viewing entity health status and availability

Using the *Health statistics* report, you can check the availability statistics of your system entities and monitor the health of your system.

What you should know

By monitoring the health and availability of resources such as server roles, video units, door controllers, intrusion detection panels, and so on, you can identify instabilities and prevent critical system failures.

Availability is expressed as a percentage in the report pane.

To view the health status and availability of an entity:

1 Open the *Health statistics* task.

2 Set the query filters for your report:

- **Event timestamp:** Define the time range for the query. You can define the time range for a specific period or a relative period, such as the previous week or the previous month.
- **Observer entity:** The entity (role, server, unit, and so on) that reported the event.
- **Show current health events:** Restrict the search to entities with active health events. Only entities with events that have been active for longer than the specified duration are listed in the report.
- **Source entity:** Source entity of the event.
- **Source group:** Source entity group of the event. Usually a role or a unit.

NOTE: The *Health statistics* report only returns data for entities that exist in the query time range. For example, if an entity is deleted prior to the time range set in the query, that data is ignored.

3 Click **Generate report**.

The report pane lists the health statistics for the selected entities. If health statistics could not be calculated for a given role or entity, the reason is shown in the *Calculation status* column:

- **One or more events used to calculate availability are currently disabled:** The system administrator must select which health events to monitor by configuring the Health Monitor role.
- **One or more servers from the system are offline:** The server hosting the selected role is offline, therefore the health statistics for the role cannot be calculated.

Example

A door controller called *Gym* was down four times over the last week, producing 90.72% availability. From the report results, you can see that this door controller is a potential concern, and have a maintenance crew investigate the door.

Report pane columns for the Health statistics task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Health statistics task.

- **Source entity:** Source entity associated to the alarm or the event.
- **Availability:** The percentage of time available for a given entity.
- **Uptime:** How many days, hours, and minutes the entity has been online and available.
- **Expected downtime:** How many days, hours, and minutes the entity has been offline or unavailable by user choice or *mode*. For example, deactivating a server role or disconnecting a client application causes expected downtime. Expected downtime is always omitted from the *Availability* percentage calculation.
- **Unexpected downtime:** How many days, hours, and minutes the entity has been offline or unavailable, excluding time spent in *mode*. Unexpected downtime is not caused by user choice.
- **MTBF:** Mean time between failures, in hours.

- **MTTR:** Mean time to recovery, in hours.
- **Failures:** Number of failures that have occurred.
- **RTP packet lost high:** Number of *Real-time Transport Protocol* packets lost.
- **Calculation status:** If health statistics are unavailable, the reason is shown here.
- **Last error timestamp:** Timestamp for when the entity last became unexpectedly offline or unavailable.
- **Observer entity:** The entity (role, server, unit, and so on) that reported the event.

Monitoring your computer resources

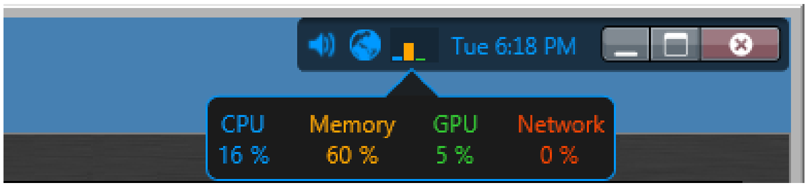
You can monitor the usage percentage of your computer resources by hovering the mouse pointer over the **Resources meter** icon in the notification tray. Click the same icon to view a summary of the hardware installed on your computer and their current use in a dialog box.

What you should know

If you do not see the **Resources meter** icon (📊) in the notification tray, set its display property to **Show**.

To monitor the resources on your computer:

1 Hover your mouse pointer over the **Resources meter** icon in the notification tray to view the current usage of your computer resources in percentages.



The usage of your computer resources is shown in four categories:

- CPU (blue)
- Memory (oange)
- GPU (green)
- Network (red)

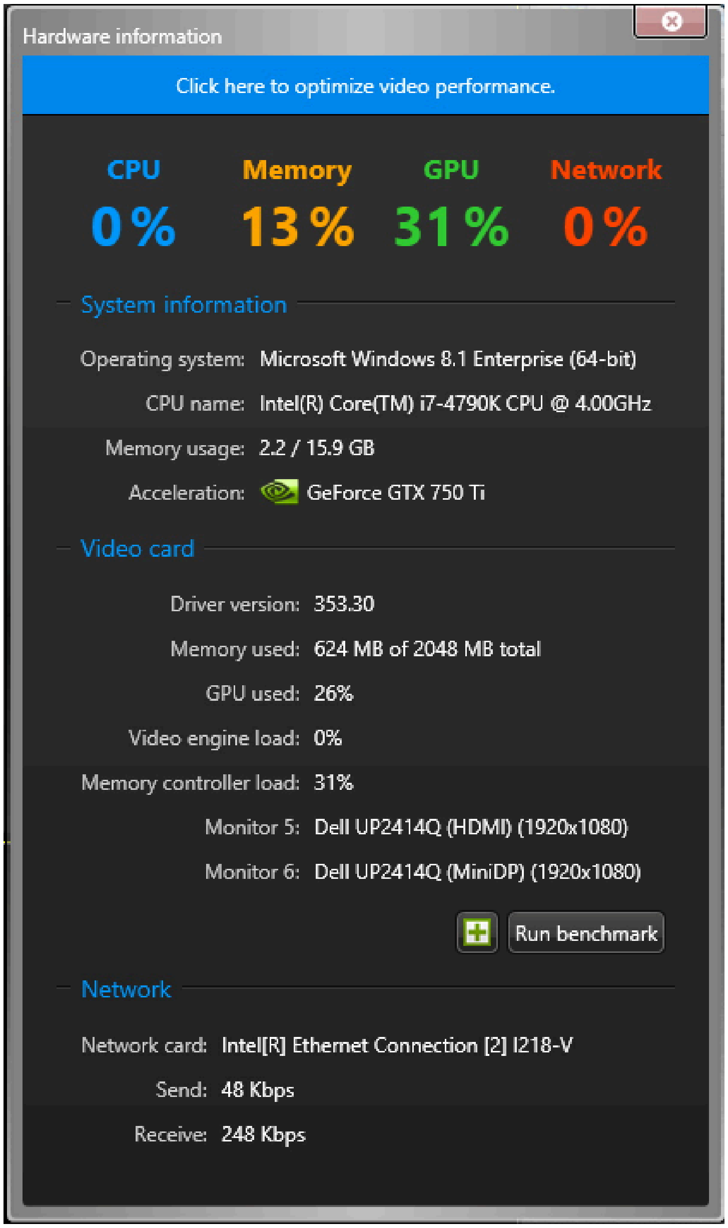
NOTE: The GPU (Graphic Processing Unit) is shown only if your video card supports hardware acceleration and if that feature is turned on in the Security Desk video options. See *Video options* in the *Security Center User Guide*.

2 Click the **Resources meter** icon in the notification tray to view detailed information about your computer resources in the Hardware information dialog box.

Hardware information dialog box

The Hardware information dialog box gives you a summary of the hardware components detected on your computer as well as their current usage percentage. You can also run the hardware benchmark tool from the Hardware information dialog box.

When performance doesn't match your expectation, use this information to find out which aspect of your system is causing the bottleneck. If your video card has reached its limits, display less video streams.



CPU 0 %
Memory 13 %
GPU 31 %
Network 0 %

System information

Operating system: Microsoft Windows 8.1 Enterprise (64-bit)
CPU name: Intel(R) Core(TM) i7-4790K CPU @ 4.00GHz
Memory usage: 2.2 / 15.9 GB
Acceleration: GeForce GTX 750 Ti

Video card

Driver version: 353.30
Memory used: 624 MB of 2048 MB total
GPU used: 26%
Video engine load: 0%
Memory controller load: 31%
Monitor 5: Dell UP2414Q (HDMI) (1920x1080)
Monitor 6: Dell UP2414Q (MiniDP) (1920x1080)

Network

Network card: Intel[R] Ethernet Connection [2] I218-V
Send: 48 Kbps
Receive: 248 Kbps

Video card information is not available if you are connected to your computer through remote desktop.

The GPU (Graphic Processing Unit) usage percentage is shown only if your video card supports hardware acceleration and if that feature is turned on in the Security Desk video options. If your computer has multiple video cards, click the **Acceleration** list to pick the one you want to monitor. For information about enabling the *Hardware acceleration* feature, see the *Security Center User Guide*.

For more information about running the hardware benchmark tool, see Using the hardware benchmark tool on page 380.

Related Topics

Optimizing video decoding performance on your computer on page 716

Using the hardware benchmark tool

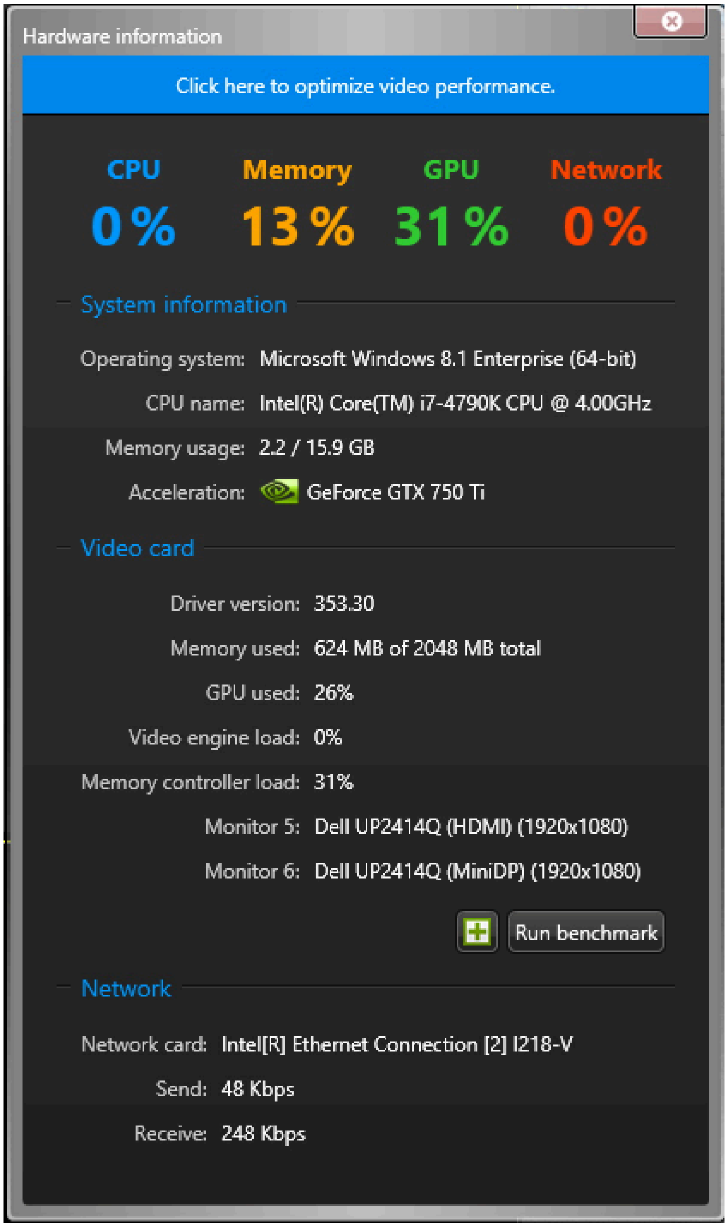
The hardware benchmark tool enables you to calibrate your settings to optimize the performance of your installed video cards. You can run the hardware benchmark tool in Config Tool or Security Desk.

What you should know

- You are prompted to run the hardware benchmark tool the first time you start Security Desk. There is also a yellow warning icon that appears on the notification tray whenever you change your video card configuration. There are no prompts in Config Tool.
- Running the benchmark tool is GPU intensive. Close all other tasks and applications when performing a benchmark test to ensure you get valid results.
- For best results, make sure your GPU drivers are up to date before running the hardware benchmark tool.

To use the hardware benchmark tool:

1 In the notification tray, click the **Resources meter** icon (📊).
The *Hardware information* dialog box opens.



Hardware information

Click here to optimize video performance.

CPU 0 %
Memory 13 %
GPU 31 %
Network 0 %

System information

Operating system: Microsoft Windows 8.1 Enterprise (64-bit)
CPU name: Intel(R) Core(TM) i7-4790K CPU @ 4.00GHz
Memory usage: 2.2 / 15.9 GB
Acceleration: GeForce GTX 750 Ti

Video card

Driver version: 353.30
Memory used: 624 MB of 2048 MB total
GPU used: 26%
Video engine load: 0%
Memory controller load: 31%
Monitor 5: Dell UP2414Q (HDMI) (1920x1080)
Monitor 6: Dell UP2414Q (MiniDP) (1920x1080)

Network

Network card: Intel[R] Ethernet Connection [2] I218-V
Send: 48 Kbps
Receive: 248 Kbps

2 From the **Acceleration** list, select the video card you want to run the benchmark test on.

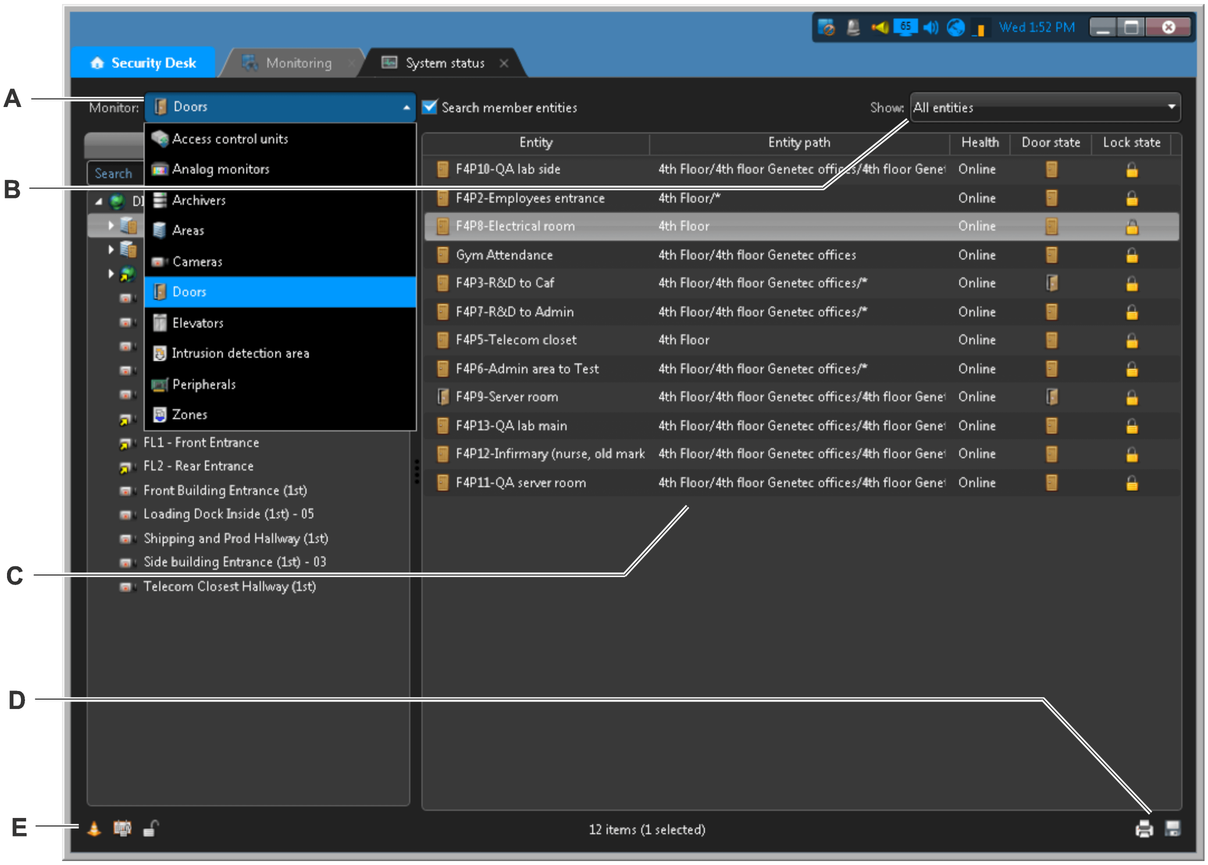
3 Click **Run benchmark**.
Once the benchmark test is complete, the **Frame rate** capability of the selected card is listed.

4 Click **Close**.

Overview of the System status task

Use the *System status* task to monitor the current status of different types of entities and investigate health issues they might have.

The following figure shows the System status task.



☑ Search member entities

Show: All entities

Entity	Entity path	Health	Door state	Lock state
F4P10-QA lab side	4th Floor/4th floor Genetec offices/4th floor Gene	Online	🚪	🔒
F4P2-Employees entrance	4th Floor/*	Online	🚪	🔒
F4P8-Electrical room	4th Floor	Online	🚪	🔒
Gym Attendance	4th Floor/4th floor Genetec offices	Online	🚪	🔒
F4P3-R&D to Caf	4th Floor/4th floor Genetec offices/*	Online	🚪	🔒
F4P7-R&D to Admin	4th Floor/4th floor Genetec offices/*	Online	🚪	🔒
F4P5-Telecom closet	4th Floor	Online	🚪	🔒
F4P6-Admin area to Test	4th Floor/4th floor Genetec offices/*	Online	🚪	🔒
F4P9-Server room	4th Floor/4th floor Genetec offices/4th floor Gene	Online	🚪	🔒
F4P13-QA lab main	4th Floor/4th floor Genetec offices/4th floor Gene	Online	🚪	🔒
F4P12-Infirmary (nurse, old mark	4th Floor/4th floor Genetec offices/4th floor Gene	Online	🚪	🔒
F4P11-QA server room	4th Floor/4th floor Genetec offices/4th floor Gene	Online	🚪	🔒

12 items (1 selected)

A	Entity types you can monitor.
B	Type of issues that you can monitor.
C	The entity statuses are listed in the report pane.
D	Click 💾 to export or 🖨 to print the report.
E	Entity-specific commands.

Related Topics

Upgrading Security Center with Global Cardholder Synchronizer roles on page 905

Monitoring the status of your Security Center system on page 389

System status task columns

In the *System status* task, you can monitor the current status of different types of entities and investigate the health issues that they might have.

The following table lists the columns that are displayed for each entity type in the **Monitor** list.

Entity	Column	Description
Access control units	Entity	Unit name
	Health	Online, Offline, or Warning
	IP address	IP address of the unit
	Sync	Synchronization status
	AC fail	Yes (✓) or No (blank)
	Battery fail	Yes (✓) or No (blank)
	Firmware	Firmware version of the unit
	Tampered	Indicates whether the unit has been tampered with Yes (✓) or No (blank)
	Maintenance	Indicates if the entity is in *maintenance mode*, and states the duration of the *maintenance mode*. The maintenance mode reason is shown as a tooltip and the font color for the entire row is set to the color associated to the reason.
	Parent	The direct parent of the interface module or downstream panels. If the direct parent is the access control unit, only the Parent unit column is filled.
	Parent unit	The parent access control unit.
Analog monitors	Entity	Analog monitor name
	Entity path	List of all parent areas, starting from the system entity. If the analog monitor has multiple parent areas, “*\” is shown as the path
	Health	Online, Offline, or Warning
	Connected entity	Name of the cameras displayed in the analog monitor
Applications	Entity	Type of application (Config Tool or Security Desk)
	Source	Computer it is running on
	Username	Name of the user who is connected
	Version	Software version of the client application
Archivers	Entity	Archiving role name

Entity	Column	Description
	Servers	List of servers assigned to this role
	Active cameras	Number of cameras detected by the Archiver
	Archiving cameras	Number of cameras that have archiving enabled (Continuous, On event, or Manual) and that are not suffering from any issue that prevents archiving
	Total number of cameras	Total number of cameras assigned to this role.
	Used space	Amount of space used by video archives.
	Archiving disk space usage	Percentage of space used over the allotted space.
	Archiver receiving rate	Rate at which the Archiver is receiving data
	Archiver writing rate	Rate at which the Archiver is writing to disk
	Maintenance	Indicates if the entity is in *maintenance mode*, and states the duration of the *maintenance mode*. The maintenance mode reason is shown as a tooltip and the font color for the entire row is set to the color associated to the reason.
	Last update	Time of the last status update
Areas	Entity	Area name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
	Threat level	Indicates if a threat level is activated on the selected area, along with the threat level name. If no threat level is set, the column is blank
	Security clearance	(Only visible to administrative users) Indicates the minimum security clearance level required from cardholders to access this area, on top of the restrictions imposed by the access rules
	People count	Working (✓) or Not working (blank)
	Antipassback	Hard, Soft, or None (no antipassback)
	Interlock	Working (✓) or Not working (blank)
	Priority	Interlock input priority: Lockdown or Override
Cameras	Entity	Camera name
	Entity path	List of all parent areas, starting from the system entity. If a camera has multiple parent areas, “*\” is shown as the path

Entity	Column	Description
	Health	Online, Offline, or Warning
	Recording	Recording state
	Analog signal	Lost, Available, or Unknown (IP cameras)
	Blocked	Indicates if the camera is blocked from some users. Blocked (✓), or not blocked (blank)
	Maintenance	Indicates if the entity is in *maintenance mode*, and states the duration of the *maintenance mode*. The maintenance mode reason is shown as a tooltip and the font color for the entire row is set to the color associated to the reason.
Doors	Entity	Door name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
	Door state	Open (🚪) or closed (🚪)
	Lock state	Locked (🔒) or unlocked (🔓)
Elevators	Entity	Elevator name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
Health issues	Entity type	Icon representing the entity type
	Entity	Entity name
	Source	For a local entity, shows the server it is running on. For a federated entity, shows the Federation™ role name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
	Maintenance	Indicates if the entity is in *maintenance mode*, and states the duration of the *maintenance mode*. The maintenance mode reason is shown as a tooltip and the font color for the entire row is set to the color associated to the reason.
Intrusion detection areas	Entity	Intrusion detection area name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
	Alarm state	Alarm active, Alarm silenced, Entry delay, or Normal

Entity	Column	Description
	Arming state	Arming, Disarmed (not ready), Disarmed (ready to arm), *Master armed*, or *Perimeter armed*
	Bypass	Active or inactive (represented by an icon)
	Trouble	Yes (✓) or No (blank)
Intrusion detection units	Entity	Intrusion detection unit name
	Health	Online, Offline, or Warning
	AC fail	Yes (✓) or No (blank)
	Battery fail	Yes (✓) or No (blank)
	Tamper	Yes (✓) or No (blank)
	Maintenance	Indicates if the entity is in *maintenance mode*, and states the duration of the *maintenance mode*. The maintenance mode reason is shown as a tooltip and the font color for the entire row is set to the color associated to the reason.
Macros	Entity	Macro name
	Start time	Time the macro was started
	Instigator	Name of the user who started the macro
Mobile applications	Entity	Mobile device name
	Source	Mobile device model
	Username	Name of the user connected through this device
	Version	Genetec™ Mobile version
	Blacklisted	Indicates whether the device is blacklisted (✓), or not (blank)
	OS	OS version installed on the device
	Current role	Name of the Mobile Server role the device is connected to
Peripherals*	Name	Peripheral name
	Type	In (Input), Out (Output), Reader
	State	Normal, Active, or Shunted (inputs and readers)
	Additional info	Settings specific to the type of peripheral
	Controlling	Entity controlled by the peripheral.
	Health	Online, Offline, or Warning

Entity	Column	Description
	Logical ID	Logical ID assigned to the peripheral
	Physical name	Peripheral name assigned by the system
Roles	Entity	Role name
	Health	Online, Offline, or Warning
	Current server	Name of the server hosting this role
	Servers	List of servers assigned to this role
	Version	Software version of role
	Status	Activated (🟢) or Deactivated (🟠)
	Maintenance	Indicates if the entity is in *maintenance mode*, and states the duration of the *maintenance mode*. The maintenance mode reason is shown as a tooltip and the font color for the entire row is set to the color associated to the reason.
Routes	Route	Route name, showing the two networks it joins
	Current configuration	Unicast TCP, Unicast UDP, or Multicast
	Detected capabilities	Unicast TCP, Unicast UDP, or Multicast **NOTE:** A *Redirector* is required on each network to be able to detect the capabilities.
	Status	OK, or warning message stating the reason of the problem **NOTE:** A *Redirector* is required on each network to be able to display the status
Servers	Entity	Server name
	Health	Online, Offline, or Warning
	Roles	Roles assigned to this server
	Certificate	Current *server certificate* and its validity period
	Maintenance	Indicates if the entity is in *maintenance mode*, and states the duration of the *maintenance mode*. The maintenance mode reason is shown as a tooltip and the font color for the entire row is set to the color associated to the reason.
	Version	Version of Security Center installed on the server.
Video modules	Server	Server hosting the video analytics module
	Entity	Type of video analytics module

Entity	Column	Description
	Total cameras	Number of video streams being processed vs. total number of cameras configured to be analyzed by this module
	CPU usage	Current CPU usage on the server
	Memory usage	Current memory usage on the server
	Analytics agent receiving rate	Current network input bandwidth on the server
	Analytics agent sending rate	Current network output bandwidth on the server
	GPU model	Nvidia graphics card detected on the server
	GPU driver	Nvidia driver version installed on the server
	GPU usage	Current GPU usage on the graphics card
	Video engine load	Percentage of dedicated video decoding chip in use in the GPU
	Video memory usage	Currnet memory usage on the graphics card
	Memory controller load	Current memory bandwidth usage on the graphics card (memory transfer between CPU and GPU)
	Last update	Last statistics update
Zones	Entity	Zone name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
	State	Normal, Active, or Trouble
	Armed	Indicates if the zone is armed or not
	Maintenance	Indicates if the entity is in *maintenance mode*, and states the duration of the *maintenance mode*. The maintenance mode reason is shown as a tooltip and the font color for the entire row is set to the color associated to the reason.

* You can also monitor the I/O status of individual units from their *Peripherals* page in Config Tool.

Monitoring the status of your Security Center system

You can monitor the current status of different types of entities and investigate health issues they might have, using the *System status* report.

What you should know

Use the *System status* report to monitor your system live. For example, if you have a camera that is not working, you can select the camera entity in the *System status* task, and then diagnose why it is offline. From the *System status* task, you can also launch the *Health history* task and generate a health report to investigate further.

When monitoring *Routes*, a *Redirector* must be configured on each network to be able to detect the network capabilities and display the current status.

To monitor the status of your system:

1. Open the *System status* task.
2. From the **Monitor** list, select one of the following:
   - Access control units
   - ALPR units
   - Analog monitors
   - Applications (only if you are an administrator)
   - Archivers
   - Areas
   - Cameras
   - Cash registers
   - Doors
   - Elevators
   - Health issues
   - Intrusion detection areas
   - Intrusion detection units
   - Macros
   - Media Gateway
   - Mobile applications
   - Mobile Server
   - Patrollers
   - Peripherals
   - Roles
   - Routes
   - Servers
   - Video modules
   - Zones
3. If required, select an area in the *Selector*.
4. To search for entities within nested areas, select the **Search member entities** option.

   The related entities, roles, applications, and items are listed in the report pane.

5 (Optional) Do one of the following, depending on the selected entity:

- To launch a *Health history* report, click 📋.
- To troubleshoot the selected entity, click ✚.
- To print the report, click 🖨.
- To change the configuration of an entity, right-click the entity in the report pane, and click **Configure entity** (⚙).
- To save the report, click 💾.

Related Topics

System status task columns on page 383

Viewing system health events on page 374

Troubleshooting: entities on page 90

Overview of the System status task on page 382

16

System audits

This section includes the following topics:

Investigating user-related activity on your Security Center system

Using the *Activity trails* report, you can view several categories of user activity: access control, ALPR, general, and video.

Before you begin

To receive results in the *Activity trails* report, you must already be monitoring user activity. You can select which activities to monitor and record in the database from the *System* task.

What you should know

You can use the *Activity trails* task to investigate various user activities such as:

- Who played back which video recordings.
- Who blocked a camera.
- Who activated a threat level.
- Who requested a credential badge to be printed.
- Who used the *Hotlist and permit editor* task.
- Who enabled hotlist filtering.

To investigate user-related activity on the system:

1. From the Config Tool or Security Desk homepage, open the *Activity trails* task.
2. In the **Activities** filter, select the user activity you want to investigate.
3. Set up the other query filters for the report. Choose from one or more of the following filters:
   - **Application:** Which application type was used for the activity.
   - **Event timestamp:** Define the time range for the query. You can define the time range for a specific period or a relative period, such as the previous week or the previous month.
   - **Impacted:** The entities that were impacted by this activity.
   - **Initiator:** User or role responsible for the activity.
4. Click **Generate report**.
   The activity results are listed in the report pane.

User activity you can investigate

To investigate user activity in Security Center using the *Activity trails* report, familiarize yourself with the activity definitions.

General user activity

You can investigate the following general user activity:

- **Alarm acknowledged:** Who acknowledged an active alarm.
- **Alarm context edited:** Who edited the context of an alarm.
- **Alarm forcibly acknowledged:** Who forcibly acknowledged an active alarm.
- **Alarm forwarded:** Who forwarded an active alarm.
- **Alarm snoozed:** Who snoozed an active alarm.
- **Alarm triggered (manually):** Who manually triggered an alarm.

- **All alarms forcibly acknowledged:** Who forcibly acknowledged all active alarms.
- **Connected to remote Security Desk:** Who connected to a remote Security Desk workstation.
- **Disconnected from remote Security Desk:** Who disconnected from a remote Security Desk workstation.
- **Email a report:** Who sent a report, based on a saved reporting task, as an email attachment.

  NOTE: The *Activity trails* report cannot indicate whether or not the recipient has received the email.
- **Email a snapshot:** Who sent a series of snapshots of a video feed as an email attachment.

  NOTE: The *Activity trails* report cannot indicate whether or not the recipient has received the email.
- **Executed record fusion search:** Who performed a search for records registered with the Record Fusion Service.
- **Health event dismissed:** Who dismissed a health event.
- **Intrusion alarm acknowledged:** Who acknowledged an intrusion alarm.
- **Intrusion alarm silenced:** Who silenced an intrusion alarm.
- **Intrusion alarm triggered:** Who manually triggered an intrusion alarm.
- **Intrusion detection area disarmed:** Who disarmed an intrusion detection area.
- **Intrusion detection area input bypass activated/deactivated:** Who activated or deactivated a sensor bypass in an intrusion detection area.
- **Intrusion detection area master armed:** Who master armed an intrusion detection area.
- **Intrusion detection area perimeter armed:** Who perimeter armed an intrusion detection area.
- **Macro started/aborted:** Who started or stopped a macro.
- **Output triggered (manually):** Who triggered an output pin (for example, using a hot action).
- **Record modified in cache:** Who modified a record in the record cache.
- **Report exported/generated/printed:** Who exported, generated, or printed a report.

  IMPORTANT: To comply with State laws, if the **Report generated** option is used for an Activity trails report that contains ALPR data, the reason for the ALPR search is included in the **Description** field.
- **Send an email:** Who sent an email to users, cardholders, or specified email addresses.

  NOTE: The *Activity trails* report cannot indicate whether or not the recipient has received the email.
- **Threat level set/cleared:** Who set or cleared a threat level, and on which area or system.
- **Unit certificate changed:** Who changed the unit certificate.
- **Unit password changed:** Who changed the unit password and whether the password was manually entered or system generated.
- **Unit password history consulted:** Who viewed the password history of a unit.
- **Unit password recovered:** Who recovered the password of a unit.
- **Unit passwords exported:** Who exported the *Hardware inventory* report with unit passwords.
- **User logged on/off:** Who logged on or off of which Security Center client application.
- **User logon failed:** Who failed to log on to a Security Center client application, and why.

User activity related to access control

You can investigate the following user activity related to access control:

- **Access control unit rebooted (manually):** Who manually rebooted an access control unit.
- **Access control unit support logs enabled/disabled:** Who enabled or disabled support logs for an access control unit.
- **Access control unit synchronization started (manually):** Who manually started an access control unit synchronization.
- **Antipassback violation forgiven:** Who forgave an antipassback violation.
- **Badge printed:** Who printed a credential badge.
- **Card encoded with a DESFire configuration:** Who encoded a card with a MIFARE DESFire configuration from the *MIFARE DESFire configuration* task.
- **Card encoding tested with a DESFire configuration:** Who tested a card encoded with a MIFARE DESFire configuration from the *MIFARE DESFire configuration* task.

- **Credential request canceled/completed:** Who completed or canceled a credential badge print request.
- **Credential requested:** Who requested a credential badge to be printed, and why.
- **Device shunted:** Who shunted (disabled) an access control device.
- **Door maintenance mode canceled:** Who canceled the maintenance mode on a door.
- **Door set in maintenance mode:** Who unlocked a door by setting it in maintenance mode.
- **Door unlock schedule overridden (lock/unlock):** Who overrode the lock or unlock schedule of a door.
- **Door unlock schedule override canceled:** Who canceled the unlock schedule override of a door.
- **Door unlocked (explicitly):** Who unlocked a door from Security Desk using a hot action or alarm event-to-action.
- **Door unlocked (manually):** Who manually unlocked a door from the Security Desk *Door* widget.
- **Elevator floor access schedule override canceled:** Who canceled an elevator schedule override.
- **Elevator floor access schedule overridden (free access):** Who overrode a free access elevator schedule.
- **Elevator floor access schedule overridden (restricted access):** Who overrode a controlled access elevator schedule.
- **Exported DESFire configuration to file:** Who exported MIFARE DESFire configurations to a file from the *MIFARE DESFire configuration* task.
- **Exported DESFire configuration to unit:** Who exported MIFARE DESFire configurations to an access control unit from the *MIFARE DESFire configuration* task.
- **Exported DESFire cryptographic keys to unit:** Who exported MIFARE DESFire cryptographic keys to an access control unit from the *MIFARE DESFire configuration* task.
- **Firmware upgrade for access control unit scheduled with interface module upgrade:** Who scheduled a firmware upgrade for an access control unit and its associated interface modules.
- **Firmware upgrade for access control unit scheduled without interface module upgrade:** Who scheduled a firmware upgrade for an access control unit.
- **Firmware upgrade for interface module scheduled:** Who scheduled a firmware upgrade for an interface module.
- **Imported DESFire configurations:** Who imported MIFARE DESFire configurations from the *MIFARE DESFire configuration* task.
- **Minimum security clearance modified:** Who changed the minimum security clearance for an entity, and what the minimum security clearance was set to.
- **People count reset:** Who reset the people count of an area to zero.
- **Person added to area:** Who added a cardholder to an area, using the SDK.
- **Person removed from area:** Who removed a cardholder from an area in the *People counting* task.
- **Scheduled firmware upgrade for access control unit canceled:** The unit's scheduled upgrade was canceled.
- **Set reader mode:** Who changed the reader mode for accessing doors between *Card and PIN* and *Card or PIN*.
- **Trusted certificate reset:** Who reset the trusted certificate of a Synergis™ Cloud Link unit.
- **Unlock area perimeter doors:** Who unlocked an area perimeter door.
- **Zone armed/disarmed:** Who armed or disarmed a zone.

User activity related to ALPR

You can investigate the following user activity related to ALPR:

- **Application updated:** Who updated a Genetec Patroller™ or a Sharp unit.
- **Enforce in-lot violation triggered:** Who enforced an in-lot violation in a parking zone.
- **Hit deleted:** Who deleted a hit.
- **Hotlist or permit list edited:** Who loaded a hotlist or permit list, or added, modified, or deleted license plates in the list.
- **Past read matching triggered:** Who performed past read matching in Patroller.
- **Photo evidence report printed (Hits/Reads):** Who printed a hits/reads evidence report.
- **Plate filtering enabled:** Which ALPR Manager role has plate filtering enabled.

- **Read edited/triggered:** Who edited/triggered a license plate read.
- **Read/hit protected:** Who protected a license plate read or hit.
- **Read/hit unprotected:** Who unprotected a license plate read or hit.
- **Reset parking zone inventory:** Who reset the inventory of a parking zone.
- **Set parking zone occupancy:** Who modified the occupancy of a parking zone.

User activity related to video

You can investigate the following user activity related to video:

- **Archive backup started/stopped (manually):** Who manually started or stopped video from being backed up from an Archiver.
- **Archiver consolidation started/stopped (manually):** Who started or stopped video from being consolidated from a secondary Archiver to the primary Archiver.
- **Archive duplication started/stopped (manually):** Who started or stopped video from being duplicated from one Archiver to another.
- **Archive restore started/stopped (manually):** Who started or stopped video archive from being restored to an Archiver.
- **Archive retrieval from units started/stopped (manually):** Who started or stopped transferring video from video units to an Archiver.
- **Bandwidth limit exceeded:** Who requested a video stream that was unable to connect because the bandwidth limit for redirected video was reached. Or, who lost a redirected video stream connection because the bandwidth limit was reached and a user with a higher user level requested a stream.
- **Bookmark deleted/modified:** Who deleted or modified a bookmark.
- **Camera blocked/unblocked:** Who blocked or unblocked a camera.
- **Confidential video requested:** Who requested to view a confidential video stream.
- **Connected to analog monitor:** Who connected to an analog monitor.
- **Disconnected from analog monitor:** Who disconnected from an analog monitor.
- **Key stream removed:** Who removed a key stream.
- **Live/Playback streaming requested from Federation™:** Which Federation™ host requested streaming and from which camera.

  NOTE: The name given to the Federation™ user should be descriptive of the Federation™ host. For example, instead of using *federation_1*, use *PoliceDepartment* or *CompanyHeadquarters*.
- **Live streaming started/stopped:** Which camera was displayed or removed.
- **Playback streaming:** Which recording was played.
- **PTZ activated:** Who moved an idle PTZ.
- **PTZ command sent:** Which PTZ command the user sent.
- **PTZ locked:** Who locked PTZ on which camera.
- **PTZ zoom started/stopped:** Who started or stopped PTZ zoom on which camera.
- **Recording started/stopped (manually):** Who started or stopped recording video manually.
- **Sequence paused/resumed:** Who paused or resumed a video sequence.
- **Snapshot printed/saved:** Who printed or saved a snapshot.
- **Video exported:** What did the user export and where did they save it.

  NOTE: If the user lacks the *Single user export* privilege, both usernames are reported. In a federated system, only the federated username is reported.
- **Video file deleted (manually):** Who deleted a video file from the system.
- **Video file protected/unprotected:** Who started or stopped protection on a video file.
- **Video stream not delivered:** Who's video request was terminated without having a single frame being rendered.
- **Video unit identified/rebooted/reconnected:** Who identified/rebooted/reconnected a video unit.
- **Visual tracking enabled/disabled:** Who enabled or disabled *visual tracking* in a tile.

Report pane columns for the Activity trails task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Activity trails task.

- **Initiator:** Who or what performed the activity or caused the activity event.
- **Initiator type:** The type of entity that initiated the activity.
- **Activity name:** Type of activity.
- **Description:** Description of the event, activity, entity, or incident.

  IMPORTANT: To comply with State laws, if the **Report generated** option is used for an Activity trails report that contains ALPR data, the reason for the ALPR search is included in the **Description** field.
- **Impacted entity:** Which entities were impacted by this activity.
- **Impacted entity type:** The type of entity impacted by this activity.
- **Initiator machine:** Which computer the activity was performed on.
- **Initiator application:** The application used for this activity.
- **Event timestamp:** Date and time that the event occurred.
- **Impacted entity version:** The version number of the entity impacted by this activity. This field is empty if the impacted entity is not a role.
- **Initiator application version:** The version number of the application. This field is empty if the activity is initiated by a role entity.
- **Initiator version:** The version number of the initiator. This field is empty if the activity is initiated by a user.
- **Original initiator:** (Used for remote logging on federated systems) Who or what role performed the activity on the Federation™ host. In this case, the *Initiator* corresponds to the Federation™ user.

Configuring event logging for video sequences

For systems that have many video sequences configured, the *Activity trails* report can be extremely large due to the number of camera connections and disconnections. You can reduce the size of the report by configuring the system to only log the connections and disconnections of camera sequences.

What you should know

- By default, logging is enabled for all connections and disconnections by all cameras and camera sequences. If the *Activity trails* report size is manageable using this default, then it is not necessary to modify this configuration.
- If you disable *Activity trail* on sequences, the camera connection changes inside a sequence are not logged; only the camera sequence connections and disconnections are logged.
- This configuration change applies only to the workstation on which the file is modified.

To configure event logging for video sequences:

1 In a text editor, open the file *GeneralSettings.gconfig* found in the *ConfigurationFiles* folder under the Security Center installation folder (*C:\Program Files (x86)\Genetec Security Center 5.11*).

2 Find the `<mediaPlayer>` node and modify it to `<mediaPlayer IsActivityTrailEnabledOnSequence="false">` or `<mediaPlayer IsActivityTrailEnabledOnSequence="true">`, as required.

3 Save your changes and close the file.

The new configuration takes effect immediately.

4 Repeat the procedure for other workstations, as required.

Finding out what changes were made to the system configuration

You can find out what configuration changes were made on the system, who made them, when, and on which entity settings (before and after values), using the *Audit trails* report.

What you should know

The Audit trails report is helpful if you see that the properties of an entity have changed and you must find out who made those changes and when (for example, if the recording mode of a camera has been modified). Also, if you requested an update for an entity (for example, the privileges for a user), you can check to see if the changes have been made from Config Tool.

To find out what changes are made to the system configuration:

1 From the homepage, open the *Audit trails* task.

2 Set up the query filters for the report. Choose from one or more of the following filters:

- **Application:** Which application type was used for the activity.
- **Entities:** Select the entities you want to investigate. You can filter the entities by name and by type.
- **Modification time:** Entities modified within the specified time range.
- **Modified by:** User or role responsible for the entity modification.

3 Click **Generate report**.

The description of the changes (before and after values) to the selected entities, as well as who made those modifications and when, are listed in the report pane.

Report pane columns for the Audit trails task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Audit trails task.

- **Entity:** Name of the entity affected by the modification.
- **Entity type:** Type of entity affected by the modification.
- **Description:** The description of the entity modification.
- **Initiator:** Who or what role made entity modification.
- **Initiator type:** The type of entity initiating the entity modifications.
- **Initiator machine:** The computer used to make the change.
- **Initiator application:** The application used to make the change.
- **Initiator application version:** The version number of the application. This field is empty if the activity is initiated by a role entity.
- **Modification time:** Time the entity was last modified.

Configuration changes logged by the Security Center system

All configuration changes are logged by the system. You can investigate those changes with the *Audit trails* report.

The following table outlines the change descriptions you can expect from the *Audit trails* report.

Modification type	Description
Entity creations	Entity created: <*Entity name at creation*>.
Entity deletions	Entity deleted: <*Entity name at deletion*>.
Membership modifications	• <*Entity*> is now a member of <*Group entity*>. • <*Entity*> is no longer a member of <*Group entity*>. **NOTE:** <Group entity> can be an area, a partition, a cardholder group, or a user group.
Access rights modifications	• <*User or User group*> gained access rights to <*Partition*>. • <*User or User group*> lost access rights to <*Partition*>.
Privilege modifications	Value of <*Privilege*> changed from <*Old value*> to <*New value*>.
Property modifications	Value of <*Property*> changed from <*Old value*> to <*New value*>. **NOTE:** Not all property modifications are described with before and after values.
Role activations/deactivations	Value of Active state changed from <*Old value*> to <*New value*>.
Map modifications	• <*Entity*> has been added as a link to map <*Map entity*>. • <*Entity*> has been removed as a link from map <*Map entity*>. • <*Entity*> setting modified. • <*Camera entity*> setting modified to Motion on/off. • <*Camera entity*> setting modified to Recording on/off. • <*Zone entity*> state settings modified. • Map layers added/removed (<*layer(s)*>) • Georeference modified. • Default view modified. • Background modified.

17

Mobile access

This section includes the following topics:

About Genetec Mobile

You can perform many of the Security Desk monitoring and investigation functions from your smartphone using Genetec™ Mobile.

To use the Genetec Mobile features, you need to:

- Configure the Mobile Server role.
- Install Genetec Mobile on your smartphones (Android and iOS).
- Configure your networks (Wi-Fi, VPN, and so on) so that the mobile devices can connect to the Mobile Server role.

The following sections describe the features that are available through Genetec Mobile.

Genetec Mobile features

A mobile user is a Security Center user. Thus, what the user can do on the Genetec Mobile app is defined by user privileges and access rights, the same way it does on Security Desk.

- Secure connection to Security Center system
- Area view (similar to the *Monitoring* task in Security Desk)
  - View Security Center entities as a list or as tiles (cameras are shown as thumbnails)
  - Add or remove entities from favorites
  - Show or hide inactive entities
  - View cameras
    - View cameras in landscape or portrait mode
    - View cameras in a layout mode or in full screen mode
    - Live video control (PTZ, presets, add bookmark, digital zoom, and more)
    - Playback video control (timeline, bookmark markers, go to specific time, and more)
    - View live and playback video simultaneously (picture in picture)
  - View camera sequences (all cameras are displayed simultaneously)
  - View doors (lock and unlock door, set maintenance mode, override unlock schedule)
  - View live ALPR events (reads and hits) on ALPR units
  - View display layouts (only cameras and doors are supported)
- Maps (similar to the *Maps* task in Security Desk)
  - Display on the device-native map, entities represented as map objects on the user or system default map
  - Only supports GIS maps (not maps imported from image files)
  - Only show cameras, camera sequences, doors, fixed ALPR cameras, patrol vehicles, and other mobile users on the map
- Alarms (monitor and acknowledge alarms as in Security Desk)
- Threat levels (view and set threat levels as in Security Desk)
- Video events (query and filter bookmarks and camera events as in Security Desk)
- Two-way messaging with Security Desk users and other mobile users
- Stream video from the device camera

- Customizable options:
    - Language (**English** or **French**)
    - Distance unit (**Imperial** or **Metric**)
    - Default startup page (**Maps**, **Area view**, **Alarms**, **Threat levels**, **Video events**)
    - Auto logon (**ON** or **OFF**)
    - Video over cellular (**ON** or **OFF**)
    - Advanced settings
        - Enforce security validity (**ON** or **OFF**)
        - Prevent redirection (**ON** or **OFF**)
        - Enable debugging (**ON** or **OFF**)
        - Show diagnostics (for Support)
    - Share location (**ON** or **OFF**)
    - Notifications (**ON** or **OFF**)

Mobile features in Security Desk

- Track mobile users on maps
- Two-way messaging with mobile users (from the map or through hot actions)
- Share cameras with mobile users (from the map or through hot actions)

Mobile features in Config Tool

- Configure Security Center users for Genetec Mobile (requires the *Mobile application* privilege)
- Configure Security Desk users to track mobile users (requires the *View mobile users* privilege)
- Mobile Server configuration (using the *System* task)
    - Configure common Genetec Mobile behavior, such as session timeout
    - Configure role failover and load balancing
    - Enable or disable Security Center Mobile features
    - Enable new Security Center Mobile features introduced after your current Security Center release
- View all mobile devices that ever connected to your system (using the *System status* task)
    - View mobile device configuration (OS version, app version, current user, and so on)
    - Blacklist a mobile device (prevent future connections from that device and log off current user)
    - Kick out a mobile user (forced log off)

Related Topics

Configuring the Map Manager role on page 288

About the Mobile Server role

The Mobile Server role provides Security Center access on mobile devices.

If your license supports mobile devices (**Number of mobile devices** > 0), the Mobile Server and Media Gateway roles are created by default after you install Security Center on the main server.

You can create multiple Mobile Server roles on your system. The Genetec™ Mobile app connects to the Mobile Server using a unique URL.

The format of the URL is *host:port/web address*, where *host* is the IP address or hostname of the server hosting the Mobile Server role, *port* is HTTPS port 443 by default, and *web address* is Mobile by default.

Mobile Server setup scenarios

You can configure the following setup scenarios for the Mobile Server:

- **Single role on a single server:** This is the default setup, ready to be deployed immediately after installation.
- **Single role on multiple servers:** Use this setup to support role failover and load balancing. Load balancing for Mobile Server is based on the number of client connections and media sessions handled by each server.
- **Multiple roles on multiple servers:** Use this scenario if you want to implement network segmentation. For security purposes, you might create one mobile access point on your intranet and another on the Internet. If your mobile users are scattered around the world, you might create one Mobile Server role for each relevant country or continent to boost your system performance. You can assign each role to one or multiple servers.

Related Topics

About the Media Gateway role on page 605

Role failover on page 160

Configuring Mobile Server roles

You only need to change the Mobile Server configuration if the default settings are not ideal, or if you created multiple Mobile Server roles in your system.

To configure a Mobile Server role:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Click the Mobile Server that you want to change.

3 (Optional) From the *Identity* page:

- Change the name of the role as it appears in Config Tool.
- Assign the role to a different partition to restrict its use to certain user groups.

4 Click the **Properties** tab.

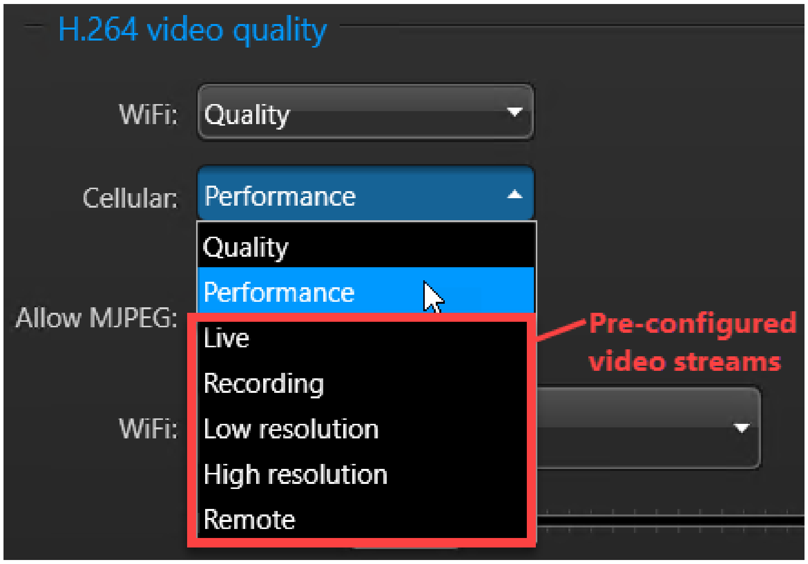
5 In the *General settings* section, configure the Mobile Server properties and the characteristics shared by all mobile applications connected to this role.

- **Web address:** Define the suffix of the URL used by Genetec Mobile to connect to the Mobile Server. The format of the URL is *host:port/web address*, where *host* is the IP address or hostname of the server hosting the Mobile Server role, *port* is HTTPS port 443 by default, and *web address* is Mobile by default. Each Mobile Server role must have a unique URL. If two roles are hosted on the same server, they must have different web addresses or use different ports.
- **Use the default secure HTTP port of the server:** By default, the Mobile Server communicates with the mobile devices over HTTPS port 443. If your IT policy requires a different port, or there is some sort of conflict, you can change this port. Turn off this option and then change the port number.
- **Maximum inbox messages per user:** Define the maximum number of messages that Genetec Mobile keeps in its inbox. If a new message is received while the inbox is full, the oldest message is deleted.
- **Session timeout:** Define the maximum period of inactivity, meaning the app is in the background, before the Mobile Server automatically logs the user off.
- **Maximum number of client sessions:** Set a limit to the number of Genetec Mobile connections that this role can handle to avoid overloading the server. The default is no limit.

6 In the *Features* section, select the features you want to enable in Genetec™ Mobile on devices connected to this role.

- **Alarms:** Allow Genetec Mobile users to monitor and acknowledge alarms.
- **Device camera streaming:** Allow Genetec Mobile to enroll mobile device cameras in Security Center. Click ⚙ to configure the settings.
  - **Maximum sequence length:** Maximum duration of the streamed video. After the duration elapses, the streaming automatically stops to prevent battery drain.
  - **Port start and end index:** Port range used for mobile device cameras.
  - **Archiver:** Archiver role responsible to manage the device cameras.
  - **Location:** Area entity where the device cameras are grouped under.
- **License plate management:** (Genetec Mobile 5.1.0 and later) Allow mobile users to view live ALPR events (reads and hits), to add license plates to hotlists, and to generate reports on reads and hits.
- **Maps:** Allow Genetec Mobile to display Security Center entities and live events on maps.
- **Push notifications:** Allow Genetec Mobile to receive push notifications from the Mobile Server.
- **Threat levels:** Allow the Genetec Mobile user to display and set threat levels.
- **Tracking:** Allow Genetec Mobile to share its device location with other users on the system so that its user can be displayed on georeferenced maps, in Security Desk, and other instances of Genetec Mobile.
- **Video:** Allow Genetec Mobile to display video from Security Center. Click ⚙ to configure the settings.

- **Maximum number of video streams:** Set a limit to the number of video streams that this role can handle to avoid overloading the server. The default is no limit.
- **Limit Media Gateway role usage:** Turn on this option to assign Media Gateway roles to this Mobile Server and limit the use of the Media Gateway roles to the selected servers to accommodate your network limitations. Only the servers assigned to the selected Media Gateway roles are listed.
- **H.264 video quality:** For cameras that support H.264 streams, choose the video stream to use when the Genetec mobile app connects over Wi-Fi and cellular networks. You can choose:
  - A preconfigured stream usage: **Live**, **Recording**, **Low resolution**, **High resolution**, or **Remote**. For more info, see Configuring video streams of cameras on page 616.
  - **Quality** so that the system uses the preconfigured stream usage that has the highest resolution and frame rate.
  - **Performance** so that the system uses the preconfigured stream usage that requires the least amount of bandwidth.



- **Allow MJPEG:** Enable or disable MJPEG streams. When enabled, if the camera requested by Genetec Mobile does not support H.264, then video is sent in MJPEG format.

  Choose the maximum resolution and frame rate to use when sending MJPEG video over Wi-Fi and cellular networks. The mobile user can override these settings in Genetec Mobile.
  When a mobile user requests to view a camera, the Mobile Server gets all the streams configured for that camera and selects the one closest to the maximum settings. If a stream is found with a resolution close to that, the Media Gateway sends that stream to the Mobile Server which then sends it to the mobile device. If no stream is found close to the resolution, the Media Gateway must transcode the stream to get the desired resolution.
  IMPORTANT: The transcoding process is very CPU intensive and should be avoided. For every camera susceptible to be viewed by mobile users, always ensure that you have one stream configured that is close to the maximum settings configured in the Mobile Server. Alternatively, you can turn off the **MJPEG** option to avoid any possibility of transcoding.

7 (Optional) Enable Security Center Mobile features that were added after your current Security Center release.

   You can enable new features on Genetec Mobile without having to upgrade your Security Center system by clicking ➕. For more information, contact one of our sales representatives.

8 If you have multiple Mobile Server roles, move this role to its own expansion server.

9 (Optional) Add failover and load balancing to this Mobile Server role.

After you finish

Test the connection of Genetec Mobile to Security Center. To connect to a Mobile Server, you must specify the URL corresponding to the Mobile Server role. You can omit the port and the web address if they match the default values.

Related Topics

About the Mobile Server role on page 403

Showing mobile users on maps

To show mobile users on maps, you must enable tracking on the Mobile Server roles and location sharing on Genetec™ Mobile devices, and grant the *View mobile users* privilege to Security Desk users.

What you should know

Mobile users are only displayed on georeferenced maps.

NOTE: A mobile user might not show up correctly on a map that is georeferenced manually, such as a floor plan, because manual processes have a certain level of inaccuracy.

To show mobile users on maps:

1. From the Config Tool homepage, open the *System* task and click the **Roles** view.
2. Enable the tracking feature on your Mobile Server roles.
   a) Select the appropriate Mobile Server role and click the **Properties** tab.
   b) Select the **Tracking** option and click **Apply**.
3. Grant the *View mobile users* privilege to Security Desk users.
   a) Open the *User management* task.
   b) Select the appropriate user or user group, and click the **Privileges** tab.
   c) In the **Search** field, enter `Mobile` and click **Search** (🔍).
   d) On the *View mobile users* row, click **Allow**, and then click **Apply**.
4. Enable location sharing on Genetec Mobile devices.
   a) Open the Settings app on your phone.
   b) Ensure that the **Location** service is enabled on your phone.
   c) Open the Security Center Mobile app.
   d) Go to the *Settings* page.
   e) Under *Features*, enable **Share location**.

18

Web access

This section includes the following topics:

About Genetec Web App

The Genetec™ Web App is a unified, portable, and map-centric way to monitor your entities and to generate reports from a web browser.

The Genetec Web App features the following:

- Intuitive user interface.
- *Maps* task to monitor entities, interact with their associated video and events, and command functions on a map.
- *Tiles* task to view live and playback video, and perform other video management and Access control tasks.
- *Reports* task to search for door activities.
  - *Alarms* report to search for alarms generated on your system.
  - *Bookmarks* report to search for bookmarked video.
  - *Camera events* report to search for camera-related events generated on your system.
  - *Door activity* report to search for access control events, such as access denied events and door status.
  - *Incidents* report to search and review incident-related activities.
  - *Anything* report to search multiple report categories simultaneously.
- *Watch list* to monitor events from specific entities.
- *Threat levels* lets you respond to dangerous situations, such as a fire or a shooting, while you are monitoring your system. You can respond by changing the state of the entire Security Center system or specific areas.

About Security Center Web Client

If you do not have access to the Security Desk application, you can use the Security Center Web Client to configure and monitor various entities of your Security Center system, and to generate reports from a web browser.

The Web Client features the following:

- Intuitive Web Client user interface.
- *Monitoring* task to view live and playback video, and perform other video surveillance tasks.
- *Bookmarks* task to search for bookmarked video.
- *Door activity* task to search for door activities.
- *Alarm report* task to search for alarms generated on your system.
- *Alarm list* to view, investigate, forward, and acknowledge current alarms from any page in Web Client.
- *Plate report* task to search for license plate reads and hits generated on your system.
- *Access configuration* task for access control activities, such as creating cardholders, checking visitors in and out, managing cardholder groups, and searching for credentials.
- *Threat levels* lets you respond to dangerous situations, such as a fire or a shooting, while you are monitoring your system. You can respond by changing the state of the entire Security Center system or specific areas.

NOTE: Web Client only supports custom fields for local cardholders and visitors. Other custom fields are not displayed.

About the Web Server role

The Web Server role is used to configure the Genetec™ Web App and the Web Client, two web applications that give users remote access to Security Center. Each role created defines a unique web address (URL) that users enter in their web browser to log on to the Genetec™ Web App or Web Client and access information from Security Center.

Multiple instances of the Web Server role are permitted. You might create one role for local users and a different role for remote users, who access the Security Center network over the Internet.

Configuration requirements

- It is recommended to deploy Web Server roles on separate expansion servers.
- Each Web Server role must have a unique URL. The URL format is *https://computer host name or IP address:port/webAddress*.
- If multiple roles are created on the same server, they must each use a different HTTPS port or web address. Otherwise, the role entity turns yellow and an *Entity warning* event is generated.
- To view video in the Genetec™ Web App or Web Client, Media Gateway must be running on the server that hosts the Web Server role.
- If you deploy multiple instances of the Genetec Web App or Web Client on the same server, make sure the URL of each is unique. Otherwise, the Web Server role turns yellow and an *Entity warning* event is generated.
- If end-users will monitor video in the Web Client using Mozilla Firefox or Microsoft Edge browsers, make sure that **one** of the following conditions is met:
  - A valid SSL certificate is installed on the server hosting the Web Server role.

    NOTE: If a third-party certificate was already installed on the server through Windows, you can apply the certificate to Security Center from Server Admin:

    1. In the *Secure communication* section, select your server from the list.
    2. Click **Select certificate**.
    3. Select the certificate you want, and then click **Select** > **Save**.
  - If using the default self-signed SSL certificate, make sure that the REST ports on the Media Gateway role and the Web Server port settings match.

    The defaults are port 80 for HTTP and port 443 for HTTPS.

Related Topics

About the Media Gateway role on page 605

Role failover on page 160

Creating Web Server roles

Create a Web Server role to host the Genetec™ Web App or Web Client and to define the web address (URL) that users enter in their web browser to access theGenetec Web App or Web Client.

Before you begin

- Read About the Web Server role on page 411.
- Ensure that you have a Media Gateway role in your system. If none exists, a Media Gateway role is created by default when you create the first Web Server role.

What you should know

- If there is only one Web Server role in your system, you can create the role using the default settings. However, if you have a complex system involving multiple private networks, you might choose to deploy multiple Web Server roles, in which case, you might need to change the default settings of each role.
- When the Web Server role is created, it is deployed to the main server. If you have multiple Web Server roles, move each role to an expansion server so that traffic loads are well distributed.
- It is possible to simultaneously run the Genetec Web App and the Web Client on separate Web Server roles.

To create a Web Server role:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Click **Add an entity** (✚), and then click **Web Server** (🌐).

3 (Optional) In Web Client, you can turn on the **Unlimited session time** option so users remain logged in on the Web Client as long as their browser window stays open. Otherwise, users are automatically signed out of the Web Client after 12 hours of inactivity.

4 On the *Basic information* page, enter a name and description for the role.

5 If there is a **Partition** field, select the partition this role is a member of.

Partitions determine which Security Center users have access to this entity. Only users who have been granted access to the partition can see this role.

6 Click **Next** > **Create** > **Close**.

The Web Server role (🌐) is created.

7 In the Web Server page, click **Properties** tab.

8 If you have multiple Web Server roles, verify that the default URL under **Communications settings** does not match the URL of other Web Server roles in your system. If it does, change the **Web address** or the port settings so that the URL of the Genetec Web App or Web Client is unique.

The default URL of the Genetec Web App is *https://host:443/WebApp*.The default URL of the Web Client is *https://host:433/SecurityCenter*, where host is the IP address or computer host name of the server that hosts the Web Server.

9 Click **Apply**.

After you finish

- If this is one of many Web Server roles, move this role to its own server.
- To view video using the Web Client, ensure that the Media Gateway role is running on the server that hosts the new Web Server role. If required, you can add the server to the existing Media Gateway role.
- To configure failover for this role, add a standby server.
- If the default port settings conflict with other applications on your system, you can change the ports used by the Web Server role and the Media Gateway roles. In the Web Server role, on the *Properties* page, turn off the **Use the default web ports of the server** option, then change the HTTP and HTTPS ports. The

default settings are HTTP port 80 and HTTPS port 443. Click **Apply** to save your changes. Then make the same changes to the REST port settings in the Media Gateway role.

Configuring Web Server roles

After you have created a Web Server role, you can configure user session time, usage statistics, the URL, port settings, and the SSL certificate for the Genetec™ Web App or Web Client.

Before you begin

Read About the Web Server role on page 411.

What you should know

By default, a Genetec Web App Web Server role is deployed to the main Security Center server. If you have multiple Web Server roles, assign each role to a different expansion server.

To modify a Web Server role:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Click the **Web Server** role that you want to change.

3 (Optional) From the *Identity* page:

- Change the name of the role as it appears in Config Tool.
- Assign the role to a different partition to restrict its use to certain user groups.

4 Click the **Properties** tab.

5 (Optional) In Web Client, you can turn on the **Unlimited session time** option so users remain logged in on the Web Client as long as their browser window stays open. Otherwise, users are automatically signed out of the Web Client after 12 hours of inactivity.

6 To change the URL used to access the Genetec Web App or Web Client, change the **Web address**.

To see the URL, look under the *Communication settings*.

7 (Optional) If necessary, for example, if you do not want to clutter your C: drive, change the **Vault location**.

In Web Client, when you download video, the files are packaged and temporarily stored in the Web Client vault. These temporary files are deleted when the download is complete. The default location is *ProgramData\Genetec Security Center\WebClientExports*.

NOTE: This only applies to the Web Client role.

8 If the default port settings conflict with other roles or applications on your system, turn off the **Use the default web ports of the server** option and change the ports.

By default, the HTTP port is 80 and the Secure HTTP port is 443.

9 If your Genetec Web App or Web Client has specific streaming requirements, create a Media Gateway role with these requirements and select it in the **Media Gateway** drop-down list.

10 Click **Apply**.

11 Verify that the URL opens the Web Server, by clicking the URL under *Communication settings* on the *Properties* page.

If you are using the default self-signed certificate and it is not installed on your computer, your browser displays an error message. Proceed to the logon page by doing the following:

- In Google Chrome, click **Show Advanced** and then click **Proceed to *ComputerName* (unsafe)**.
- In Internet Explorer, click **Continue to this website (not recommended)**.

The Genetec Web App or Web Client log on page appears.

12 If you have multiple Web Server roles, move this role to its own expansion server.

13 (Optional) Click the **Resources** tab and add standby servers for failover and load balancing.

When multiple servers are assigned to the Web Server role, Security Center automatically uses the server with the least number of connections for new connection requests.

Part III

System security

This part includes the following chapters:

19

Introduction to system security

This section includes the following topics:

Defining who can access Security Center

When configuring who can access Security Center, you should first define the security partitions (responsibility boundaries), and then select the user groups and individual users who can access these partitions.

What you should know

While Security Center protects your company's assets (buildings, equipment, important data collected in the fields, and so on), your job as administrator is to protect the Security Center software against illegal access.

When securing access to your software, you should ask the three following questions:

- Who needs to use the system? – Which *users* and *user groups* can log on?
- What do they use it for? – What *privileges* must they have?
- Which parts of the system are they responsible for? – Which *partitions* must they have access to?

BEST PRACTICE: It is easier to define security partitions when you first set up your system. That way, as you create entities in your system, you can place them directly into the partitions where they belong. If you start by creating users first, you might end up having to revisit their access rights every time you add a new partition to your system.

To define who can access Security Center:

1. Decide whether partitions are helpful in your situation.
2. If partitions are helpful, identify the parts of your system that are relatively independent of each other, and create a partition for each part.

   Example: If your system covers multiple sites, and if the security staff at each site work independently of the security staff at other sites, then create a partition for each site.
3. Identify the groups of users who share the same roles and responsibilities, create a user group for each.

   Example: All security operators can form one group, and all investigators can form another group.
4. If you have groups of personnel working on different partitions, define a user group for each of them, add them as members of the larger user group, and give them access to their respective partitions.

   Each individual subgroup would be allowed to access a different partition. With this organization, the purpose of the parent user groups is to separate users according to their roles and responsibilities (operators, investigators, supervisors, and so on). The purpose of the child user groups is to separate the users according to their areas of responsibility.

   Depending on whether you want the user management to be centralized or decentralized, each individual subgroup can belong to the same partition as their parent user group, managed by the same administrator, or can belong to different partitions, managed by different administrators.
5. Define the individual users and add them as members of the user groups.

   BEST PRACTICE: Try to add the users as members of the smallest group. Let each user inherit everything from the parent user group, and only resort to configuring them individually for exceptions.

Protecting your data center against outside threats

If the security policy of your company requires all corporate databases to reside on a secured network, you must create Directory gateways to allow the Security Center applications located outside the secured network to log on to the system.

Before you begin

Make sure that the *Number of additional Directory servers* supported by your Security Center license allows you to add the *Directory gateways* you need to create. The Directory gateways are counted as *Directory servers* in your Security Center license.

What you should know

All Security Center applications (roles and client applications) must connect to a Directory server in order to log on to the system. All Directory servers must access the Directory database where the system configuration is stored. If the Directory database resides on a secured network, no applications located outside the secured network are allowed to access it. To avoid violating the security policy, you must create Directory gateways on the non-secured network.

To create Directory gateways:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Select the **Directory Manager** () role, and then click the **Directory servers** tab.

3 At the bottom of the server list, click **Advanced** ().

An extra column, **Gateway**, opens in the list.

4 At the bottom of the list, click **Add an item** (✚).

5 In the dialog box that opens, select the server you want to add, and click **Add**.

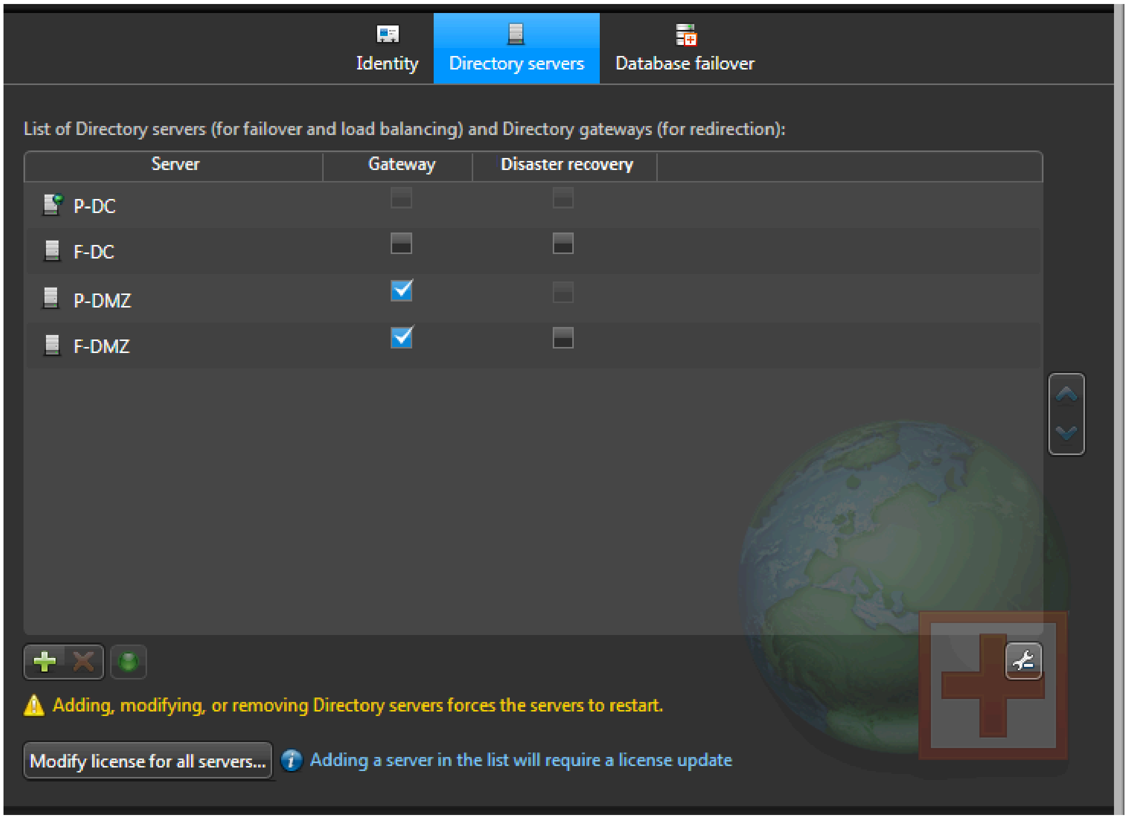
6 Add more servers to the list if necessary.

7 Select the **Gateway** option on servers you want to use as Directory gateways.

A Directory gateway must be located on the non-secured network. It does not need to access the Directory database, but it needs to connect to the main server. The following example shows a system with two Directory servers, one of which is the main server, and two Directory gateways.

NOTE:

- *Load balancing* only occurs between Directory servers. A user trying to connect to a Directory gateway will not be redirected to a Directory server, and vice versa.
- The **Disaster recovery** option only applies to Directory servers, not to Gateways.



List of Directory servers (for failover and load balancing) and Directory gateways (for redirection):

Server	Gateway	Disaster recovery
P-DC	☐	☐
F-DC	☐	☐
P-DMZ	☑	☐
F-DMZ	☑	☐

Adding, modifying, or removing Directory servers forces the servers to restart.

Adding a server in the list will require a license update

8 Update your license to include the servers that you have just promoted to Directory gateways.

9 Click **Apply**.

After you finish

If you have client workstations that are forced to connect to a specific Directory, update their settings so they connect to one of the Directory gateways instead.

Related Topics

Preparing Directory failover and load balancing on page 167

About hardening

Hardening is the process of enhancing hardware and software security. When hardening a system, basic and advanced security measures are put in place to achieve a more secure operating environment.

The Security Center default settings offer a balance between system security, usability, and performance. By hardening your system, you are optimizing it for more security, but potentially at the expense of some usability or performance. Hardening is an incremental process. How much you harden your security system depends on your threat model and the sensitivity of your information.

The *Security Center Hardening Guide* outlines our recommended procedures to improve your system security.

We define two levels of security in this guide:

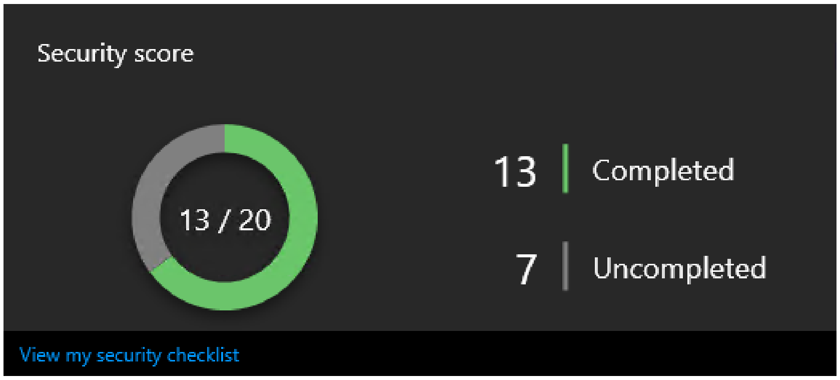
- **Basic level:** Security measures for systems that require minimal security.
- **Advanced level:** Security measures that provide higher security, but are more complex, or take longer to implement. Organizations with strict security policies should adhere to this level. Advanced includes all basic level security measures.

To help you improve your system security and identify areas of concern, the *Security score* widget rates your adherence to the *Security Center Hardening Guide*.

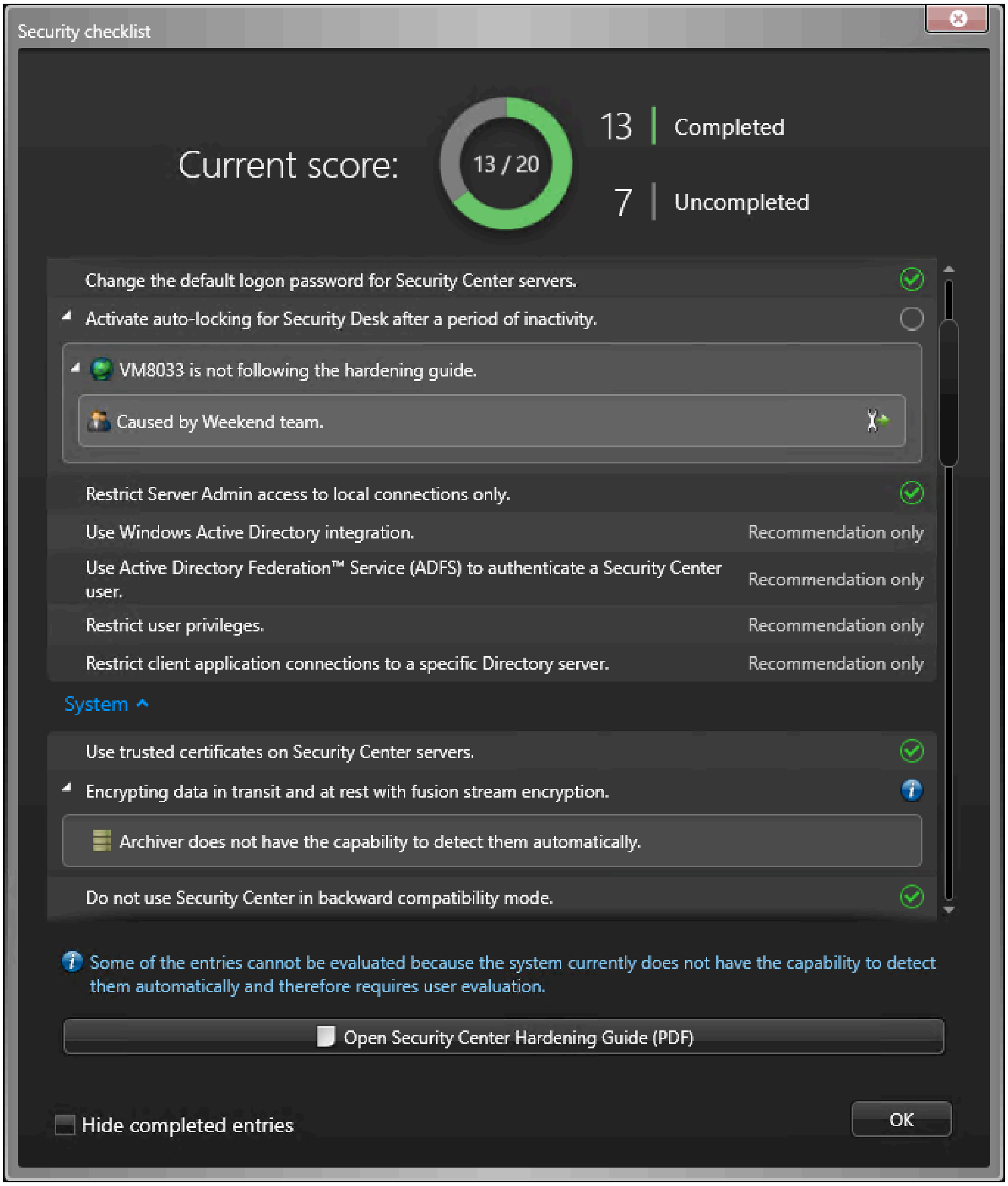
How the Security score widget works

You can track your system security and identify potential vulnerabilities in near real time with the *Security score* dashboard widget.

The security score widget evaluates the local system and measures compliance to the best practices outlined in the *Security Center Hardening Guide*, such as password strength, use of certificates and encryption, and more. Security scores are automatically recalculated as you configure your system.



Your security score is based on a checklist of hardening tasks that apply to the local system. Each completed entry adds one point. The score only includes entries that can be assessed automatically. Hardening tasks that cannot be evaluated or that are flagged *Recommendation only* are not included in the security score.



Security checklist

Current score: 13 / 20

13 | Completed

7 | Uncompleted

Change the default logon password for Security Center servers. ✓

Activate auto-locking for Security Desk after a period of inactivity. ○

VM8033 is not following the hardening guide.

Caused by Weekend team.

Restrict Server Admin access to local connections only. ✓

Use Windows Active Directory integration. Recommendation only

Use Active Directory Federation™ Service (ADFS) to authenticate a Security Center user. Recommendation only

Restrict user privileges. Recommendation only

Restrict client application connections to a specific Directory server. Recommendation only

System

Use trusted certificates on Security Center servers. ✓

Encrypting data in transit and at rest with fusion stream encryption. ⓘ

Archiver does not have the capability to detect them automatically.

Do not use Security Center in backward compatibility mode. ✓

ⓘ Some of the entries cannot be evaluated because the system currently does not have the capability to detect them automatically and therefore requires user evaluation.

Where possible, the security checklist identifies specific roles or entities that do not follow our best practices. To help you complete hardening tasks that are performed in Config Tool, you can click the direct link to open the associated configuration.

Getting started

The *Security score* widget is available with Security Desk dashboards. For more information, see "About dashboards" in the *Security Center User Guide*.

To see the *Security score* widget and add it to a dashboard, your user account must have the *View security widget* privilege.

Entries in the security checklist are named after tasks in the *Security Center Hardening Guide*. For more information on hardening tasks refer to the corresponding topic in that guide.

]

20

Partitions

This section includes the following topics:

About partitions

A partition is an entity in Security Center that defines a set of entities that are only visible to a specific group of users. For example, a partition could include all areas, doors, cameras, and zones in one building.

Partitions eliminate the tedious task of creating one-to-one relationships between users and the entities they are allowed to see in the system. If a user has no rights to a partition, that partition and everything it contains are hidden from that user.

Each partition is defined by the following:

- **List of members:** Entities that belong to the partition (areas, doors, cameras, cardholders, users, and so on).
- **List of authorized users:** Users and user groups that have the right to access the entities in the partition. The type of access each user has (view, add, modify, delete) is determined by the *privileges* of each individual user. Exceptions to the basic privileges of a user can be configured for each partition the user has access to.

  NOTE: An authorized user of a partition is not necessarily a member of that partition, nor is a user who is a member of a partition necessarily an authorized user.

Benefits of partitions

Dividing your system into smaller parts has the following benefits:

- It reduces the scope of what a user can access for security reasons. For example, in a multi-site system, it might be undesirable for the security team of one site to be able to see or interfere with the activities of the security team of another site.
- It reduces the scope of a user's work to make it more manageable. If a user is only responsible for one part of the system (one site in a multi-site system), it is better not to distract the user with the entities the user is not responsible for.

System-created partitions

By default, two partitions are created in Security Center. They are invisible unless you explicitly created other partitions in your system. The idea is that if you do not need to divide your system into partitions, you do not need to see any partition at all.

- **Root partition:** The *root* partition (🌐) is the partition that contains everything your create in your system. It is named after your *main server*. When there are no user-created partitions in the system, all created entities belong to the root partition, and all users are authorized users of the root partition.
- **System partition:** The *System* partition (🌐) is a partition that is exclusively managed by the system for the purpose of always keeping certain system entities accessible to all users, such as the *Always* schedule, the *Default network* entity, the main server entity, the Health Monitor role, the Report Manager role, and so on. No one can alter the System partition, not even the system administrators.

NOTE: The root partition and the System partition are the only two top level partitions in the system. All partitions you create are subordinate to the root partition.

Creating partitions

To divide your system into smaller, manageable parts, and hide some of those parts from certain users, you can create partitions.

What you should know

The first partition you create is always added to the root partition. Subsequent partitions you create are added to the partition you select in the entity tree. If none are selected, the system will ask you to specify under which partition you want to create the new partition.

To create a partition:

1 From the Config Tool home page, do one of the following:
- Open the *User management* task, click **Add an entity** (➕), and then click **Partition**.
- Open any administration task, click **Add an entity** > **Show all** > **Partition**, or click **More** (▼) beside the **Add** (➕) button, and then click **Partition**.

2 If a partition is selected in the entity tree before you click **Add**, the new partition is immediately created under the selected partition.

a) Enter the name of the **New partition**.

b) In the **Identity** tab, enter the partition description.

3 If no partition was selected in the entity tree before you click **Add**, the *Create partition* wizard opens.

a) On the *Basic information* page, enter the name and description of the new partition.

b) From the **Partition** list, select the parent partition that this new partition should belong to.

The new partition is created.

4 If you already have entities ready to be added to the new partition, add them.

5 If users and user groups are already created in your system, grant access rights for the new partition to those who need it.

You can add newly created entities directly to the partition.

Related Topics

About partitions on page 423

Updating the content of partitions on page 425

Granting access rights for partitions on page 426

Updating the content of partitions

You can control the visibility of entities to users in your system by adding or removing entities from the partitions these users are authorized to access.

What you should know

When you put related entities, such as cardholders and credentials, into different partitions, users that are not authorized to access all the partitions involved may not have all the access rights they need to perform their tasks. To simplify the partition configuration process, when you add or remove entities from a partition, the system automatically adds or removes their related entities from that partition. The common sense rules applied by the system are as follows:

- Adding a user group or a cardholder group also adds their members.
- Adding a user or a cardholder does not automatically add their parent groups.
- Removing a user group or a cardholder group also removes their members.
- Removing a user or a cardholder does not automatically remove their parent groups.
- Adding a cardholder also adds their associated credentials.
- Removing a cardholder also removes their associated credentials.
- Adding a credential does not automatically add its associated cardholder.
- Removing a credential does not automatically remove its associated cardholder.
- When adding an entity that has child entities attached (such as an area or a role), you need to specify whether or not you want to add its child entities as well (which includes everything that's below that entity's hierarchy).
- When removing an entity that has child entities attached (such as an area or a role), you need to specify whether or not you want to remove its child entities as well (which includes everything that's below that entity's hierarchy).
- Adding an entity to a partition does not remove it from the other partitions it belongs to. There is no limit to the number of partitions an entity can belong to.
- Removing an entity from a partition automatically adds it to the root partition if that entity does not belong to any other user-created partition.
- You cannot remove an entity from the root partition if that entity does not belong to any other partition.

To update the content of a partition:

1 From the Config Tool home page, open any administration task, and select a tab that shows an entity tree.

   If the partitions are not visible, click **Show partitions** (🌐) in the **Search** box or press **F4**.

2 Select the partition you want to modify, and click the **Properties** tab.

   The current contents of the partition are displayed in the **Members** list.

3 Do either one of the following:

   - To add entities to the partition, click **Add** (➕), select the entities from the *Search* dialog box, and then click **Select**.
   - To remove entities from the partition, select the entities from the **Members** list, and then click **Remove** (✖).

   TIP: Alternatively, you can change the content of partitions directly from the entity tree, using drag-and-drop to move entities, and Ctrl+drag-and-drop to copy entities.

All changes are immediately applied.

Granting access rights for partitions

To allow users to access the entities contained in a partition, you must grant access rights for that partition to the concerned users and user groups.

What you should know

Access rights for partitions are governed by the following rules:

- Access rights for partitions are inherited from parent user groups.
- Inherited access rights cannot be revoked.
- Access rights not granted to a user group can be granted to the members of the user group.
- Granting access rights for a partition to a user or user group also grants access rights for its child partitions to the same user or user group.
- Revoking access rights for a parent partition from a user or user group also revokes access rights for its child partitions from that user or user group, except when those access rights are inherited from parent user groups.
- Revoking access rights for a child partition from a user or user group does not revoke the access rights for its parent partition from that user or user group.

To grant access rights for a partition to a user:

1. From the Config Tool home page, open the *User management* task, select a user, and then click the **Access rights** tab.
2. Select the check box beside the partition you want to grant access rights for.

   This action automatically grants access rights for all its child partitions as well.
3. To revoke access rights for some of the child partitions, clear the check box beside the selected child partitions.
4. Click **Apply**.
5. If necessary, overwrite the basic privileges this user has over the partition.
6. Click **Apply**.

21

Users and User groups

This section includes the following topics:

About user groups

A user group is an entity that defines a group of users who share common properties and privileges. By becoming member of a group, a user automatically inherits all the properties of the group. A user can be a member of multiple user groups. User groups can also be nested.

Benefits of user groups

Since all the users that are part of the user group automatically inherit all the properties of that group, this simplifies the configuration of users on large systems.

Administrators user group

The *Administrators* user group is a system entity that is created during installation. It cannot be deleted or renamed. Members of this user group are also known as *system administrators*. They have the same administrative rights as the *Admin* user, and their rights cannot be revoked.

BEST PRACTICE: For reasons of traceability, rather than letting everyone use the same *Admin* account, it is best to create a separate user account for each administrator.

Creating user groups

To group users who share common properties and privileges, you can create user groups.

What you should know

You can also import user groups from your corporate directory service.

To create a user group:

1. From the Config Tool home page, open the *User management* task.
2. Click **Add an entity** (➕) and then click **User group** (👤).
3. On the *User group information* page, enter a name and description for the user group.
4. From the **User group** list, select the parent group for the new user group.

   The user group automatically inherits the properties of its parent user group.

   NOTE: Concerning the user group's partition membership:

   - If you select **Unassigned**, the new user group will be added to the root partition.
   - If you select a parent user group, the new user group will be added to the same partition that the parent user group belongs to.
5. To grant the user group a predefined set of privileges, select a **Privilege template** from the list.

   NOTE: If you are unsure of what privileges the user group needs, you can postpone this decision to later. The privilege template can be applied at any time.
6. Click **Next**.
7. If partitions are in use, go to the *Access rights* page and select the partitions for which access rights are to be granted to this user group.
8. Click **Next**.
9. On the *Creation summary* page, verify that both the partition the user group belongs to and the ones the user group is authorized to access are as you intended.
10. Click **Create** > **Close**.

    The new user group is created.
11. (Optional) Make this user group a subordinate of another user group.

Related Topics

Privilege templates on page 440

Adding subordinate user groups

To save time on configuring your system, you can create sub-user groups that inherit all the attributes of their parent group.

What you should know

Adding sub-user groups is helpful if you have multiple levels in your management team, and the sub-groups share almost all the same properties and privileges, for example, a day shift user group and a night shift user group on your security team.

To add a subordinate user group:

1. Open the *User management* task.

2. In the entity browser, select the user group to configure.
3. In the *Relationships* section of the *Identity* page, select **Parent user groups**, and click **Insert an item** (➕).
4. Select one or more parent user groups, and click **Select** > **Apply**.

Adding users as members of user groups

To simplify the configuration of your system, you can add users as members of a user group so they inherit all the properties of that group.

To add a user as a member of a user group:

1. From the Config Tool home page, open the *User management* task.
2. Select the user group to configure, and click the **Properties** tab.
3. Under the **Members** section, click **Add** (➕).
4. Select one or more users, and click **Select** > **Apply**.

   TIP: Alternatively, you can modify the user groups' membership directly from the entity tree, using drag-and-drop to move, and Ctrl+drag-and-drop to copy.

About users

A user is an entity that identifies a person who uses Security Center applications and defines the rights and privileges that person has on the system. Users can be created manually or imported from an Active Directory.

Each user is assigned a username and a password, which are the credentials required to log on to the system.

What a person can do on the system is restricted by their user attributes:

- **Privileges:** Limits the types of activities the user can perform on the system.
- **Access rights for partitions:** Limits the entities the user can exercise their privileges on.

A user can be a member of one or more *user groups*. Users can inherit the privileges and the access rights from their parent user groups.

Admin user

The *Admin* user is a user created by default and cannot be deleted or renamed. It has full administrative rights to configure Security Center. A person logged on as *Admin* can add, modify, and delete any entity in Security Center.

BEST PRACTICE: The *Admin* user is created with a blank password at software installation. For security reasons, you should immediately change the *Admin* user's password after software installation.

User levels

A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera PTZ, viewing the video feed from a camera, or staying logged on when a threat level is set. Level 1 is the highest user level, with the most privileges. User levels range from 1-254. The user level can be inherited from a parent user group. If the user has multiple parents, the highest user level is inherited. If the user has no parent group, the lowest user level (254) is inherited.

User levels affects four things in Security Center:

- They determine which users are logged out of the system when a threat level is set. For example, if you configure a threat level to trigger the *Set minimum user level* action, when the threat level is set, users with a lower user level than the one you specified are logged off.
- They determine which users can continue viewing a video stream when a camera is blocked in Security Desk. When you block a camera, users that have a lower user level than the one you specified can no longer view the video stream.
- They determine which users lose their video stream connections if a maximum bandwidth limit is configured for video streams that are redirected from a remote site, and the bandwidth limit is exceeded. When the bandwidth limit is reached and a user with a high user level requests a stream, the user with the lowest user level who is currently viewing video that is being redirected through that redirector loses their stream connection. If multiple users with the same user level are viewing video streams from that redirector, the user who requested the video stream last loses the stream connection.
- They determine which user has priority over the PTZ controls of a camera when two or more users are trying to take control of a camera at the same time.

  Users can be given different user levels for PTZ controls that override their general user level. Priority is always given to the user with the highest level (1=highest). If two competing users have the same user level, the user who requested the stream first is given priority.

  Once a user gains control over a PTZ camera, it is locked by that user. This means that no other users can take control of that camera unless they have a higher user level. The control over the PTZ camera is automatically released after a period of inactivity (configured from the camera’s **Hardware** tab).

Related Topics

About privileges on page 438
About partitions on page 423

Creating users

To allow someone to log on to Security Center, you must create a user entity for them with logon credentials.

What you should know

You can also import users from your corporate directory service.

For security purposes, the *Entity name* for this user must be unique, because it is also the username they use to log on to Security Center.

To create a user:

1. From the Config Tool home page, open the *User management* task.
2. Click **Add an entity** (➕) and then click **User** (👤).
3. On the *User information* page, enter a username that does not already exist.
4. Type a password for this user to log on to Security Center, and then confirm the password.
5. Enter the user's first and last name.
6. From the **User group** list, select the parent group for the new user.

   The user automatically inherits the properties of its parent user group.

   NOTE: Concerning the user's partition membership:

   - If you select **Unassigned**, the new user will be added to the root partition.
   - If you select a parent user group, the new user will be added to the same partition that the parent user group belongs to.
7. To grant the user a predefined set of privileges, select a **Privilege template** from the drop-down list.

   NOTE: If you are unsure of what privileges the user needs, you can postpone this decision to later. The privilege template can be applied at any time.
8. If partitions are in use) Go to the *Access rights* page and select the partitions for which access rights are to be granted to this user.
9. Click **Next**.
10. On the *Creation summary* page, verify that both the partition the user belongs to and the ones the user is authorized to access are as you intended.
11. Click **Create** > **Close**.

The new user account is created.

After you finish

Configure the user.

Related Topics

Privilege templates on page 440

Configuring user settings

After a user is created in Security Center, you can configure their properties, and limit what they are allowed to do on the system.

Before you begin

Create the user.

What you should know

Instead of configuring the properties of an individual user, you can add the user as a member of a user group so that they inherit all the properties of the group.

To configure a user's settings:

1 From the Config Tool home page, open the *User management* task.

2 Select the user to configure.

3 Click the **Properties** tab, and configure the user settings as needed.

- To temporarily prevent the user from logging on to Security Center, see Deactivating user profiles on page 435.
- To be able to send emails or messages to this user, type an email address in the **Email address** field, and click **Apply**.

  You can send emails to users using the *Send an email* and *Email a report* actions.
- To change the user's password or password settings, see Changing password settings for users on page 435.
- To set the user's user level, in the **User level** option, specify if the user inherits their user level from its parent user group, or set a specific level.
- (Optional) To configure a different user level for controlling PTZ motors, see Overriding user levels for specific areas and cameras on page 641.

4 Click **Apply**.

5 Grant access rights for partitions to the user.

6 Assign privileges to the user.

7 Customize how the user can log on.

8 Click the **Advanced** tab, and configure the user settings as needed.

- To cycle the user's open tasks when they log on to Security Center, switch the **Start task cycling on logon** option to **ON**.

  TIP: To prevent the user from stopping the task cycling when Security Desk is open, deny them the *Start/stop task cycling* privilege.
- To only allow playback of recently archived video for the user, set **Limit archive viewing** to **ON** and set the length of the time window. You must switch **Inherit from parent** to **Override** to change this setting.
- (Only non-administrative users) To display GUIDs instead of entity names for the user in Security Desk and Config Tool and prevent the user from updating entity name fields, set **Scramble entity names** to **ON**. You must switch **Inherit from parent** to **Override** to change this setting.
- When the user exports video (G64x) or snapshots, the system can include metadata to exported videos or snapshots, such as camera name, creation date, and camera coordinates, which can be useful for investigation. To enable metadata with exported files for the user, switch the **Include additional properties on export/snapshot** option to **ON**.
- To discourage the unauthorized release of video footage by including identifying text in the video stream, see Configuring video watermarking on page 449.

9 Click **Apply**.

Related Topics

About users on page 431

Deactivating user profiles

You can deactivate the profile of users that should no longer be allowed to log on to Security Center.

What you should know

A user cannot log on when their profile is deactivated. Deactivating a user's profile while the user is logged on will immediately log off the user.

To deactivate a user's profile:

1 From the Config Tool home page, open the *User management* task.

2 Select the user to configure, and click the **Properties** tab.

3 Switch the **Status** option to **Inactive**, and click **Apply**.

Changing password settings for users

You can set a user's password to expire after a certain amount of time, force users to change their password on next logon, or enforce a minimum complexity for all user passwords.

What you should know

Password complexity requirements apply to all new passwords, and take effect when a user changes their current password.

Only users who have the *Change own password* user privilege can change their own password. Otherwise, they must contact their administrator to change their password.

To change the password settings for a user:

1 From the Config Tool home page, open the *User management* task.

2 Select the user to configure, and click the **Properties** tab.

3 To change the user's password, click **Change password**, type a password, confirm the password, and click **OK**.

4 To set an expiry date for the user's password, switch the **Expires** option to **ON**, and select the number of days.

The system automatically warns users if their passwords are expiring soon, and gives them a chance to set a new password immediately. You can set the password expiry notification period to between 0 and 30 days from the System task.

5 To require the user to change their password the next time they log on to Genetec Patroller™ or Security Desk, switch the **Change on next logon** option to **ON**.

6 Click **Apply**.

Creating encrypted user password files in Security Center

If you are logging on to Security Center using command-line arguments, but you do not want to show the user's password in the command line, you can create an encrypted password file for the user and reference that file in the command line instead.

Before you begin

- Make sure you are on the workstation that the user will be using to log on.
- You must be logged on as the user for whom you are creating the encrypted password file.
- The user must have the *Modify user properties* privilege to create the password file. If not, as an administrator, you can temporarily grant the user this privilege before starting this procedure, and remove this privilege after the password file is created.

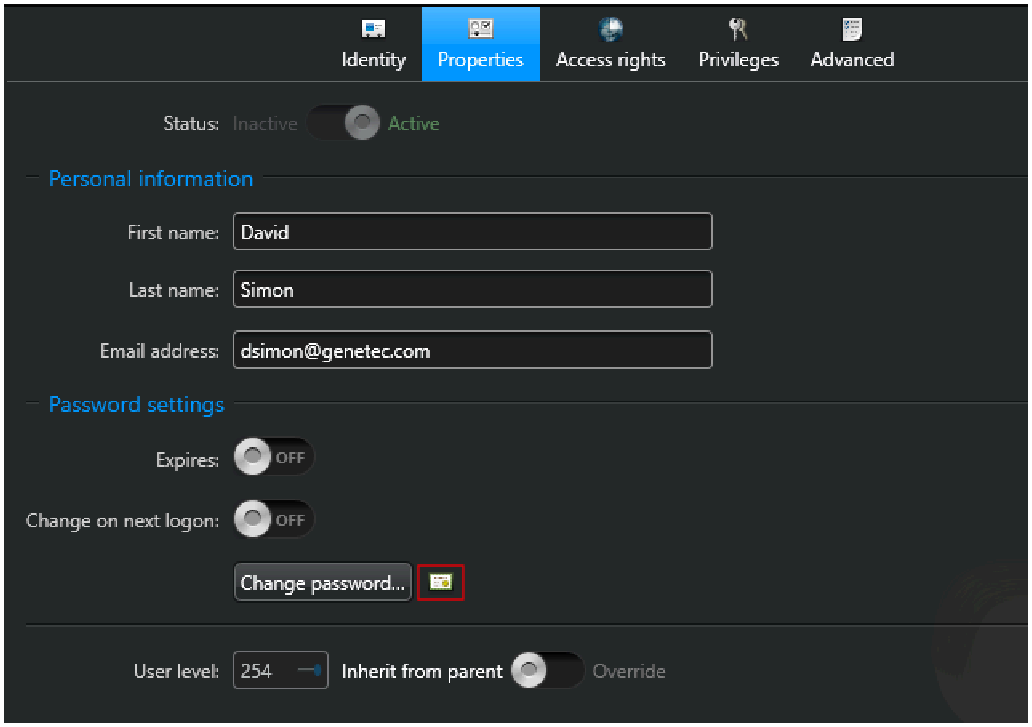
What you should know

The encrypted password file is used to authenticate the user instead of the password.

IMPORTANT: The encrypted password file is unique to the workstation it is created on, and to the user who created the file. The password file must be created by the same user who will be logged on through the command line, and on the same workstation that the user will be logged on to. If later somone changes the password, the password file must also be recreated.

To create an encrypted user password file:

1. Open Config Tool and log on to Security Center with the user for which you want to create the encrypted password file.
2. Open the *User management* task.
3. Select the user to configure, and click the **Properties** tab.
4. Click the **Save encrypted password to disk** button.



Status: Inactive Active

First name: David

Last name: Simon

Email address: dsimon@genetec.com

Expires: OFF

Change on next logon: OFF

User level: 254

5. Choose where to save the file, and then click **Save**.

The *.pwd* file is saved on the workstation. You can now reference the file in a command line to log on to Security Center with that user.

Related Topics

Modifying the Config Tool or Security Desk shortcut using command line arguments

Command line arguments for opening Config Tool or Security Desk

About privileges

Privileges define what users can do, such as arming zones, blocking cameras, and unlocking doors, over the part of the system they have access rights to.

User privileges in Security Center are divided into the following groups:

- **Application privileges:** Grant access to the Security Center applications.
- **General privileges:** Grant access to the generic Security Center features.
- **Administrative privileges:** Grant access to entity configuration in Config Tool.
- **Task privileges:** Control accessibility to the various Security Center tasks.
- **Action privileges:** Control the *actions* that can be performed on the system entities.

For a list of available privileges, refer to the *Security Center 5.11 Privileges* document available on the Genetec™ TechDoc Hub.

You can also refer to the *Privileges* page of a user or user group in the Config Tool *User management* task.

Privilege hierarchy

Privileges are organized in a hierarchy, with the following behavior:

- For a child privilege to be allowed, the parent privilege must be allowed.
- If a parent privilege is denied, all child privileges are denied.
- A child privilege can be denied when the parent privilege is allowed.

Privilege inheritance

Privilege settings can be inherited from user groups and replaced at the member (user or user group) level according to the following rules:

- A privilege that is undefined at the group level can be allowed or denied at the member level.
- A privilege that is allowed at the group level can be denied at the member level.
- A privilege that is denied at the group level is automatically denied at the member level.
- When a user is a member of multiple user groups, the user inherits the most restrictive privilege settings from its parents. This means that *Deny* overrules *Allow*, and *Allow* overrules *Undefined*.

Exceptions to privilege rules

The following exceptions apply to the privilege rules:

- **Administrative users:** Members of the *Administrators* user group (which include the *Admin* user) have full administrative rights over the system. They can configure Security Center as they see fit. The *Admin* user and the *Administrators* user group are created at system installation. They have all the privileges and cannot be modified nor deleted.
- **Actions reserved for administrative users:** There are actions that only administrative users can perform because they can potentially affect the entire system. These actions are not associated to any privilege.
  - Adding, modifying, and deleting macros.
  - Creating generic event-to-actions (without a specific source entity).
  - Running the *Diagnostic data collector*.

Privilege exceptions for partitions

A user (or user group) has a set of *basic privileges* that is the result of the privileges inherited from their parent user groups, plus the ones explicitly allowed or denied to the user.

When a user is given access to a partition, their basic privileges are applied by default to the partition. As a system administrator, you can overwrite the privileges a user has over a specific partition. For example, a user can be allowed to configure alarms in partition A, but not in partition B. This means that a user can have a different set of privileges for each partition they have access to. Only *Administrative* and *Action* privileges, plus the privileges over public tasks, can be overwritten at the partition level.

The Manage partition memberships option

To allow a user to move entities from one partition to another to which they have access, you must grant them the associated *Add/Delete <entities>* pair of privileges for each entity type you allow them to move between partitions. If you do not want users to add and delete entities, but allow them to move entities between partitions to which they have access, you can enable the *Manage partition memberships* option from the user's *Advanced* configuration page.

NOTE: The *Manage partition memberships* option is treated as a privilege in the Security Center SDK. You can enable or disable this option by granting or revoking the `SdkPrivilege.ManagePartitionMemberships` privilege using the `SetPrivilegeState()` method.

Related Topics

About partitions on page 423

Assigning privileges to users on page 441

Privilege templates

Privilege templates are predefined privilege configurations, based on standard security personnel profiles, that you can apply to users and user groups to simplify the creation process. Once applied, you can fine tune the privileges manually.

You cannot rename, modify, create, or delete privilege templates, but you can apply them at any time. You can freely modify the privilege settings after a privilege template is applied to a user or user group.

BEST PRACTICE: Create one user group for each privilege template if necessary. After your model user groups are created, users can inherit privileges from them.

Types of privilege templates

Security Centerprovides the following privilege templates:

- **Reporting:** This template only grants the privileges to run Security Desk and to execute the most basic reporting tasks, excluding those for AutoVu™ ALPR. A user with this set of privileges alone cannot view any video, control any physical devices, or report incidents.
- **Operator:** This template is for security operators who need to monitor real time events in the system. It grants them the privileges to use the Monitoring task, view video, manage visitors, credentials, and badge templates, add bookmarks and incidents, save snapshots, unlock doors, and so on.
- **Investigator:** This template is for investigators. It grants the privileges to use the Monitoring task, view video, control PTZ cameras, record and export video, add bookmarks and incidents, use investigation tasks, manage alarms and visitors, override door unlock schedules, save tasks, and so on.
- **Supervisor:** This template is for people who have supervisory responsibilities. It grants the same privileges as the *Investigator* template, plus the privileges to use maintenance tasks, manage cardholders and credentials, modify custom fields, set threat levels, block cameras, and perform people counting.
- **Provisioning:** This template is for the system installer. It grants almost all configuration privileges, with only a few exceptions (managing roles, macros, users, user groups, custom events, activity trails, threat levels, and audio files).
- **Basic AutoVu™ Operator:** This template is for security operators using AutoVu ALPR. It grants them privileges to use ALPR tasks, configure ALPR entities, create ALPR rules, monitor ALPR events, and so on.
- **Patroller user:** This template is for Genetec Patroller™ users.

Assigning privileges to users

You must grant privileges to users for them to do anything in Security Center, including logging on using Security Desk, and so on.

What you should know

Users have a set of basic privileges that are granted to them, or inherited from parent user groups. They also have a set of privileges for every partition in which they are an authorized user. Privileges granted or denied at the partition level replace the basic privileges.

BEST PRACTICE: Individual users should only have the minimum required privileges. When assigning privileges, Security Center offers templates with predefined sets of privileges that can be applied to users or groups.

To help you better understand what your users can do, Security Center includes a Privilege troubleshooter. The Privilege troubleshooter is a tool that helps you investigate the allocation of user privileges in your Security Center system. Use the troubleshooter to verify access rights and help you fix issues.

To assign privileges to a user:

1 From the Config Tool home page, open the *User management* task.

2 Select the user to configure, and click the **Privileges** tab.

3 Use one of the predefined privilege configurations as your starting point.

   At the bottom of the page, click (⚙), and select one of the following:

   - **Apply template:** Select one of the privilege templates to apply.

     Privilege templates can be combined. This means that when you apply a privilege template, you always add privileges. Existing privileges can never be removed as a result of applying a privilege template. To start with a clean slate, go to the top of the privilege hierarchy (**All privileges**) and click **Undefined**.
   - **Set configuration to read-only:** Set all entity configuration privileges found under the *Administrative privileges* group to *View properties* with *Modify properties* denied.
   - **Set configuration to read-write:** Set all entity configuration privileges found under the *Administrative privileges* group to *View*, *Modify*, *Add*, and *Delete*.

4 Fine tune the user privileges by changing the individual privilege settings if necessary.

   Keep in mind that if your user has a parent user group, the privilege inheritance rules apply.

   - **Allow:** Grant the privilege to the user. You cannot select this option if the privilege is denied to the parent user group.
   - **Deny:** Deny the privilege to the user.
   - **Undefined:** Inherit this privilege from the parent user group. If there is not parent user group, this privilege is denied.

5 If necessary, configure the privilege exceptions for each partition the user has access to.

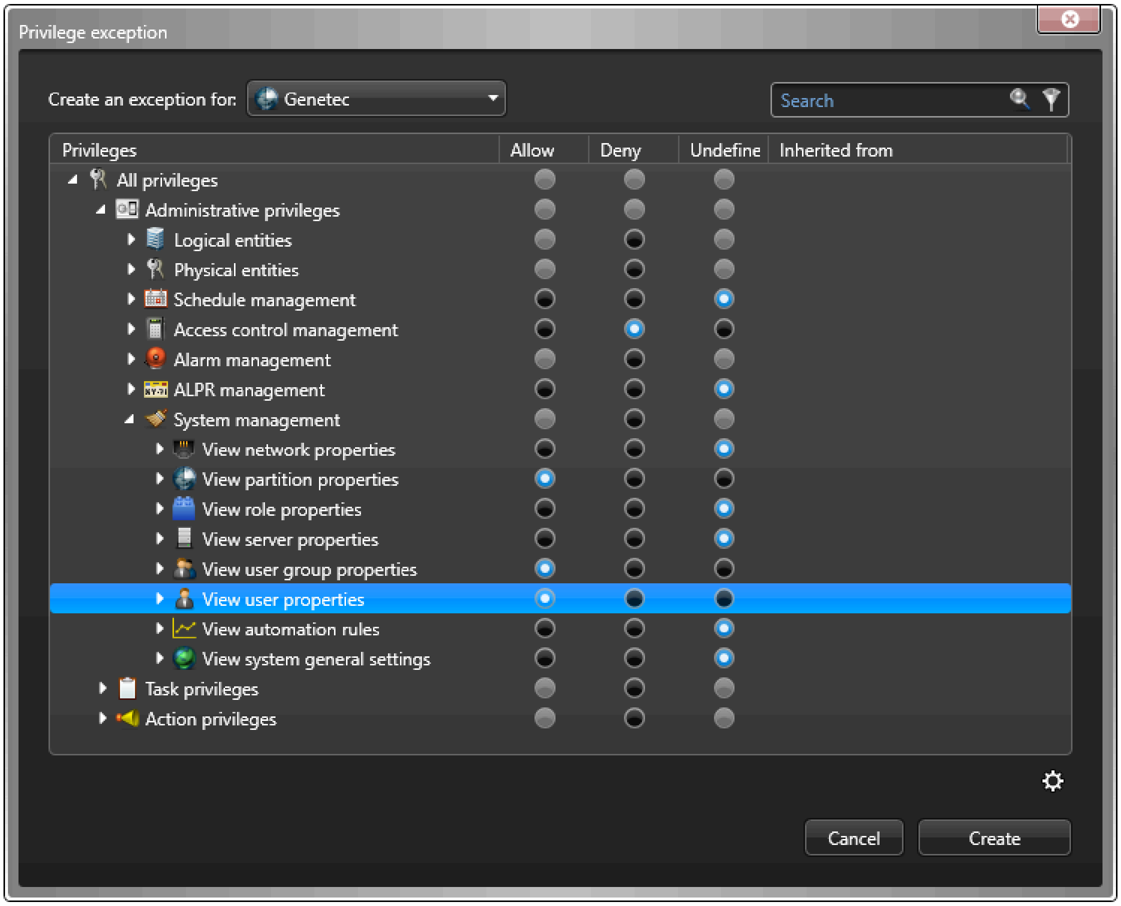
   When a user is given access to a partition, their basic privileges are applied by default to the partition. As a system administrator, you can overwrite the privileges a user has over a specific partition. For example, a user can be allowed to configure alarms in partition A, but not in partition B. This means that a user can have a different set of privileges for each partition they have access to. Only *Administrative* and *Action* privileges, plus the privileges over public tasks, can be overwritten at the partition level.

a) At the bottom of the page, click **Exceptions** (➕).

The *Privilege exception* dialog box opens.

b) In the **Create an exception for** list, select a partition.

c) Change the user's basic privileges as required.

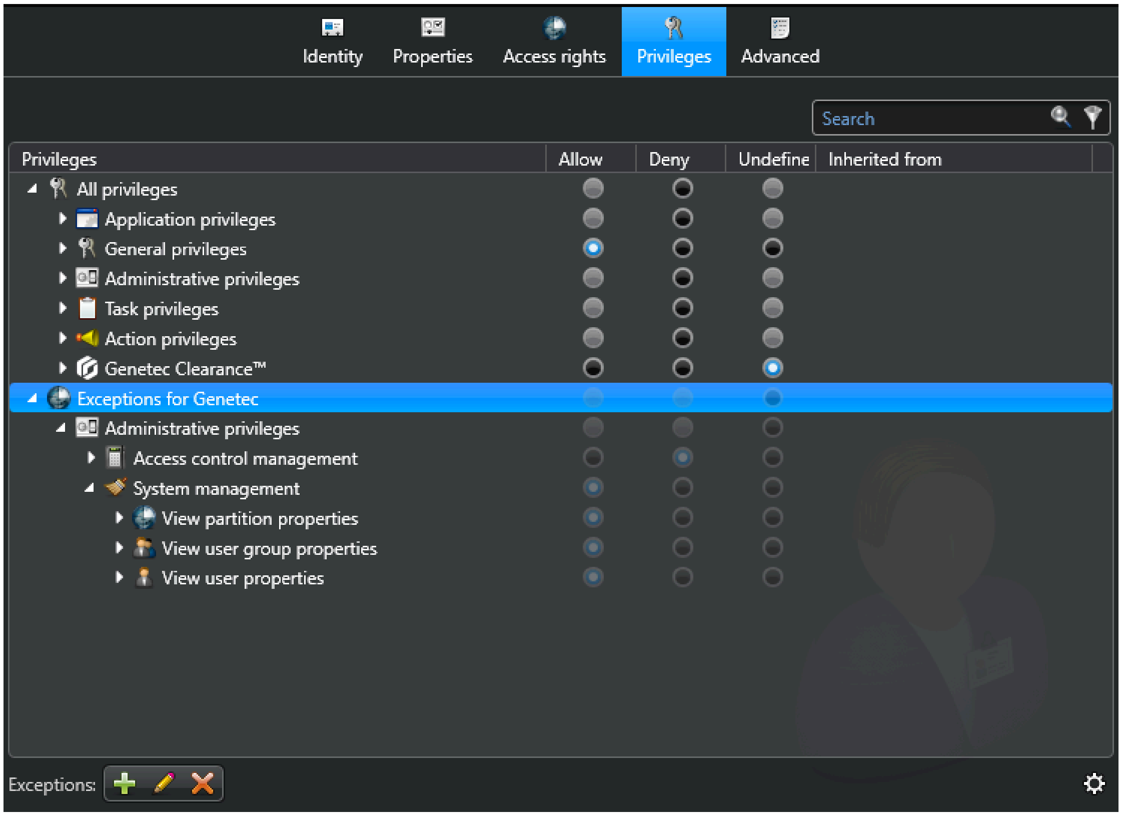


Create an exception for: Genetec

Privileges	Allow	Deny	Undefine	Inherited from
All privileges	○	○	○	
Administrative privileges	○	○	○	
Logical entities	○	○	○	
Physical entities	○	○	○	
Schedule management	○	○	●	
Access control management	○	●	○	
Alarm management	○	○	○	
ALPR management	○	○	●	
System management	○	○	○	
View network properties	○	○	●	
View partition properties	●	○	○	
View role properties	○	○	●	
View server properties	○	○	●	
View user group properties	●	○	○	
View user properties	●	○	○	
View automation rules	○	○	●	
View system general settings	○	○	●	
Task privileges	○	○	○	
Action privileges	○	○	○	

d) Click **Create**.

The privilege exceptions are added at the bottom of the privilege list.



Privileges	Allow	Deny	Undefine	Inherited from
All privileges	○	○	○	
Application privileges	○	○	○	
General privileges	●	○	○	
Administrative privileges	○	○	○	
Task privileges	○	○	○	
Action privileges	○	○	○	
Genetec Clearance™	○	○	●	
Exceptions for Genetec	○	○	○	
Administrative privileges	○	○	○	
Access control management	○	●	○	
System management	●	○	○	
View partition properties	●	○	○	
View user group properties	●	○	○	
View user properties	●	○	○	

6 Click **Apply**.

7 (Optional) Allow the user to move entities from one partition to another to which they have access.

To allow a user to move entities from one partition to another to which they have access, you must grant them the associated *Add/Delete <entities>* pair of privileges for each entity type you allow them to move between partitions.

If you do not want to grant the full *Add* and *Delete* privileges to the user but still want to allow them to move entities between partitions, enable the *Manage partition memberships* option as follows.

a) Click the **Advanced** tab.

b) Enable the **Manage partition memberships** option.

If necessary, switch **Inherit from parent** to **Override** to change this setting.

c) Click **Apply**.

NOTE: When you grant *All privileges* to a user, the *Manage partition memberships* option is also enabled. However, if you disable the **Manage partition memberships** option, it does not affect the other privileges the user has.

Related Topics

About privileges on page 438

Privilege templates on page 440

About the Privilege troubleshooter on page 444

About the Privilege troubleshooter

The Privilege troubleshooter is a tool that helps you investigate the allocation of user privileges in your Security Center system.

The actions available to users in Security Center are controlled by many privileges, which can be defined for individual users or inherited from user groups. The Privilege troubleshooter examines the allocation of privileges in your system, helping you to verify user permissions and fix issues.

You can use this tool to search for and export the following:

- Who has permission to work with a selected entity
- What privileges are granted to selected users or groups
- Who has been granted a privilege, has access to a specific entity, or both

About using the tool

You can open the Privilege troubleshooter from the **Tools** menu in Config Tool if you have the following privileges:

- *View user properties*
- *View user group properties*

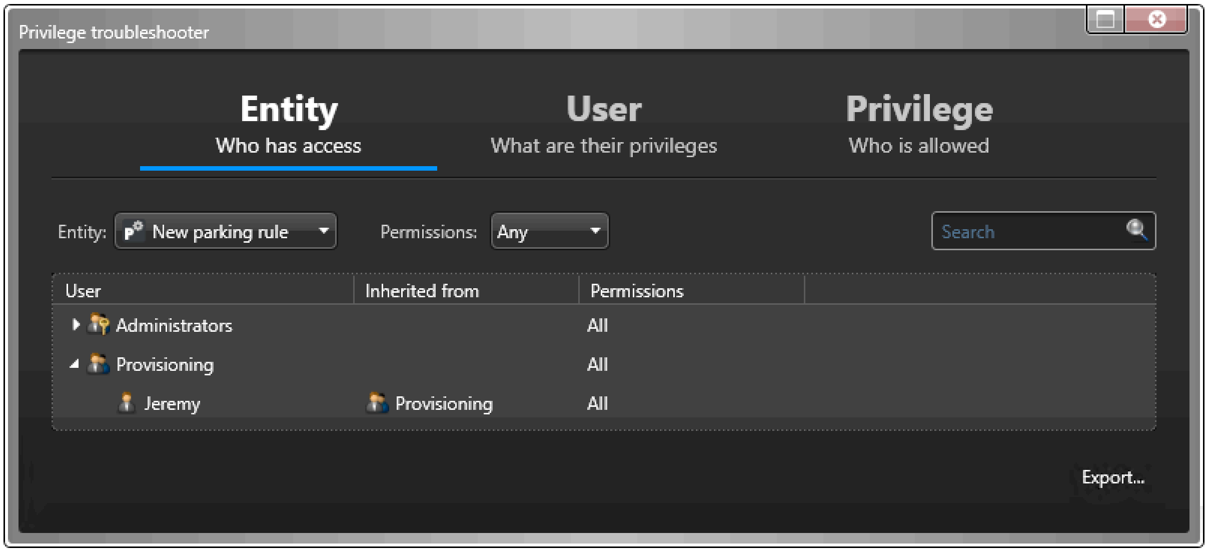
The tool opens in a separate window that is divided into three views in which you can investigate entities, users, or privileges.

You can export the results of your search as an Excel, CSV, or PDF file. Consider the following before exporting:

- The **Export** button is only visible if you have the *Print/export reports* privilege. If you do not have the *Single user print/export* privilege, a second user who does have that privilege must enter their credentials to authorize the export.
- If you filter the results using the search bar, only the visible results are exported.
- The exported data cannot be used as part of a scheduled task or a hot action.
- When there are more than 2000 results, only the CSV format is supported.

Entity view

The *Entity* view shows which users or user groups have sufficient privileges to view, modify, add, or delete the selected entity. If the entity is in a specific partition, these users also have access to the entity.



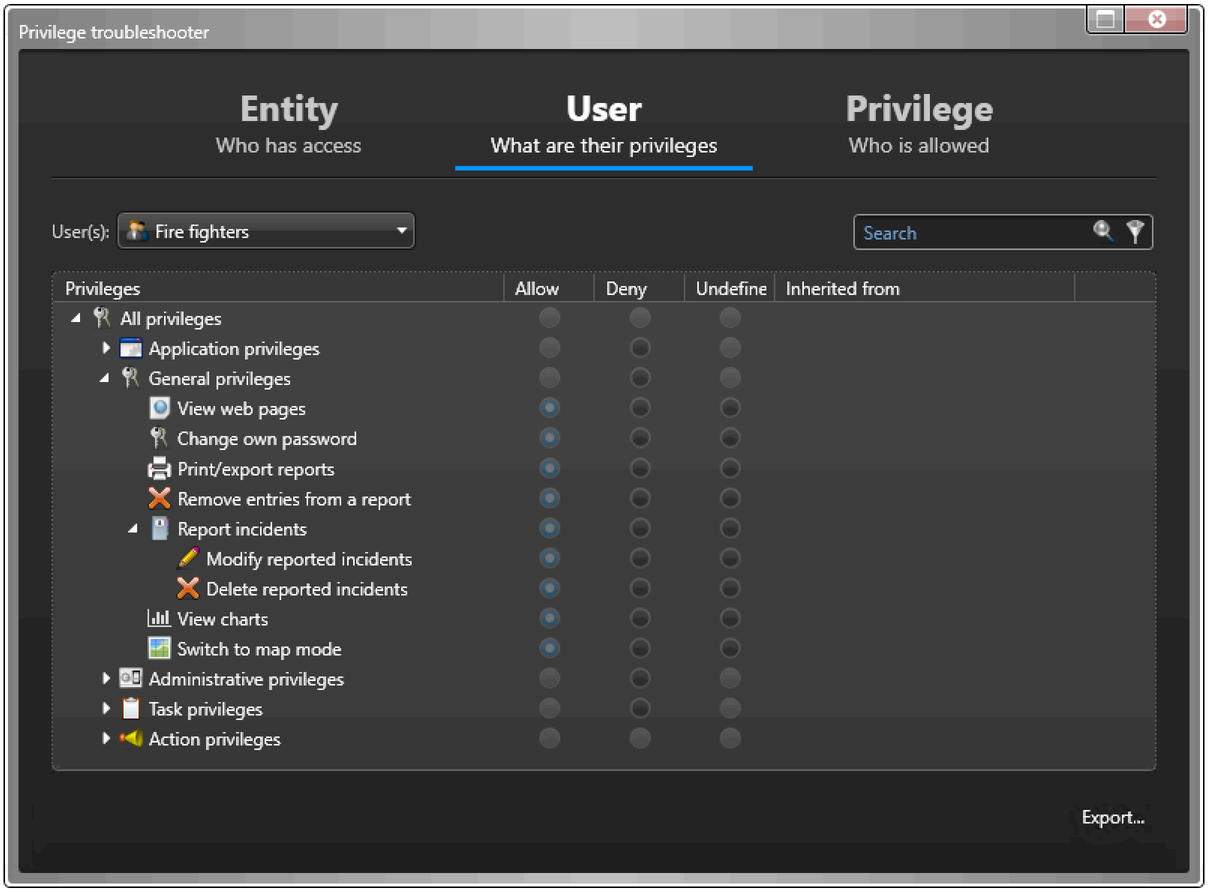
Entity: New parking rule

Permissions: Any

User	Inherited from	Permissions
Administrators		All
Provisioning		All
Jeremy	Provisioning	All

User view

The *User* view shows the full allocation of privileges to a selected user or group.



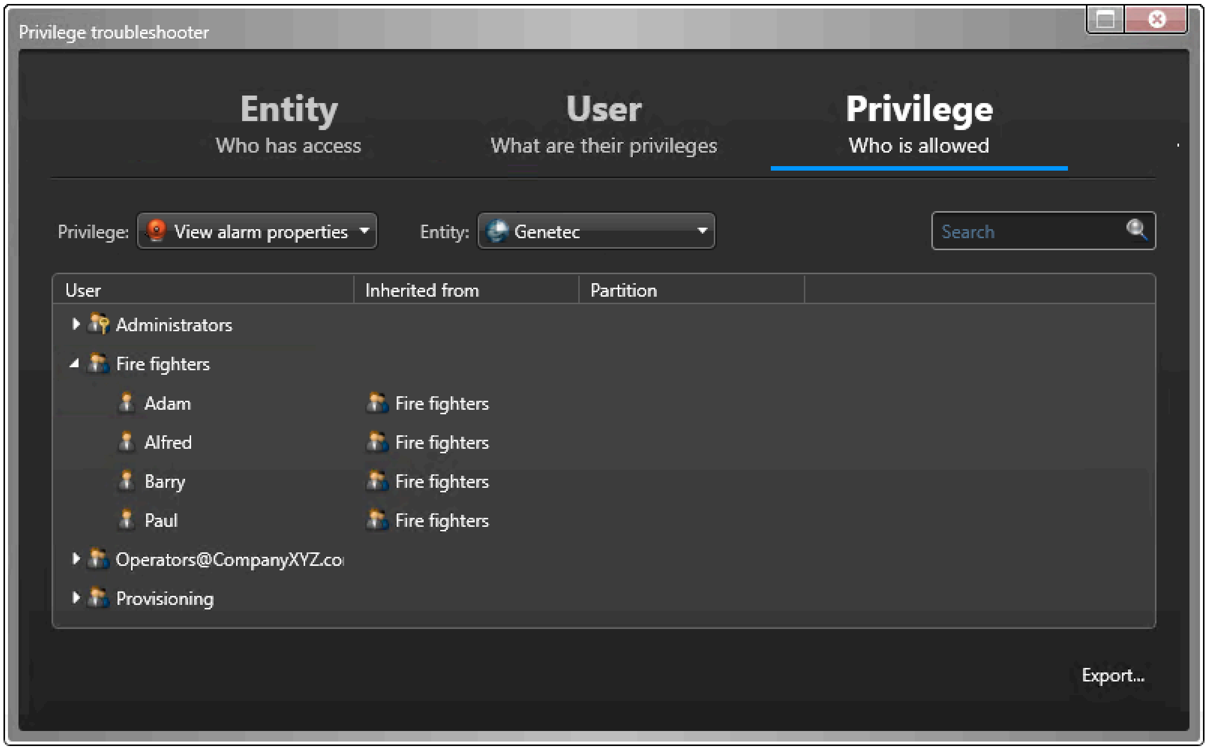
User(s): Fire fighters

Privileges	Allow	Deny	Undefine	Inherited from
All privileges	○	○	○	
Application privileges	○	○	○	
General privileges	○	○	○	
View web pages	●	○	○	
Change own password	●	○	○	
Print/export reports	●	○	○	
Remove entries from a report	●	○	○	
Report incidents	●	○	○	
Modify reported incidents	●	○	○	
Delete reported incidents	●	○	○	
View charts	●	○	○	
Switch to map mode	●	○	○	
Administrative privileges	○	○	○	
Task privileges	○	○	○	
Action privileges	○	○	○	

TIP: To limit the list to permissions that are allowed, denied, or undefined, click **Apply a custom filter** ( ) in the search bar.

Privilege view

The *Privilege* view shows which users or groups have been granted a selected privilege, have access to a selected entity, or both.



Privilege: View alarm properties

Entity: Genetec

User	Inherited from	Partition
Administrators		
Fire fighters		
Adam	Fire fighters	
Alfred	Fire fighters	
Barry	Fire fighters	
Paul	Fire fighters	
Operators@CompanyXYZ.co		
Provisioning		

TIP: Click the **Entity** list and select an entity type to filter the listed entities. You can also use **Apply a custom filter** ( ) to perform an advanced search.

Related Topics

Assigning privileges to users on page 441

About video watermarking

Video watermarking adds visible text to live, playback, and exported video processed by Security Center. This text includes identifying information that is intended to deter unauthorized users from leaking video recordings.

Watermarking is configured for specific users or user groups. When enabled, video requested by affected users through Config Tool, Security Desk, the Web Client, and Genetec™ Web App includes identifying text.

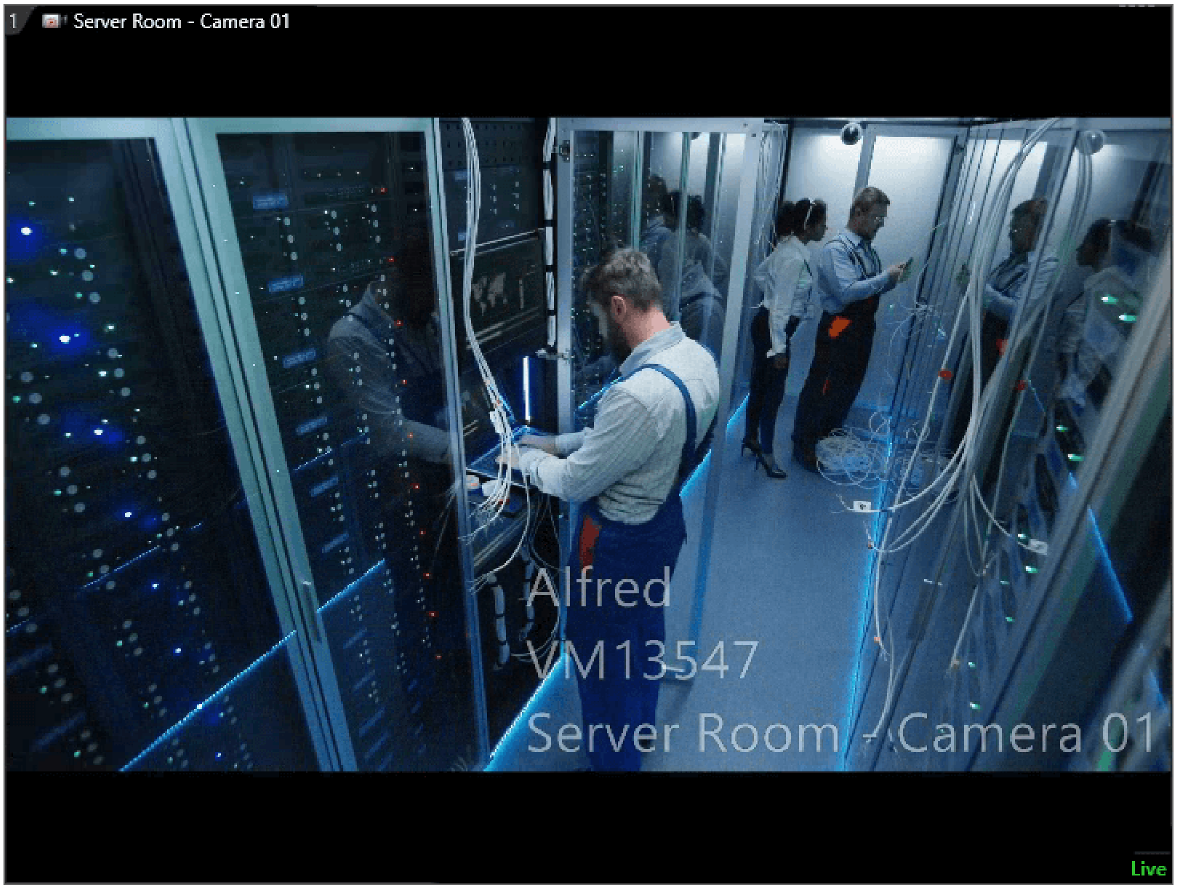
Video watermarks are printed as an overlay onto live and playback video. These static overlays are not redrawn when performing a digital zoom or dewarping.

BEST PRACTICE: To prevent users from bypassing video watermarks, disable digital zoom, especially if watermark text is positioned in a corner.

The text can include one or more of the following variables:

- Security Center user who requested the video
- Workstation where the user logged in
- Camera where the video originated

Each selected variable is displayed on a separate line forming the watermark.



The position, size, and opacity of watermark text can be configured as needed. Watermarks can also be displayed as a mosaic, which duplicates the text to cover the video.

Only users with watermarking enabled see this text. If another user with watermarking disabled views the same live or playback video, it does not include identifying information. This allows authorized users to display and release unobstructed video.

Watermarks and exported video

Watermarks in exported files are visible to all users. To permanently incorporate the text overlay into the video stream, watermarked recordings are transcoded to H.264 during the export process. This transformation is supported to a maximum resolution of 1080p, and can affect video quality.

NOTE: If you are exporting warped video, be aware of the following interactions with video watermarking:

- Watermark text that is exported with a warped video stream is distorted after dewarping.
- Some dewarping software requires unadulterated input. Applying a watermark during export can interfere with future dewarping.

To permit transcoding, users need the *Convert exported files* privilege, which allows them to export watermarked video. The following table summarizes when an exported video file is transcoded:

File format	Input watermarked?	Output transcoded?
G64x and G64	No	No
	Yes	Yes
ASF	No	Yes
	Yes	Yes
MP4	No	No
	Yes	Yes

Video watermarking introduces transcoding to the export process for G64x, G64, and MP4 files. Exporting video in these file formats takes more time for users with watermarking enabled. The delay is most significant on client workstations without hardware acceleration, where it can take up to the duration of a video sequence to export it. Hardware acceleration can greatly reduce the time required to export watermarked video. The performance gain varies with the graphics processing unit (GPU).

BEST PRACTICE: Use workstations capable of hardware acceleration to export watermarked video.

Any digital signatures and encryption in the video source are excluded from the exported file. In addition to *Convert exported files*, users need the *Remove encryption* privilege to export encrypted video with a watermark.

Limitations of video watermarking

The following video sources are not watermarked when viewed by a user with video watermarking enabled:

- Cached video files
- Media Gateway RTSP streams
- Thumbnails and alarm still frames
- Video previews for motion detection, security monitoring, and people counting
- Video accessed by the *VideoSourceFilter* of the Security Center Media SDK
- Video accessed by Config Tool and Security Desk version 5.8 and earlier

Configuring video watermarking

You can configure video watermarking for specific users and user groups. When enabled, all video requested by those users through Config Tool, Security Desk, Web Client, and Genetec™ Web App includes identifying text.

What you should know

Instead of configuring a separate watermark for each user, the video watermarking configuration can be inherited. You can add the user to a user group so they inherit the watermarking configuration of that group.

To configure a video watermark:

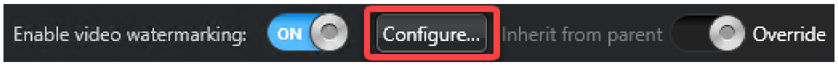
1 From the Config Tool home page, open the *User management* task.

2 Select the user or user group to configure, and click the **Advanced** tab.

3 Under *Security*, set **Enable video watermarking** to **ON**.

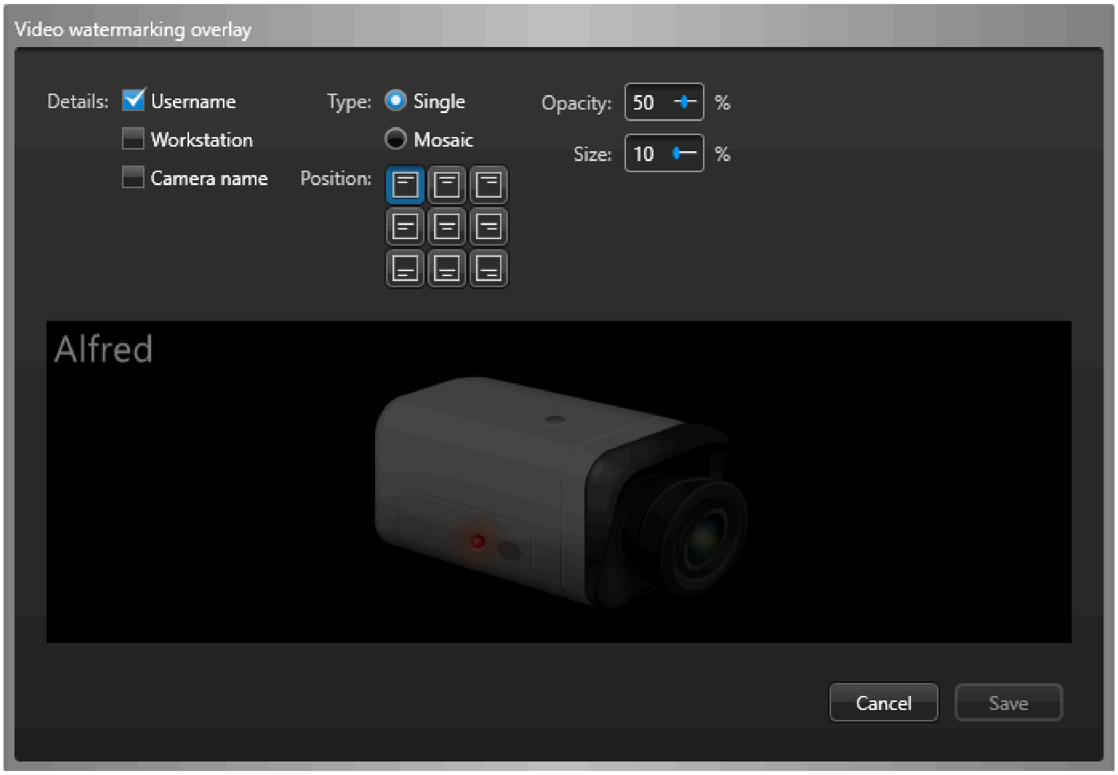
You must switch **Inherit from parent** to **Override** to change this setting.

The **Configure** button is displayed.



4 Click **Configure**.

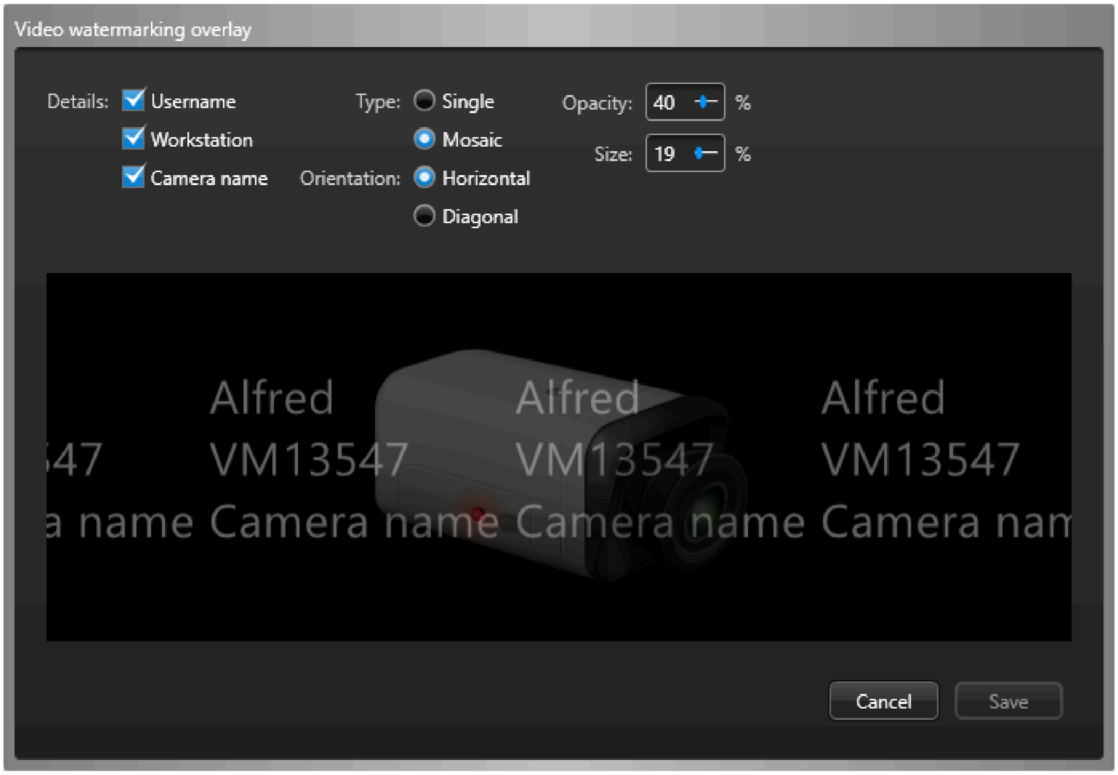
The *Video watermarking overlay* dialog box opens.



5 Set up the video watermark as required and click **Save**.

- **Details:** Select **Username**, **Workstation**, or **Camera name** to add that information to the watermark. At least one detail must be selected.
- **Type:** Select **Single** for a single watermark, or **Mosaic** to repeat the watermark text.
- **Position (Single type only):** Select the location of the watermark text on the video.
- **Orientation (Mosaic type only):** Select **Horizontal** or **Diagonal** to set the orientation of the watermark text
- **Opacity:** Set the opacity of the watermark text. 100% is completely opaque.
- **Size:** Set the size of the watermark text. To ensure a consistent look, text size is independent of the video resolution.

NOTE: The preview screen shows how the watermark will look on the video stream.



Video watermarking overlay

Details: ☑ Username ☑ Workstation ☑ Camera name

Type: ○ Single ● Mosaic

Orientation: ● Horizontal ○ Diagonal

Opacity: 40 %

Size: 19 %

6 Click **Apply**.

The watermark text is added to all live, playback, and exported video processed for the affected users.

Performance impact of video watermarking on client workstations

Video watermarking increases the workload of Security Desk. To ensure acceptable performance, you might need to reassess the capability of your client workstations before enabling this feature.

Watermark impact on workstation performance

Video watermarks are rendered by the client workstation. This extra load reduces the maximum number of live and playback video streams that can be displayed simultaneously. On average, the maximum number of tiles that can be displayed when hardware acceleration is enabled is reduced by 10%. This reduction reaches 30% on machines without hardware acceleration. The performance impact increases with the video resolution.

The following tables show the capability of a sample client workstation to display tiles at VGA and full HD resolutions with software or hardware rendering:

VGA (640x480) at 30 FPS H.264

Rendering	Video watermarking disabled	Video watermarking enabled
Software	31 tiles	24 tiles
Hardware	50 tiles	50 tiles

Full HD (1920x1080) at 30 FPS H.264

Rendering	Video watermarking disabled	Video watermarking enabled
Software	7 tiles	5 tiles
Hardware	20 tiles	18 tiles

BEST PRACTICE: Use workstations capable of hardware acceleration to display watermarked video.

Watermark impact on exporting video

Video watermarking introduces transcoding to the export process for G64x, G64, and MP4 files. Exporting video in these file formats takes more time for users with watermarking enabled. The delay is most significant on client workstations without hardware acceleration, where it can take up to the duration of a video sequence to export it. Hardware acceleration can greatly reduce the time required to export watermarked video. The performance gain varies with the graphics processing unit (GPU).

The following table shows how long it takes to export a 10 minute video sequence to MP4 on a sample client workstation with software or hardware rendering:

Full HD (1920x1080) at 30 FPS H.264, exporting 10 minute sequence to MP4 format

Rendering	Export time with watermarking disabled	Export time with watermarking enabled
Software	10 seconds	8 minutes
Hardware	10 seconds	46 seconds

BEST PRACTICE: Use workstations capable of hardware acceleration to export watermarked video.

Customizing user logon options

You can select how and when users are allowed to log on to Security Center.

What you should know

The settings apply to the local workstation, and affect Security Desk and Config Tool for all users. Changes only take effect the next time a user starts Security Desk or Config Tool.

NOTE: If **Use Windows credentials** is set to **Always** or the **Force Directory to** option is selected, and a user is stuck and cannot log on, hold Ctrl+Shift, and click **Log on**. This either lets the user log on using their Security Center credentials, or forces the **Directory** field to be displayed.

To customize user logon options:

1 From the home page in Config Tool, click **Options** > **General**.

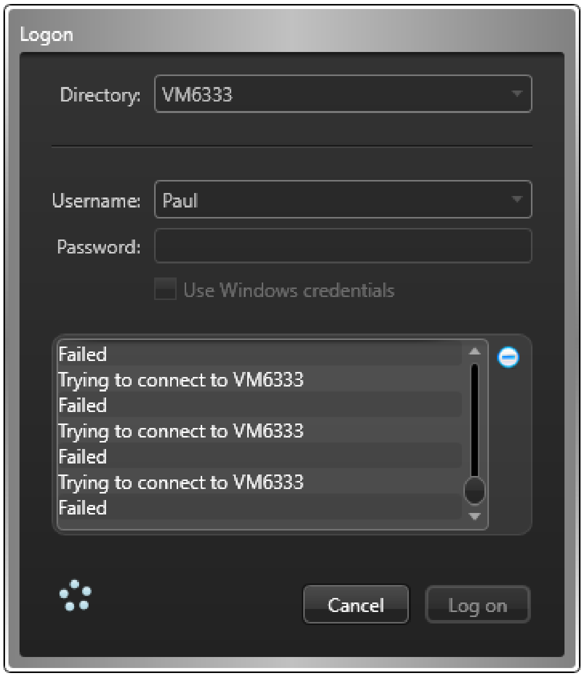
2 To force users to log on using Windows credentials, set the **Use Windows credentials** option to **Always**.

For this option to work, the users who are expected to log on using this computer must be imported from an *Active Directory*.

3 To restrict the access of all users to a specific Directory, select the **Force Directory to** option, and type the name of the Directory.

With this option, users cannot choose the Directory to which they want to connect; the **Directory** field is not displayed in the *Logon* window. However, they can automatically be redirected to another Directory when load balancing is used.

NOTE: If there is a mistake in the Directory name (for example, a typo), users will not be able to connect the next time they try to log on.



Directory: VM6333

Username: Paul

Password:

□ Use Windows credentials

```
Failed
Trying to connect to VM6333
Failed
Trying to connect to VM6333
Failed
Trying to connect to VM6333
Failed
```

4 To bypass Directory load balancing, select the **Prevent connection redirection to different Directory servers** option.

Users will connect to the default Directory or to the Directory they specify when logging on, and will not be automatically redirected to another server. This option is meaningful only if Directory *load balancing* is configured.

5 Click **Save**.

6. To limit the number of workstations a user can log on to at the same time, do the following:
   a) Open the *User management* task.
   b) Select the user you want to configure, and click the **Advanced** tab.
   c) Switch the **Limit concurrent logons** option to **ON**, and select the number of workstations.
7. To select when a user can log on, click **Ad an item** (+) under the **User logon schedule** section.
8. Select predefined schedules, and click **Select**.

   If you select multiple schedules, the schedule conflict rules apply. When two schedules with the same priority level overlap, the blocking schedule has priority over the allowing schedule.
9. To lock the user's session after a period of inactivity, switch the **Auto lock** option to **ON**, and select how long the session must remain inactive before being locked.

   This option only applies to Security Desk. Before being locked, the message Session is about to lock is displayed to the user. After the application is locked, the user must log back on to resume with the current session.

   NOTE: If the user is authenticated through ADFS with passive authentication, the user will be logged off and their current session closed instead of being locked.
10. Click **Apply**.
11. To require the user to log on to Security Center with a logon supervisor, in the *User management* task, select the user to be the supervisor, and click the **Advanced** tab.
12. Under the **Logon supervisor of** section, click **Ad an item** (+), select the user to be supervised, and click **OK**.
13. Click **Apply**.

Related Topics

Importing security groups from an Active Directory on page 481

Logging on to Security Center through Config Tool on page 7

Forcing Security Desk to run in full screen mode

If a user's job is to focus on monitoring live video, you can force Security Desk to run in full screen mode to prevent the user from switching to Windows mode.

What you should know

You can also set Security Desk to start in full screen operation mode on a specific workstation.

To force Security Desk to run in full screen mode for a user:

1 From the Config Tool home page, open the *User management* task.

2 Select a user, and click the **Privileges** tab.

3 Expand the **Application privileges**, and the **Security Desk** privileges.

4 Deny the privilege **Change client views** to that user.

5 Click **Apply**.

Security Desk now always runs in full screen mode for that user. The *Restore Down* command and the **F11** key (switch between full screen and windowed mode) are disabled.

Setting Security Desk to start in full screen mode on workstations

If a workstation is mainly used for monitoring live video, you can set Security Desk to always start in full screen mode on that workstation.

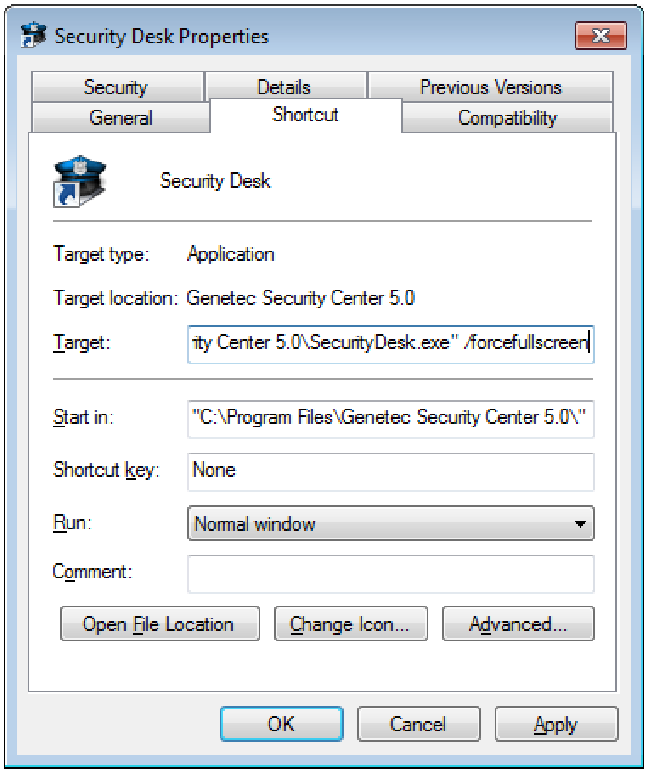
What you should know

Setting Security Desk to start in full screen mode does not prevent the user from minimizing the Security Desk window with Alt+ESC or to switch to another application with Alt+Tab.

To set Security Desk to start in full screen mode on a workstation:

1 On the workstation, open the **Security Desk Properties** dialog box.

2 Select the **Shortcut** tab, and add the option /forcefullscreen (or /ff) to the end of the string found in **Target**.



Security Desk Properties

Security Desk

Target type: Application

Target location: Genetec Security Center 5.0

Target: ity Center 5.0\SecurityDesk.exe" /forcefullscreen

Start in: "C:\Program Files\Genetec Security Center 5.0\"

Shortcut key: None

Run: Normal window

Comment:

3 Click **Apply**.

The next time a user starts Security Desk using this shortcut, the application starts in full screen mode. The *Restore Down* commands and the F11 key (switch between full screen and windowed mode) are disabled.

Selecting which workstations users can remotely control

You can select which Security Desk workstations and monitors a user is allowed to remotely control using a CCTV keyboard, or using the *Remote* task in Security Desk.

What you should know

Every monitor controlled by Security Desk is assigned a unique *monitor ID* (displayed in the notification tray, and found in the *General settings - Logical ID* page in the *System* task). Using a CCTV keyboard, you can display an entity on a remote Security Desk workstation by specifying its monitor ID, *tile ID*, and the *logical ID* of the entity.

IMPORTANT: In addition to having the *remote control rights* over Security Desk workstations and users, the following conditions must also be met for a local user to be able to connect to a remote Security Desk workstation:

- Both local and remote Security Desk must be running and connected to the same Security Center Directory.
- The local user must have the same or more user privileges than the user who is logged on to the remote Security Desk.
- The local user must be a member of all the partitions that the user who is logged on to the remote Security Desk is a member of.

To select which workstations a user can remotely control:

1. From the Config Tool home page, open the *User management* task.
2. Select the user to configure, and click the **Advanced** tab.
3. Under the **Allow remote control over** section, click **Add an item** (➕).
4. From the drop-down list, select one of the following entity types:
   - **User:** Any Security Desk workstation where that user is logged on can be remotely controlled.
   - **User group:** Any Security Desk workstation where a member of that user group is logged on can be remotely controlled.
   - **Application:** The specified workstation (*COMPUTER - SecurityDesk*) can be remotely controlled, regardless of who is logged on.
5. Select the associated entities, and click **OK** > **Apply**.

Granting extra access rights and privileges to specific workstation users

You can grant extra access rights and privileges to selected users when they log on to Security Center through specific Security Desk workstations.

Before you begin

Before you can configure a workstation with access rights and privileges, you must connect Security Desk to the Directory at least once from that workstation. You can do so with any user account. This creates a *workstation* entity (🖥) in the system that you can later configure.

What you should know

- You configure the access rights and privileges of a workstation with the *Workstation management* task.
- The *Workstation management* task is only available to Security Center administrators.
- A workstation affects the access rights and privileges of a user the same way that a parent user group does.
- A workstation affects the access rights and privileges of a user only if the user is connected through Security Desk and is part of the workstation's user list.

To configure a workstation to add extra access rights and privileges to its users:

1 (First use only) Enable the *Workstation management* feature.

  a) From the Config Tool home page, open the *System* task.

  b) Click **General settings** > **Features** and select **Workstation management**.

  c) Click **Apply**.

  d) Restart Config Tool.

  The *Workstation management* task is now available in the Config Tool home page.

2 From the Config Tool home page, open the *Workstation management* task.

3 Click **Workstation** (➕).

  The workstation creation wizard opens.

4 In the *Workstation information* page, select the workstation you want to configure.

  Only Security Desk workstations that are not yet configured are listed.

5 Click **Next** > **Create** > **Close**.

  The selected workstation (🖥) is added to the list of configured workstations.

6 (Optional) Click the **Identity** tab and give the workstation a more meaningful name.

  By default, the workstation is given the computer's name.

7 Click the **Access rights** tab, select the partitions that you want the user of this workstation to inherit, and then click **Apply**.

  NOTE: A user can inherit more access rights from the workstation, but what they already have cannot be removed. If the existing partitions do not provide the exact access rights you want to grant to the user, create a partition for what you need.

8 Click the **Privileges** tab, configure the privileges that you want to add or deny from the users of this workstation, and then click **Apply**.

  NOTE: You can only add a privilege to a user if that privilege is undefined for that user, but you can always deny a privilege that a user currently has.

9 Click the **User access** tab, and add the users and user groups you want this workstation to affect.

Now, whenever a user from the workstation's user list uses Security Desk to connect to the Directory through this workstation, the access rights and privileges configured for this workstation will be combined to the access rights and privileges of that user.

NOTE: You must recreate the workstation entity if you change the physical machine, even if you keep the same domain name.

Related Topics

Creating partitions on page 424

About privileges on page 438

Selecting which user activities to log

You can select which types of user-related activity are logged in the database, and available for reporting in the *Activity trails* task.

Before you begin

The data for Activity logging is saved to the Directory database. If you are using the Express edition of SQL Server, which has a storage limit, make sure that it has enough available space. Enable Disk space and Database usage notifications for the Directory in Server Admin to warn you when space on the database is running low. We recommend that you configure the **Database usage** value to 90% or less, to give you enough time to take action.

What you should know

The activities you can log are events that are generated by users who connected to Security Center.

To select which user activities to monitor:

1. From the Config Tool homepage, open the *System* task.
2. Click the **General settings** view, and then go to the *Activity trails* page.
3. From the list, select the events to monitor.

   You can select general events, or events specifically related to video, access control, or ALPR.
4. Click **Apply**.

You can now search for events in your system that were triggered by users, using the *Activity trails* task.

Related Topics

Event types on page 1410

Investigating user-related activity on your Security Center system on page 392

22

TLS and Directory authentication

This section includes the following topics:

What is Transport Layer Security protocol?

Transport Layer Security (TLS) is a protocol that provides communications privacy and data integrity between two applications communicating over a network. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

What you should know

TLS is used for connections to the Directory from client workstations and expansion servers. With TLS, you have the option to enforce Directory authentication on client workstations and servers during software installation.

What are the benefits of TLS?

TLS provides numerous benefits to clients and servers over other methods of authentication, including:

- **Strong authentication:** Authenticate the Directory to client applications, proving the identity of the server before connecting to it. Protects against *man-in-the-middle* attacks.
- **Data integrity:** All data are transmitted with an integrity check value.
- **Message privacy:** Protects against eavesdropping.

  NOTE: The potential of such threats is present only if you allow connections from the WAN (as opposed to through a secure VPN) or when your corporate network has been physically compromised.
- **Algorithm flexibility:** Provides options for the authentication mechanisms, encryption algorithms, and hashing algorithms that are used during the secure session.
- **Ease of use:** Most of its operations are completely invisible to the client. This allows the client to have little or no knowledge of the security of communications and still be protected from attackers.

Limitations

- Man-in-the-middle protection is only enforced if you choose to turn on Directory authentication on each machine (Client or Server).
- Client certificate are not supported for Config Tool and Security Desk.

Related Topics

Server - Properties tab on page 1291

What is Directory authentication?

Directory authentication is a Security Center option that forces all client and server applications on a given machine to validate the identity certificate of the Directory before connecting to it. This measure prevents man-in-the-middle attacks.

When do I need Directory authentication?

The purpose of Directory authentication is to protect against *man-in-the-middle* attacks. If you do not have applications connecting to your system over the Internet (or any untrusted network), the potential for this sort of attacks is very low. In that case, you are probably safe not to enable this option.

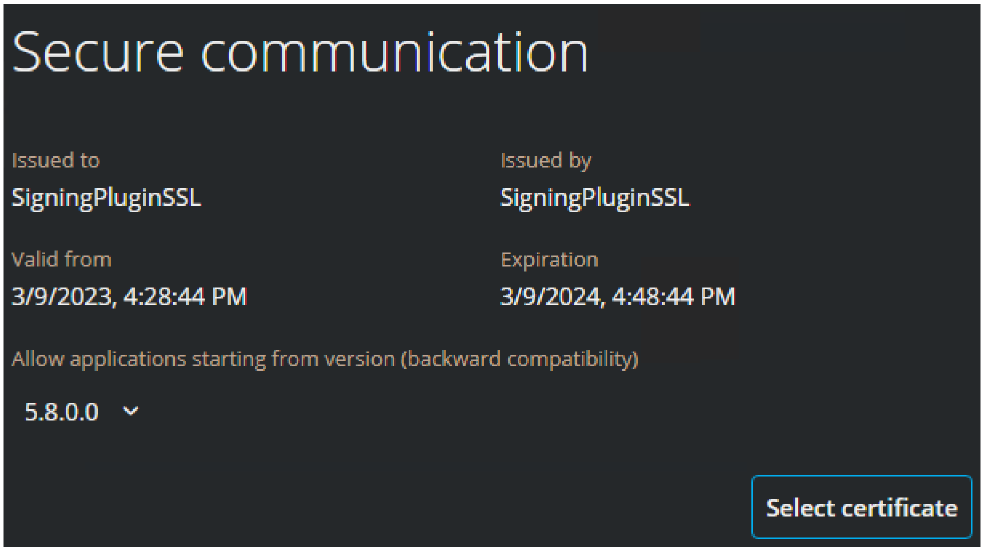
What is an identity certificate?

An identity certificate is a *digital certificate* used to authenticate one party to another in a secure communication over a public network. Identity certificates are generally issued by an authority that is trusted by both parties, called a *certificate authority (CA)*.

NOTE: All identity certificates used in Security Center are *server certificates*. A server certificate is an *identity certificate* used to authenticate the server's identity to the client. Server certificates are also used to encrypt data-in-transit to ensure data confidentiality. In the context of communication security, the party initiating the connection is the client, and the party accepting the connection is the server.

How it works

When installing the Server components of Security Center, a *self-signed certificate* named *GenetecServer-{MachineName}* is automatically created in the Local Computer Certificate Store. You can view the current certificate in Server Admin, in your server page, under the *Secure communication* section.


Secure communication

Issued to: SigningPluginSSL

Issued by: SigningPluginSSL

Valid from: 3/9/2023, 4:28:44 PM

Expiration: 3/9/2024, 4:48:44 PM

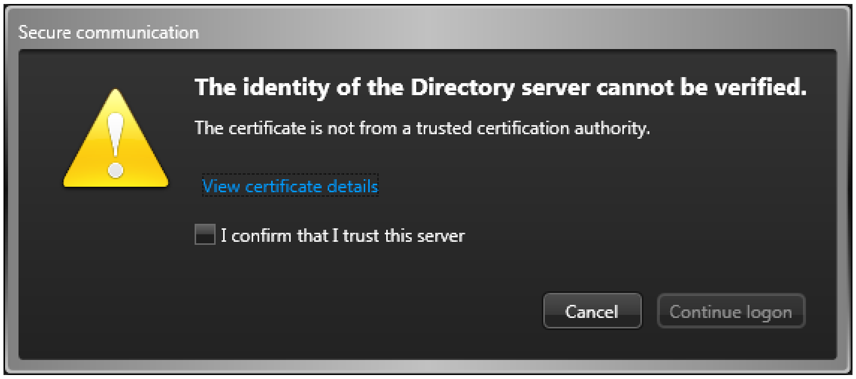
Allow applications starting from version (backward compatibility): 5.8.0.0

Self-signed certificates identify the *expansion servers* to the *main server*. As a result, the password used to connect to the main server does not need to be stored locally on the expansion servers.

Directory authentication is enabled at Security Center installation when you choose the recommended security settings, or by selecting **Always validate the Directory certificate** when you choose the custom security settings. For more information, see the *Security Center Installation and Upgrade Guide*.

BEST PRACTICE: If you choose to enable Directory authentication, we recommend that you replace the self-signed certificate on the main server with one issued by a trusted *certificate authority (CA)*. The CA can be internal or from a third party. This allows you to deploy a highly secured system without forcing your users to be aware of the underlying mechanism.

If the self-signed certificate resides on the main server, the user must confirm that the Directory server can be trusted when connecting to the Directory from a workstation for the first time.



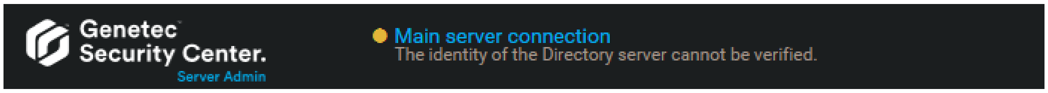
Secure communication

The identity of the Directory server cannot be verified.

The certificate is not from a trusted certification authority.

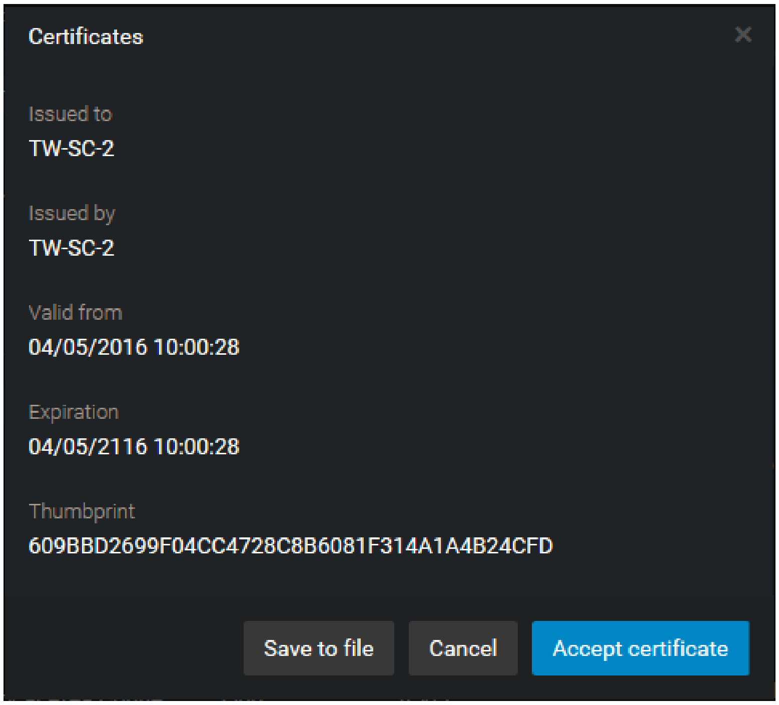
After a user confirms that the main server can be trusted, the certificate is added to an allowed list. As a result, the dialog box no longer appears.

The same confirmation is required on expansion servers. The first time you log on to the expansion server with Server Admin, this message is displayed on the dashboard.



The identity of the Directory server cannot be verified.

Click **Main server connection**, and then click **Accept certificate** in the dialog box that appears.



Certificates

Issued to
TW-SC-2

Issued by
TW-SC-2

Valid from
04/05/2016 10:00:28

Expiration
04/05/2116 10:00:28

Thumbprint
609BBD2699F04CC4728C8B6081F314A1A4B24CFD

After the main server is confirmed, you can change the password or the certificate on the main server or the expansion server. This means you no longer have to confirm your trust, as long as the two servers stay connected while you make the change.

Requirements

For Directory authentication to work, the following conditions must be met:

- DNS must be configured on the network. Servers and client workstations must be able to resolve the main server name.
- DNS must resolve the main server name to the common name on the Directory certificate.
- Client workstations and expansion servers must be able to trust the certificate provided by main server. Otherwise, a user intervention is always required to accept the certificate the first time a machine is used to connect to the main server.

How do I change this setting after installation?

To change the Directory authentication setting after software installation, you must edit the *GeneralSettings.gconfig* file on each computer where you want it changed.

Changing the Directory authentication setting

You can choose to turn Directory authentication on or off on each computer, by changing the TLS channel policy setting in their respective *GeneralSettings.gconfig* file.

What you should know

Directory authentication is enabled at Security Center installation when you choose the recommended security settings, or by selecting **Always validate the Directory certificate** when you choose the custom security settings. For more information, see the *Security Center Installation and Upgrade Guide*.

After Security Center is installed, if you want to change this setting, you must edit the *GeneralSettings.gconfig* file on each computer.

To change the Directory authentication setting after software installation:

1 Open the *GeneralSettings.gconfig* file in the configuration folder with a text editor.

The configuration folder is found under the Security Center installation folder (default = *C:\Program Files (x86)\Genetec Security Center 5.11*\ConfigurationFiles).

2 Edit the `<tlsChannel policy="value">` tag.

Change the value to `"AllowAll"` to disable Directory authentication, or to `"TrustedOnly"` to enable it.

3 Save your changes and restart the *Genetec Server* service.

Disabling backward compatibility

Security Center systems that are backward-compatible with older versions that do not support the Transport Layer Security (TLS) protocol (5.4 and earlier) are more vulnerable to network attacks.

What you should know

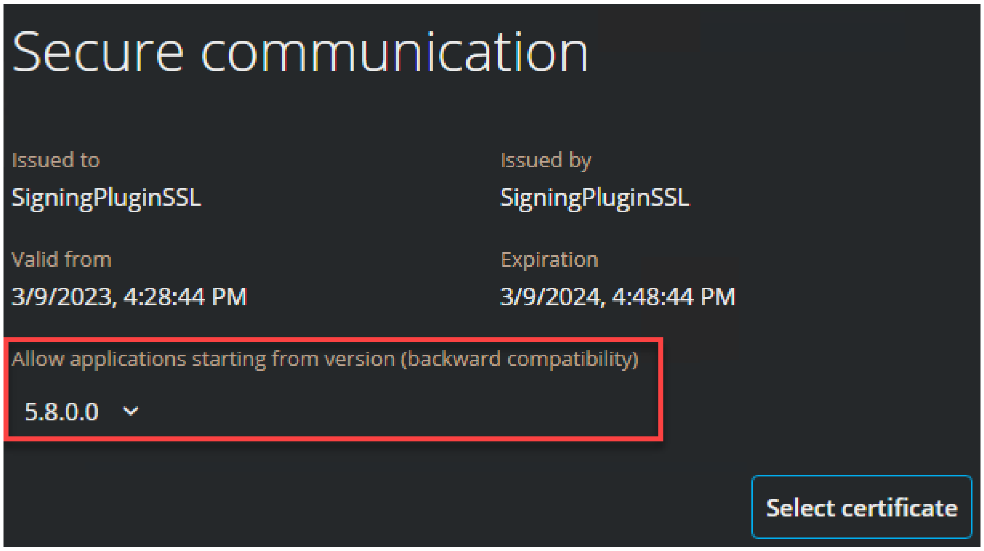
Mobile Server 4.0 does not support Transport Layer Security (TLS) protocol. If you disable backward compatibility, the Mobile apps and the Web Clients 4.0 can no longer connect to Security Center. Expansion servers that have not been upgraded to version 5.5 or later also stop working. Both Web Client 4.1 and the role-based Web Client 5.6 and later support TLS.

To disable backward compatibility:

1 Connect to the Server Admin of your main server with a web browser.

2 Click the main server (🌐) in the server list.

3 In the *Secure communication* section, select your current version of Security Center version from the **Allow applications starting from version (backward compatibility)** list.



Secure communication

Issued to: SigningPluginSSL

Issued by: SigningPluginSSL

Valid from: 3/9/2023, 4:28:44 PM

Expiration: 3/9/2024, 4:48:44 PM

Allow applications starting from version (backward compatibility): 5.8.0.0

4 Click **Save**.

IMPORTANT: The next user who tries to connect to your system with an older Security Center version receives a *Client-server versions are incompatible* error.

Enabling backward compatibility

Each new version of Security Center includes new features that might be incompatible with earlier versions. You can use backward compatibility as a temporary solution to maintain interoperability with up to three previous major versions.

What you should know

Backward compatibility is enabled by default to allow client and server applications that have not been upgraded to allow normal functioning. For enhanced security, it is recommended to disable backward compatibility after upgrading all client and server applications. Perform this procedure to re-enable backward compatibility.

IMPORTANT: Adding backward compatible connections slows down the performance of the Directory. It is only recommended as a temporary solution before you can upgrade all servers and workstations.

IMPORTANT: For client workstations, backward compatibility applies only to Security Desk. Config Tool is not backward compatible because it must be of the same version as the Directory.

To enable backward compatibility:

1. Connect to the Server Admin of your main server with a web browser.
2. Click the main server (🌐) in the server list.
3. In the *Secure communication* section, select the previous version of Security Center from the **Allow applications starting from version (backward compatibility)** list.
4. Click **Save**.

After you finish

For enhanced security, disable backward compatibility after all client applications have been upgraded.

Replacing default certificates

To replace the self-signed certificate on a server with a certificate from a trusted source, you must import the new certificate into the Local Computer Certificate Store of your server before you can select it in Server Admin.

Before you begin

Follow your company's procedure regarding the enrollment of certificates. If your situation requires you to create a custom request, make sure you follow the recommendations required for Security Center.

What you should know

To improve the security of your system, you only need to replace the *self-signed certificate* on your main server. If you have Directory failover configured, you must replace the certificate on all Directory servers. It is not necessary to change the certificate on all expansion servers.

To import a trusted certificate into the Local Computer Certificate Store of your main server:

1 On your main server, start Microsoft Management Console (mmc.exe).

2 In the *Console* window, expand **Certificates**.

3 Under **Certificates (Local Computer)**, right-click **Personal**, and then click **All Tasks** > **Import**.

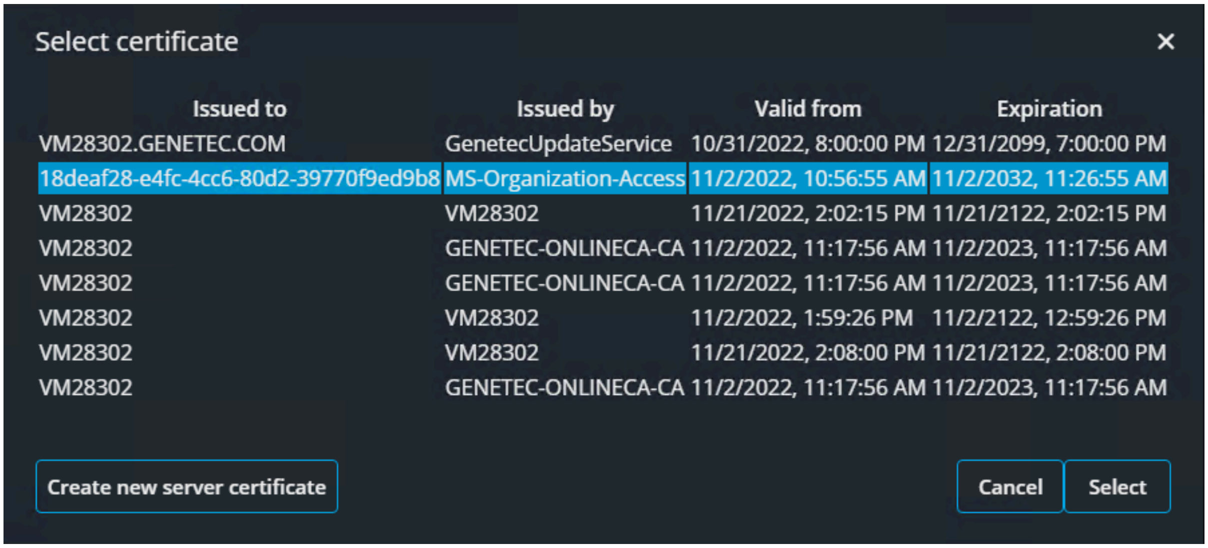
4 Follow the instructions in the *Certificate Import Wizard* to import the certificate.

5 Open Server Admin on your server.

6 Click the **Genetec Server** tab.

7 Under *Secure communication*, click **Select certificate**.

8 In the dialog box that opens, select the new certificate you imported and click **Select**.



Issued to	Issued by	Valid from	Expiration
VM28302.GENETEC.COM	GenetecUpdateService	10/31/2022, 8:00:00 PM	12/31/2099, 7:00:00 PM
18deaf28-e4fc-4cc6-80d2-39770f9ed9b8	MS-Organization-Access	11/2/2022, 10:56:55 AM	11/2/2032, 11:26:55 AM
VM28302	VM28302	11/21/2022, 2:02:15 PM	11/21/2122, 2:02:15 PM
VM28302	GENETEC-ONLINECA-CA	11/2/2022, 11:17:56 AM	11/2/2023, 11:17:56 AM
VM28302	GENETEC-ONLINECA-CA	11/2/2022, 11:17:56 AM	11/2/2023, 11:17:56 AM
VM28302	VM28302	11/2/2022, 1:59:26 PM	11/2/2122, 12:59:26 PM
VM28302	VM28302	11/21/2022, 2:08:00 PM	11/21/2122, 2:08:00 PM
VM28302	GENETEC-ONLINECA-CA	11/2/2022, 11:17:56 AM	11/2/2023, 11:17:56 AM

NOTE: If the certificate you selected is not valid (not using Legacy key for example), an error message is displayed and the certificate cannot be applied.

9 Click **Save**, and restart the Genetec™ Server service.

Creating custom certificate requests for Security Center

Custom certificate requests must be created with specific parameters in order to work with Security Center. All certificate requests must be made from the server where certificate is going to be applied.

What you should know

Creating custom certificate requests should be your last resort. There are many simpler alternatives for requesting a certificate for your server. For example, you could enroll a certificate from a certificate template of your company's Active Directory domain. For more information, see Request Certificates by Using the Certificate Request Wizard on the Microsoft Technet Library.

To create a custom certificate request for Security Center:

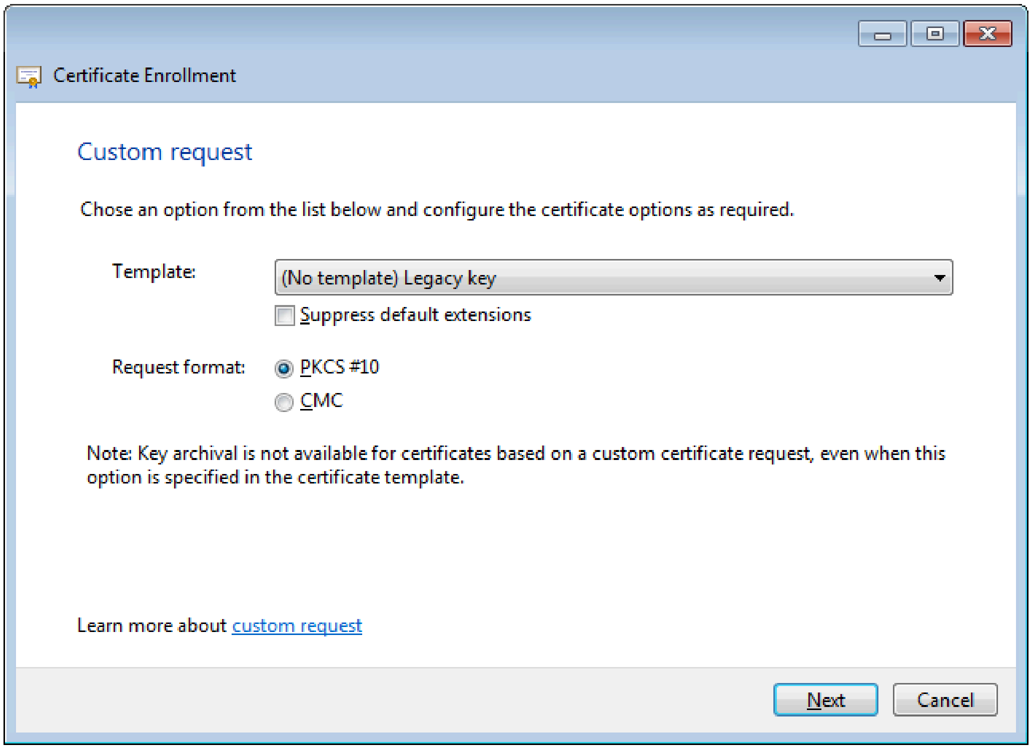
1 On your main server, start Microsoft Management Console (mmc.exe) and add the Certificates snap-in.
   a) In the *Console* window, click **File** > **Add/Remove Snap-in**.
   b) In the *Add or Remove Snap-ins* dialog box that appears, click **Certificates** and then click **Add >**.
   c) In the *Certificates snap-in* dialog box, click **Computer account** > **Next** > **Finish** > **OK**.

2 In the *Console* window, expand **Certificates**.

3 Under **Certificates (Local Computer)**, right-click **Personal**, and then click **All Tasks** > **Advanced Operations** > **Create Custom Request**.

4 In the *Certificate Enrollment* dialog box, click **Next** > **Proceed without enrollment policy** > **Next**.

5 In the *Custom request* page, select the options as shown below.



Certificate Enrollment

Custom request

Chose an option from the list below and configure the certificate options as required.

Template: (No template) Legacy key

□ Suppress default extensions

Request format: ● PKCS #10 ○ CMC

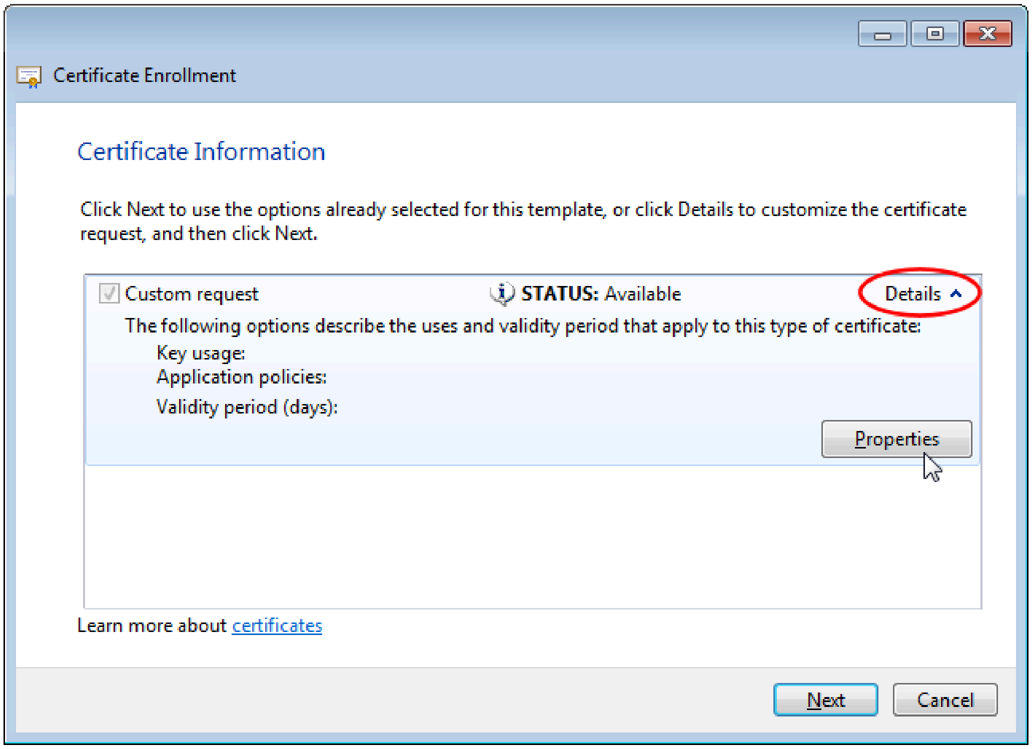
Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.

Learn more about custom request

IMPORTANT: For **Template**, select **Legacy key**. The default choice, **CNG key**, is not supported by .NET Framework 4.5, which is what Security Center uses.

6 Click **Next**

7 In the *Certificate Information* page, expand **Details**, and click **Properties**.



Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

☑ Custom request STATUS: Available Details

The following options describe the uses and validity period that apply to this type of certificate:

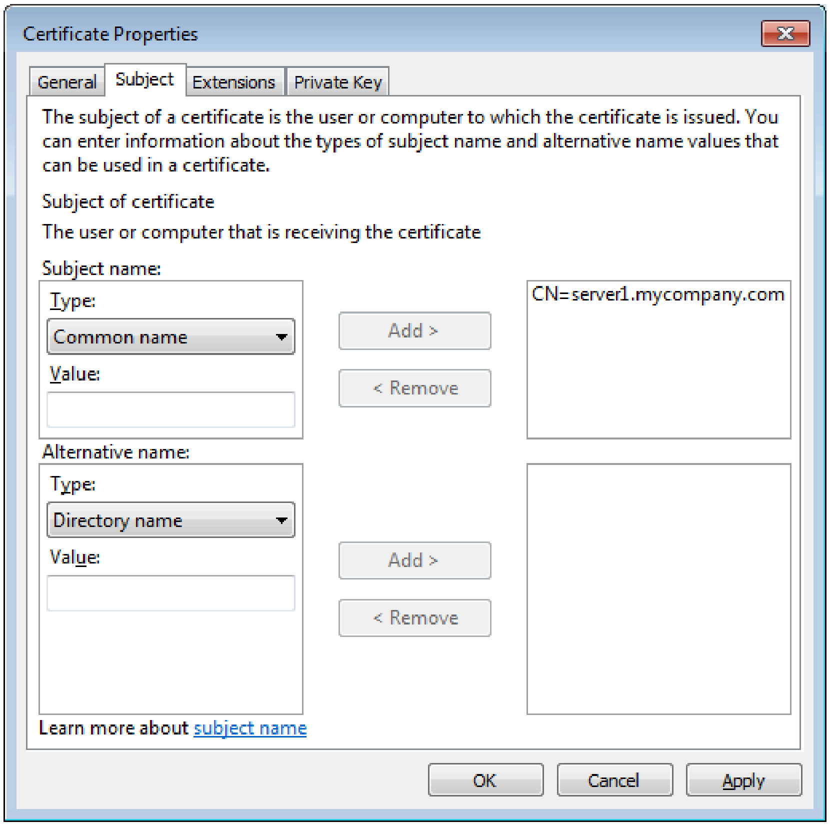
Key usage:

Application policies:

Validity period (days):

8 In the *Certificate Properties* dialog box, click the **Subject** tab, and enter the value of **Common name** under the **Subject name**.

IMPORTANT: The **Common name** must match the fully qualified domain name of the server. For example, if the hostname of your server is *server1*, and your domain is *mycompany.com*, the fully qualified domain name for your server would be *server1.mycompany.com*.



Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

Value:

CN=server1.mycompany.com

Alternative name:

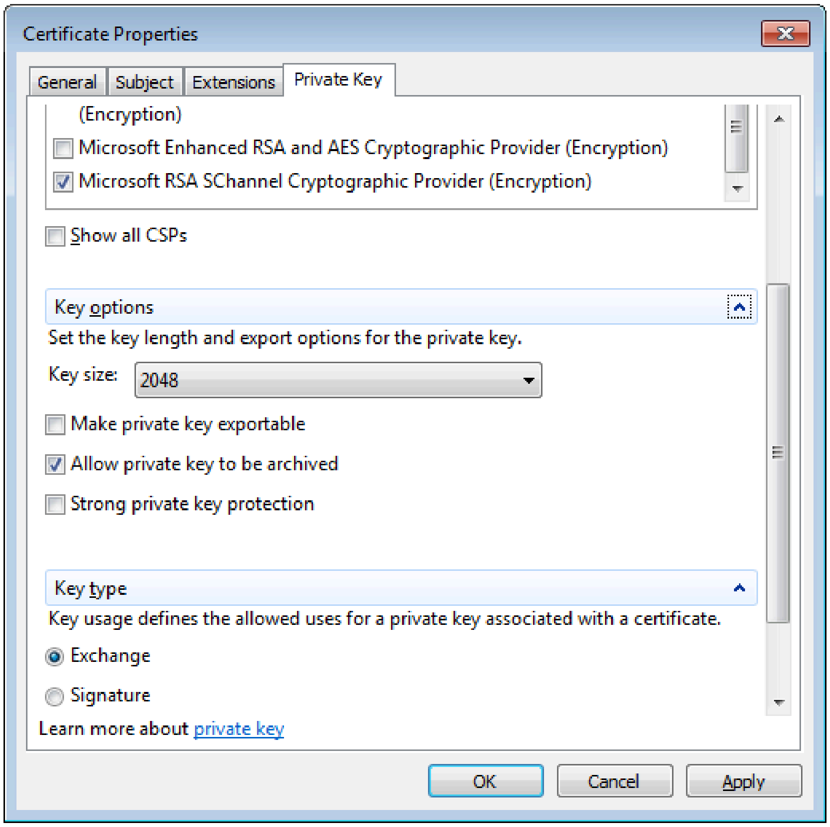
Type: Directory name

Value:

9 Click the **Extensions** tab, and set the following properties.

- **Key Usage:** Add **Digital signature** and **Key agreement**.
- **Extended Key Usage:** Add **Server Authentication** and **Client Authentication**.

10 Click the **Private Key** tab, and set the following properties.



Certificate Properties

(Encryption)

☐ Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)

☑ Microsoft RSA SChannel Cryptographic Provider (Encryption)

☐ Show all CSPs

Key options

Set the key length and export options for the private key.

Key size: 2048

☐ Make private key exportable

☑ Allow private key to be archived

☐ Strong private key protection

Key type

Key usage defines the allowed uses for a private key associated with a certificate.

● Exchange

○ Signature

Learn more about private key

- **Key Type:** Select **Exchange**. This must be set up first.
- **Cryptographic Service Provider:** Select only **Microsoft RSA SChannel Cryptographic Provider (Encryption)**. It is the last option in the list.
- **Key Options:** The **Key size** should be at least 2048.

11 Click **Apply** > **OK** > **Next**.

12 Enter the **File Name** and click **Finish**.

After you finish

Send the request (.csr) to your IT department or the external *certificate authority* for processing. Once the certificate has been generated, import and apply it to your server.

23

Active Directory integration

This section includes the following topics:

Integration with Windows Active Directory

You can manage all personnel and security information from a single location by integrating a Windows Active Directory (AD) into Security Center, whether it is for software security (IT) or for physical security (controlling access to secured areas).

Benefits of AD integration

Having a centralized security information management system provides many benefits:

- Less data entry means fewer errors and better control during initial Security Center setup, because users and cardholders can be imported from an existing AD.
- Consistency and better security because all shared information is entered only once.
  - A new user account that is added to an imported security group automatically adds a new user or cardholder in Security Center after the role is synchronized.
  - A user account that is disabled in the AD automatically disables the corresponding user or cardholder in Security Center after the role is synchronized.
- Single logon capability for synchronized Security Center users. Users logged on to Windows and imported to Security Center can enable the **Use Windows Credentials** setting to log on to Security Desk or Config Tool.

What is AD integration

In AD, you can create users, user groups, *cardholders*, *cardholder groups*, and *credentials*.

With AD integration, you can import security groups from an AD into Security Center as user groups and cardholder groups, or both. Members can be imported as users, cardholders, or cardholders with credentials. Both standard and custom attributes can be imported from the AD. Most imported fields can only be modified within the AD and are read-only in Security Center.

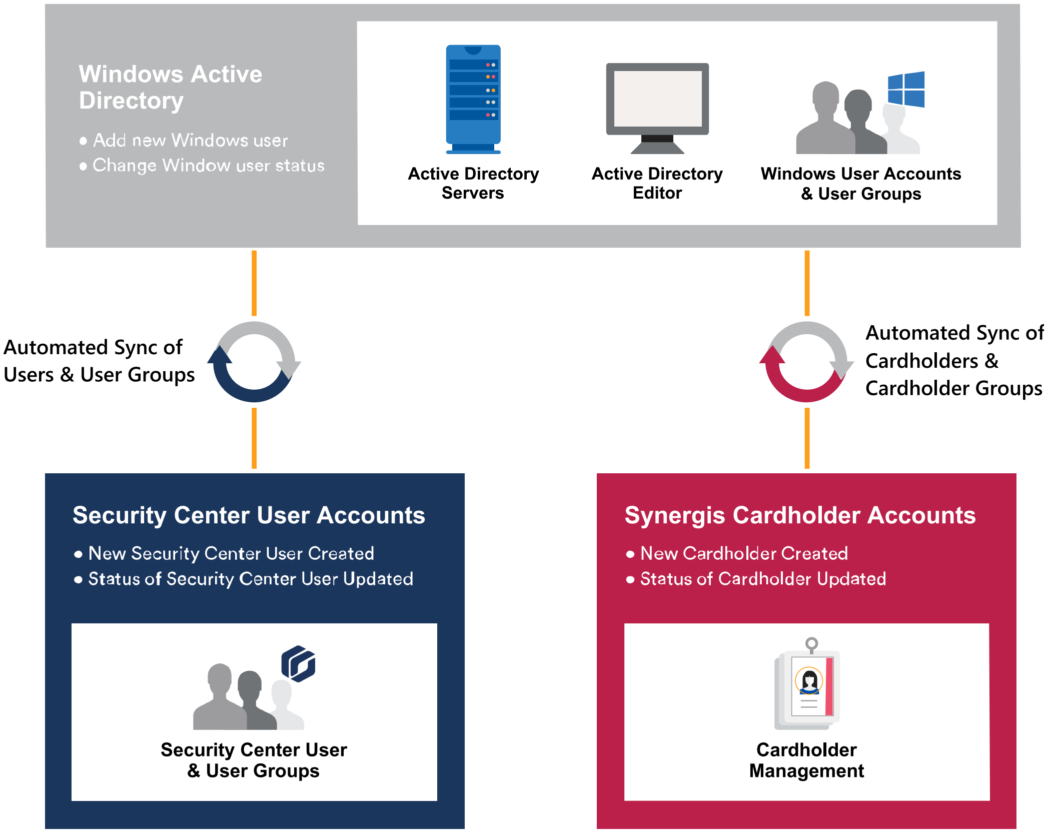
You can import entities from more than one AD if necessary. For example, from Security Center, you can manage access to a facility shared by multiple companies, such as an office building. As system administrator, you can import users and cardholders with their credentials from their individual Active Directories, and manage them in separate partitions.

For larger AD setups that have many domains that are part of an AD forest, Security Center supports synchronizing Universal groups and connecting to a global catalog. A single *Active Directory* role can be used to synchronize a universal group. For more information about using Universal groups and global catalogs with Security Center, see "About universal groups and global catalogs" in the *Security Center Administrator Guide*.

How AD integration works

To synchronize the Active Directory role, you must schedule a task. The Active Directory role then synchronizes all the changes made on the AD with the imported entities in Security Center. If Security Center users are imported from an AD, the logon credential validation is performed by the AD service. Security Center does not manage synchronized user passwords.

Imported entities are identified in Security Center by a yellow arrow (↗) superimposed on the regular entity icon.


Windows Active Directory
• Add new Windows user
• Change Window user status
Active Directory Servers
Active Directory Editor
Windows User Accounts & User Groups
Automated Sync of Users & User Groups
Automated Sync of Cardholders & Cardholder Groups
Security Center User Accounts
• New Security Center User Created
• Status of Security Center User Updated
Security Center User & User Groups
Synergis Cardholder Accounts
• New Cardholder Created
• Status of Cardholder Updated
Cardholder Management

About Active Directory synchronization

Through a process called *synchronization*, the Active Directory role also keeps all imported entities up-to-date with changes made on the Windows Active Directory (AD).

All imported entities are synchronized with their source by the *Active Directory* role.

NOTE: Make sure that the server running the Active Directory role is part of the domain that you are trying to synchronize.

Most of the attributes imported from the AD are read-only in Security Center, except for a few cardholder properties. Imported entities cannot be deleted unless they are deleted from the AD.

CAUTION: If you move a security account from a synchronized AD security group to one that is not synchronized, it is as though the account ceases to exist in Security Center. The Active Directory role deletes the corresponding entities: users, cardholders, and credentials, from Security Center the next time it synchronizes with the AD. If the deleted entities were referenced by other entities in Security Center, moving the security account back to the synchronized AD security group will not restore these relationships.

Synchronization is always initiated from Security Center. There are two ways that you can start synchronization:

- **Manually:** Synchronization is performed when you explicitly request it. This is the default setting. The advantage of this approach is that you have control over when you want the synchronization to be done.
- **On schedule:** The imported groups are synchronized using a scheduled task.

IMPORTANT: The computer requesting the synchronization and the one executing the synchronization must be configured to use the same Security Center display language. Otherwise, some types of credentials might not be synchronized and will be deleted from Security Center after the synchronization. If you are synchronizing manually, the language set on the workstation running Config Tool must be the same as the language set on the server hosting the Active Directory role. If the synchronization is performed through a scheduled task, the language set on the main server must be the same as the language set on the server hosting the Active Directory role.

Information that can be synchronized with the AD

Both standard and custom Security Center fields can be imported from the AD, and kept synchronized with the AD. You can choose which user, user group, cardholder, cardholder group, and credential fields to import from the AD in the *Links* page of the Active Directory role.

Related Topics

Scheduling a task on page 221

Default Active Directory attribute mapping

When you synchronize an AD with Security Center, certain standard AD attributes are mapped by default to the standard Security Center fields.

The following standard fields, with their *default AD attributes* shown in brackets, are imported from the AD:

Security Center field	Active Directory attribute
User groups	
Name	*sAMAccountName*

Security Center field	Active Directory attribute
Description	*description*
Email address	*mail*
All group members	*users*
Users (members of imported user groups)	
Username	*samAccountName*
Password	Not synchronized. Log on credentials are validated by the AD service
Description	*description*
First name	*givenName*
Last name	*sn*
Email address	*mail*
Status: • Active • Inactive	• *AccountExpires* • *userAccountControl*
Cardholder groups	
Name	*sAMAccountName*
Description	*description*
Email address	*mail*
All group members	*cardholders*
Cardholders (Members of the imported cardholder groups)	
Cardholder name	*samAccountName*
Description	*description*
First name	*givenName*
Last name	*sn*
Email address	*mail*
Status: • Active • Inactive	• *AccountExpires* • *userAccountControl*
Picture	Optional through the *Links* page
Partition	Optional through the *Links* page

Security Center field	Active Directory attribute
Credentials (Associations to the imported cardholders)	
Credential name	*sAMAccountName*
Card credential	• Card format (must be configured through the *Links* page) • Badge template (must be configured through the *Links* page) • Card data (must be configured through the *Links* page) • Facility code (must be configured through the *Links* page) • Card number (must be configured through the *Links* page)
PIN credential	PIN (must be configured through the *Links* page)
Plate credential	License plate (must be configured through the *Links* page)
Status: • Active • Inactive	• *AccountExpires* • *userAccountControl*
Partition	Optional through the *Links* page

If necessary, you can customize the mapping of AD attributes to cardholder and credential fields from the *Links* page of the Active Directory role. Additional attributes can also be imported from the AD by linking them to Security Center custom fields. The Active Directory role keeps all imported fields synchronized with the AD.

Limitation: When linking entity attributes from Config Tool, the entities cannot be synchronized if Config Tool is in a different language from the host running the Active Directory role.

Related Topics

Linking AD attributes to Security Center fields on page 483

About universal groups and global catalogs

Security Center supports synchronizing universal groups that belong to a global catalog. Users from different domains in an AD forest can access Security Center using one Active Directory role connected to one domain controller (global catalog). There are some things you should know before synchronizing a universal group that belongs to a global catalog.

Benefits of using a global catalog

A global catalog stores a copy of all AD objects in a forest which provides many benefits:

- The need to query multiple domains for information is eliminated since everything is stored in the global catalog.
- Less time to process information.
- Less bandwidth used.
- Less replication of information.
- Requires only a single Active Directory role connection. All users can access Security Center using the global catalog.

Requirements

Before importing a universal group that belongs to a global catalog, note the following requirements:

- There must be a trust relationship configured between all domains in the AD forest.
- Primary groups are not supported.
- In order to retrieve the directories within a forest, the Active Directory role user must be able to read the *CN=Partitions, CN=Configuration, DC=ROOTDOMAIN, DC=COM* folder.
- If you are importing a universal group that does not belong to a global catalog:
  - The Active Directory role contacts several ADs. The Active Directory role user must have the necessary permissions to access the different ADs within a forest.
  - The default port used to contact the AD is 389. If you are using a different port, you must append it to the AD server name defined in the **Active Directory** field on the *Properties* page, for example: **ADServer.Genetec.com:3393**.
- If you are importing a universal group that belongs to a global catalog:
  - All groups and subgroups belonging to a global catalog must be universal groups. Otherwise, the Active Directory role might connect to multiple domains to download the necessary information.
  - The global catalog must be updated to include the attributes required for Security Center user and cardholder information. For the list of required attributes, see Global catalog attributes on page 489.
  - The default port used to contact the AD is 3268. If you are using a different port, you must append it to the AD server name defined in the **Active Directory** field on the *Properties* page. The name and port number must be separated by a colon, for example: **ADServer.Genetec.com:3295**.

Creating an Active Directory role in Security Center

To import users and cardholders with their credentials from an AD, you must create an Active Directory role for the AD you want to import. The Active Directory role integrates your Security Center system with an AD server, and imports users, cardholders, and credentials from selected security groups.

Before you begin

If you have servers in your system that are running an earlier version of Security Center, you must upgrade the servers to the current version before using them to host a new Active Directory role.

To create an Active Directory role:

1 Open the *System* task and click the **Roles** view.

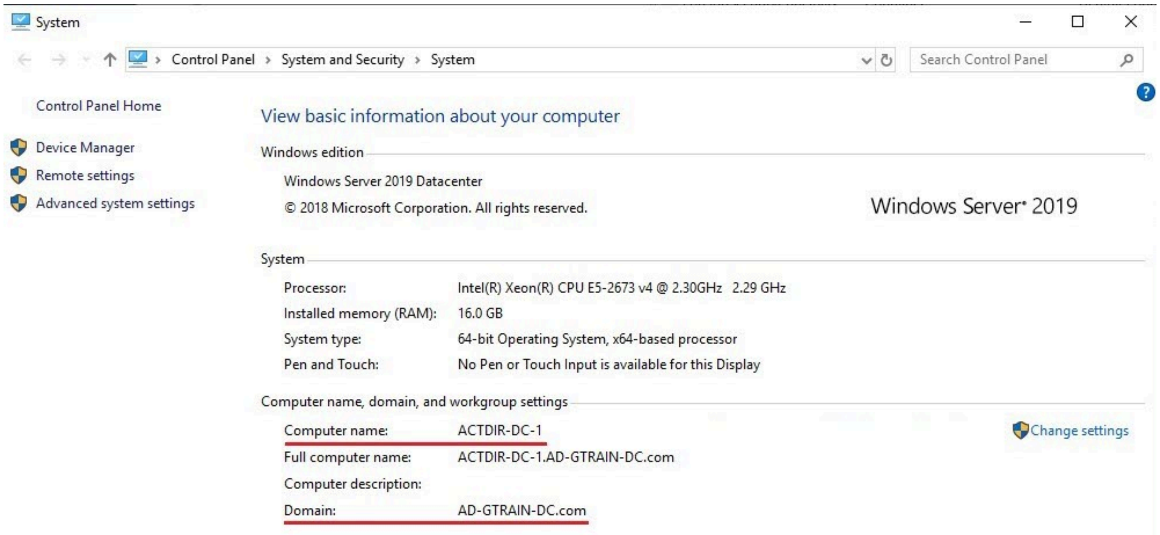
2 Click **Add an entity** (➕) and select **Active Directory**.

3 On the *Specific info* page, do the following:

a) (If you have multiple servers in your system) From the **Server** list, select the server on which you want to host the role.

b) In the **Active Directory** field, enter the AD Fully Qualified Domain Name (FQDN), hostname, or IP address of the AD server.

You must point to the domain name in the **Active Directory** field, not the computer name.



System

Control Panel › System and Security › System

Search Control Panel

Control Panel Home

Device Manager

Remote settings

Advanced system settings

View basic information about your computer

Windows edition

Windows Server 2019 Datacenter

© 2018 Microsoft Corporation. All rights reserved.

Windows Server® 2019

System

Processor:	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz 2.29 GHz
Installed memory (RAM):	16.0 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	ACTDIR-DC-1
Full computer name:	ACTDIR-DC-1.AD-GTRAIN-DC.com
Computer description:	
Domain:	AD-GTRAIN-DC.com

Change settings

If you are not using a default port, you must append the port number you are using to the AD server name, separated by a colon. For example, **ADServer.Genetec.com:123**. The default ports are as follows:

- Active Directory with no SSL: 389
- Active Directory with SSL: 636
- Global catalog no SSL: 3268
- Global catalog with SSL: 3269

c) Specify how you want the role to connect to the AD server.

You must have read access to the selected AD service.

- Use the Windows credentials assigned to the Genetec™ Server service that is running on the server hosting the Active Directory role.
- Specify a different set of Windows credentials (username, password).

4. On the *Basic information* page, enter the name, description, and partition where you want to create the Active Directory role.
5. Click**Next** > **Create** > **Close**.

   A new Active Directory role ( ) is created. Wait a few seconds for the role to connect to the AD server.
6. (Optional) If you are importing a universal group that is connected to a global catalog, turn on the **Use global catalog** option.
7. (Optional) If you have multiple servers, use the **Connect to specific domain controller** option to choose the specific server from which you want to import your schema architecture.

After you finish

Importing security groups from an Active Directory on page 481

Importing security groups from an Active Directory

To have a centralized personnel management system, you can import AD security groups into Security Center as user groups or cardholder groups.

Before you begin

- If you are importing a universal group from a global catalog, read About universal groups and global catalogs on page 478.
- When importing an AD security group, you must import all members of that group, including the subgroups. If you want to import only a subset of its members, for example, only Security Center users, you must define a new AD security group with only the members you want to import. .For more information on creating security groups in Active Directory, see the *Active Directory Integration Guide*.
- Ensure that the workstation where Config Tool is running is using the same Security Center display language as the server that is going to host the Active Directory role.

What you should know

- If you are integrating multiple ADs into Security Center, they must each belong to a different domain.
- An AD security group can be imported as a *user group*, a *cardholder group*, or both.

To import a security group:

1 On the *Properties* page of the Active Directory role, select the AD security groups you want to import.

a) Click **Add an item** (➕).

b) Select the security groups you want to add to your Active Directory role.

Use one of the following methods:

- (Recommended) Type the name of the group in **Find Active Directory groups,** and click 🔍.

  If the text you entered matches a single group, it is automatically added to the **Selected groups** list.

  If the text you entered matches multiple group names, a second dialog box opens, listing all the group names that match the text you entered.

  Select the ones you want, and click **OK** to add them to the **Selected groups** list.
- From the **Selected groups** list, click (➕).

  The *Active Directory members* dialog box opens.

  Select a security group, and click **OK**. Only security groups can be synchronized. If you selected an item that is not a security group, the **OK** button remains disabled.

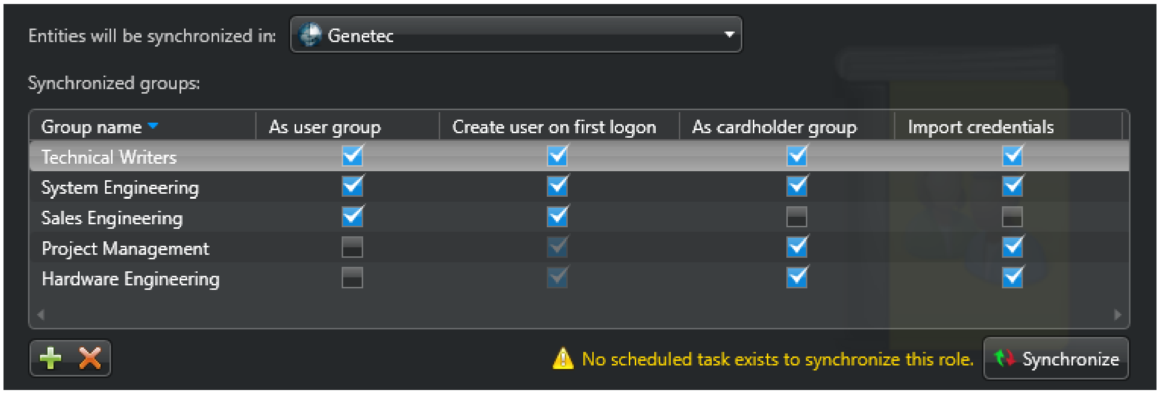
NOTE: The names shown in the dialog box are display names. Security Center only synchronizes the account names because they are guaranteed to be unique. Typically, the display names and the account names are the same. The only way to tell them apart is that the display names contain spaces.

c) Repeat the previous step as often as needed until all security groups you want to synchronize with the AD are listed in **Selected groups**, and then click **OK**.

The selected groups are listed under **Synchronized groups** in the *Properties* page.

2 Choose which partition the entities are synchronized in.

3 For each of the synchronized groups, specify how you want to import them.



Entities will be synchronized in: Genetec

Synchronized groups:

Group name	As user group	Create user on first logon	As cardholder group	Import credentials
Technical Writers	☑	☑	☑	☑
System Engineering	☑	☑	☑	☑
Sales Engineering	☑	☑	□	□
Project Management	□	☑	☑	☑
Hardware Engineering	□	☑	☑	☑

⚠ No scheduled task exists to synchronize this role.

The following options are available:

- **As user group:** Select this option to import the synchronized group as user group, and the group members as users.
- **Create user on first logon:** This is the default option, and it creates an empty user group. User entities are only created when someone tries to logs on the first time. This option avoids having to create all user entities simultaneously, which can freeze up the system. If you clear this option, all user entities are created at the same time as a user group.
- **As cardholder group:** Select this option to import the synchronized group as cardholder group, and the group members as cardholders. All synchronized cardholders are created simultaneously.
- **Import credentials:** Select this option to import the credential information of the synchronized cardholders. Multiple credentials can be imported for each cardholder.

4 If necessary, customize the mapping of AD attributes to Security Center fields.

5 If you are importing credentials, select which credential fields to synchronize with the AD.

6 Click **Apply**, and then click **Synchronize now** (⇅).

All synchronized groups and their members are imported as Security Center entities according to your specifications, with a yellow arrow (↗) superimposed on their icon.

After you finish

Some additional configuration might be required, depending on what you synchronized with the AD:

- If you already had entities configured in your system, you might need to resolve certain conflicts due to the import.
- (Optional) Configure the imported user groups with proper privileges and security options, so that when new user entities are created, they can automatically inherit these properties from their parent user group.
- (Optional) Configure the imported cardholders and cardholder groups.
- (Optional) Create a scheduled task to synchronize imported entities with the AD on a regular basis.

After you create a scheduled task, the warning message **No scheduled task exists to synchronize this role** disappears from the **Properties** tab.

Related Topics

Integration with Windows Active Directory on page 473

About Active Directory synchronization on page 475

Custom card formats on page 882

About federated entities on page 270

Linking AD attributes to Security Center fields

You can change or add to the AD attributes mapped by default to Security Center fields from the *Links* page of the Active Directory role.

Before you begin

- Familiarize yourself with the default AD attribute mapping.
- Ensure that the workstation where Config Tool is running is on the same network domain as the AD server.
- (Optional) Define the custom fields that will receive data from the AD.

What you should know

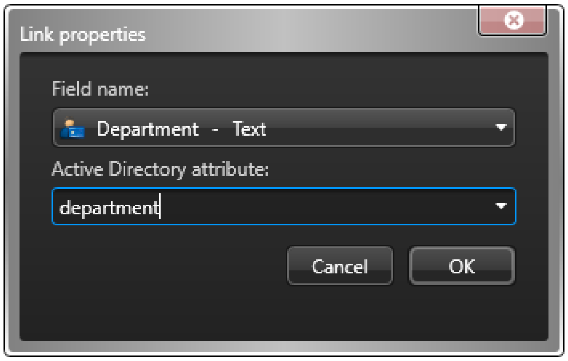
- You can import additional AD attributes to any synchronized entity type by mapping them to custom fields.
- You can only override the default mapping of *Cardholder* and *Credential* fields.
- No more than 32 custom fields can be mapped to the AD.

To customize the mapping of Security Center fields to synchronize with Active Directory:

1 From the *Links* page of the Active Directory role, under the section corresponding to the entity type you want to import, click **Add an item** (+).

The Links page is divided into three sections, *Users*, *Cardholders*, and *Credentials*.

2 In the *Link properties* dialog box, select the **Field name** and the **Active Directory attribute** you want to synchronize, and then click **OK**.



Link properties

Field name: Department - Text

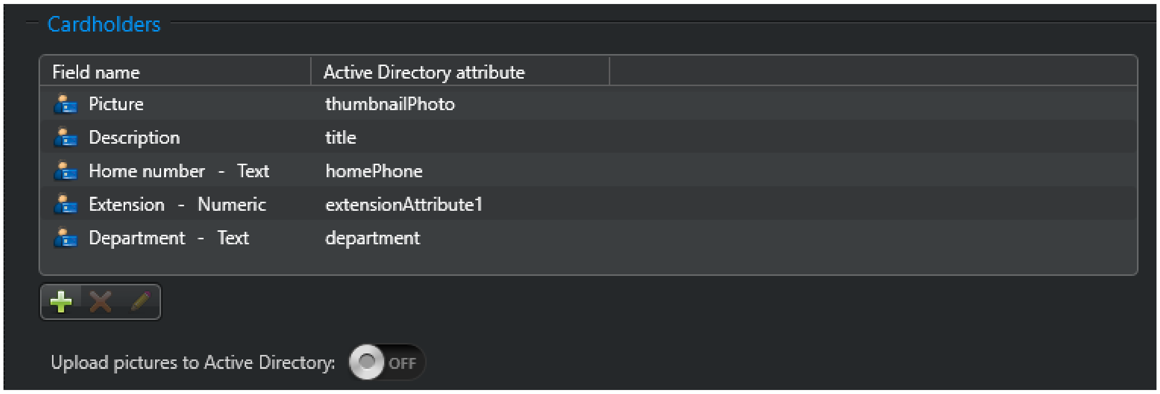
Active Directory attribute: department

Only fields corresponding to the selected entity type, both standard and custom, are listed. If you know the name of the AD attribute you want to map, you can enter it directly.

IMPORTANT: The data type of the Security Center field must match that of the AD attribute: text with text, decimal with decimal, date with date, etc. The Security Center image data type must be mapped to the AD binary data type, and the mapped AD attribute must contain a valid JPEG image.

The mapped custom fields are displayed in the *Links* page.

3 Repeat the previous steps as needed.



Cardholders

Field name	Active Directory attribute
Picture	thumbnailPhoto
Description	title
Home number - Text	homePhone
Extension - Numeric	extensionAttribute1
Department - Text	department

Upload pictures to Active Directory: OFF

4 If you are synchronizing cardholders and want to upload cardholder pictures from Security Center to the AD, set **Upload pictures to Active Directory** to **ON**.

NOTE: The cardholder picture field can be mapped to any AD binary attribute if you just want to import them from the AD. But if you want to upload the cardholder pictures from Security Center to the AD, then you must map it to the AD attribute *thumbnailPhoto*. For more information, see "Assigning picture to imported cardholders" in the *Security Center Administrator Guide*.

5 Click **Apply**.

When you synchronize with the AD, they are read-only.

Selecting which credential fields to synchronize with Active Directory

Before you can import credentials from the Active Directory (AD), you must configure which AD attributes to link to the credential fields in Security Center in the *Links* page of the Active Directory role. The mapping can be different for each Active Directory role in your system.

Before you begin

- See "Designing badge templates" in the *Security Center Administrator Guide* to define the badge templates you want to use.
- From the Active Directory role's *Properties* page, select the options **As cardholder group** and **Import credentials** for the AD security group you want to synchronize.

What you should know

Multiple credentials can be imported for a single cardholder.

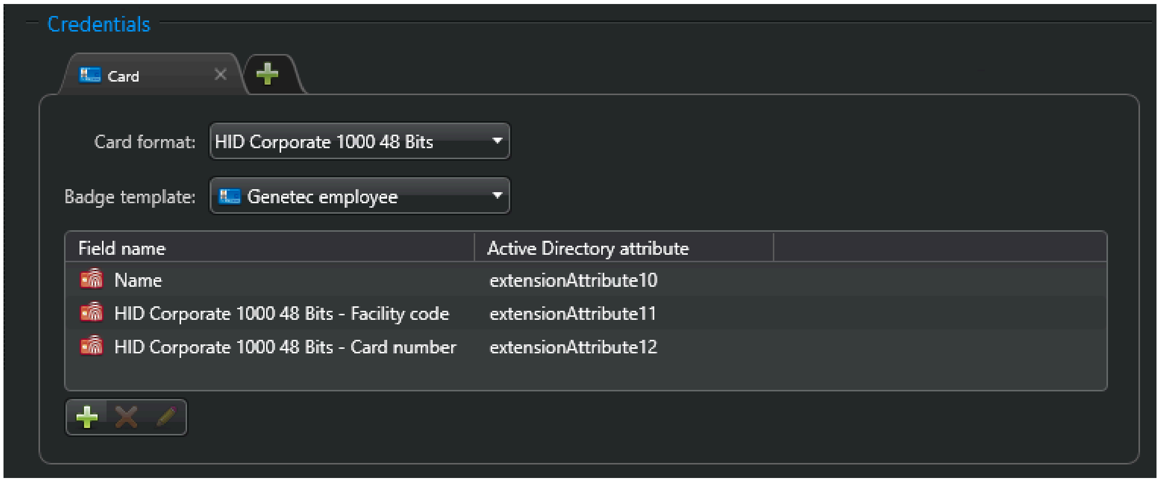
To map AD attributes to credential fields:

1 From the *Links* page of the Active Directory role, under the *Credentials* section, click **Add credential** (✚).

2 Select a credential type, enter the configuration name, and click **Add**.

3 If you selected **Card** (🪪) credential type, configure the following:

- **Card format:** Default card format to use for the imported credentials when the card format property is either not mapped to an AD attribute, or when the mapped attribute is empty.
- **Badge template:** Default badge template to use for the imported credentials when the badge template name is either not mapped to an AD attribute, or when the mapped attribute is empty.
- **Other credential fields:** Map all credential fields required by the card format. The card format can also be mapped to an AD attribute to override the default value.

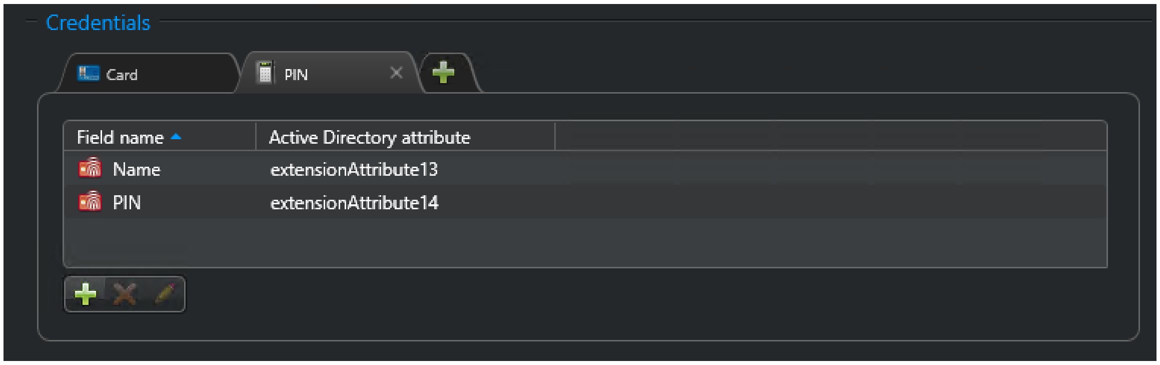


Card format: HID Corporate 1000 48 Bits

Badge template: Genetec employee

Field name	Active Directory attribute
Name	extensionAttribute10
HID Corporate 1000 48 Bits - Facility code	extensionAttribute11
HID Corporate 1000 48 Bits - Card number	extensionAttribute12

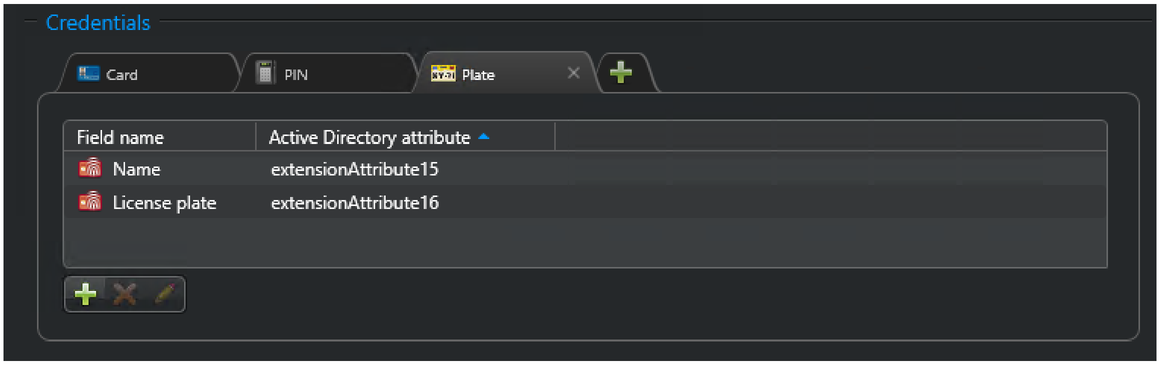
4 If you selected **PIN** (🖩) credential type, select the AD attribute to map to the *PIN* field.



Field name	Active Directory attribute
Name	extensionAttribute13
PIN	extensionAttribute14

NOTE: The *PIN* field is compulsory for PIN credentials.

5 If you selected **Plate** (🚘) credential type, select the AD attribute to map to the *License plate* field.



Field name	Active Directory attribute
Name	extensionAttribute15
License plate	extensionAttribute16

NOTE: The *License plate* field is compulsory for *Plate* credentials.

6 If necessary, map additional credential fields to AD attributes.

7 Repeat the previous steps as needed.

8 Click **Apply**.

The mapped credential fields are displayed in the *Links* page. When you synchronize with the AD, they are read-only.

Related Topics

Integration with Windows Active Directory on page 473

About Active Directory synchronization on page 475

Resolving conflicts caused by imported entities

Conflict resolution might be necessary if you have existing user or cardholder entities in your database before importing entities from the Active Directory.

What you should know

When a synchronized entity has the same name as a local entity, the Active Directory role sees it as a potential conflict. You can use the Conflict resolution tool to view potential conflicts () and resolve them by deleting the conflicting entities in the *Cardholder management* task.

To resolve conflicts caused by imported entities:

1 From the Config Tool home page, open the *System* task, and click the **Roles** view.

2 Select the Active Directory role (), and click **Conflict resolution** ().

The *Active Directory conflict resolution* dialog box opens. All synchronized entities are listed to the left. The ones that conflict with a local entity are flagged in green.

3 Resolve each cardholder conflict:

a) Open the *Cardholder management* task and find the two cardholder records that are in conflict.

b) Select one of the conflicting cardholder records and click **Modify**.

c) Add any missing information that is available in the duplicate cardholder record.

d) Save and close the cardholder record.

e) Select the duplicate cardholder record and click **Delete Cardholder**.

4 Resolve each user conflict:

a) Open the *User management* task.

b) In the entity browser, find the two user records that are in conflict.

c) Open one of the conflicting user records.

d) Add any missing information that is available in the duplicate user record.

e) Click **Apply**.

f) Select the duplicate user record and click **Delete**.

5 Return to the **Roles** view in the *System* task.

6 In the *Active Directory conflict resolution* dialog box, select the entities that are flagged as being in conflict and click **Delete**.

7 Click **Finish**.

This process will generate a file named *Conflict_Manifest.data* that documents resolved conflicts. It can be saved for future reference.

Deactivating users imported from an Active Directory

If you have users that are imported from an Active Directory, you can set their status to inactive. The users will not be synchronized with the AD until you activate them again.

To deactivate a user imported from an Active Directory:

1 From the Config Tool home page, open the *User management* task.

2 In the entity browser, select an imported user (👤), and click the **Properties** tab.

3 Set the **Status** option to **Inactive**.

4 Click **Apply**.

The user is no longer synchronized with the AD. It will only become synchronized again after you set the user’s status to **Active**.

Global catalog attributes

For the *Active Directory* role to successfully connect to a global catalog and synchronize users and cardholders in Security Center, the global catalog must be updated to include specific attributes.

IMPORTANT: Not all required attributes are enabled by default. For those that are not, you must replicate them manually in the global catalog using the Microsoft Management Console.

User attributes

The global catalog must be updated with the following user attributes:

- accountExpires (*not enabled by default*)
- cn
- description
- displayName
- distinguishedName
- givenName
- mail
- memberof (*for the SDK only*)
- name
- objectClass
- objectGUID
- objectSid
- sAMAccountName
- sn
- tokenGroup
- userAccountControl
- userPrincipalName
- any attributes to be used in the *Links* page

Group attributes

The global catalog must be updated with the following group attributes:

- cn
- description
- distinguishedName
- groupType
- mail
- member
- name
- objectClass
- objectGUID
- objectSid
- sAMAccountName

Container, domain, and organizational unit attributes

The global catalog must be updated with the following container, domain, and organizational attributes:

- displayName
- distinguishedName
- member
- name
- objectClass
- objectGUID
- objectSid

24

Third-party authentication

This section includes the following topics:

What is third-party authentication?

Third-party authentication uses a trusted, external identity provider to validate user credentials before granting access to one or more IT systems. The authentication process returns identifying information, such as a username and group membership, that is used to authorize or deny the requested access.

What is an identity provider?

An identity provider is a trusted, external system that administers user accounts, and is responsible for providing user authentication and identity information to relying applications over a distributed network.

What are the benefits of using an identity provider?

- Can impose advanced authentication requirements, like the use of smartcards or *multi-factor authentication*, to increase confidence that a user is who they say they are.
- Decouples the process of *authentication* (verifying that an entity is what it claims to be) from the process of *authorization* (establishing the rights an entity has over the features and resources of a system).

  NOTE: Security Center only uses an external identity provider for user authentication. Authorization is handled internally, using partitions and privileges.
- Allows Single Sign-On (SSO), where one user authentication grants access to multiple IT systems or even organizations.

What methods of third-party authentication does Security Center support?

Security Center supports the following third-party authentication methods:

- Active Directory integration
- ADFS using the WS-Trust protocol or WS-Federation protocol
- External identity provider using the OpenID Connect protocol
- External identity provider using the SAML 2.0 protocol

NOTE: Users authenticated by an external identity provider are only created in Security Center at first logon. Unlike with Active Directory, you cannot import external users to Security Center when the Authentication Service role connects to an identity provider.

Requirements

To use third-party authentication, the following conditions must be met:

- Security Center clients must have network access to the external identity provider.
- A TLS encryption certificate for the identity provider must be trusted by the Security Center client.

Performance impact

- The scalability of the Directory is not impacted by third-party authentication.
- User logons using third-party authentication are expected to take slightly longer than native authentication, because they require the client to connect to one or more remote identity providers before connecting to the Directory.

Related Topics

Logging on to Security Center through Config Tool on page 7

OpenID Connect Integration overview

Before users can log on to Security Center using an external identity provider with OpenID Connect (OIDC), you must follow a sequence of steps.

The following table lists the tasks required to deploy third-party authentication using OIDC:

Step	Task	Where to find more information
Understand prerequisites and key issues before integrating		
1	Learn about the different components and how they connect.	• OpenID Connect and SAML2.0 integration
2	Ensure all Security Center clients trust the connection to your identity provider. To establish trust, a trusted Certificate Authority must sign the public key certificate for the identity provider on the computer or mobile device connecting to Security Center.	
3	Verify that your Security Center license includes OpenID Connect integrations. Go to the Config Tool homepage, click **About** > **Security Center**, and confirm that Number of OpenID Connect integrations is one or more.	• License options in Security Center on page 1447
Prepare Security Center		

Step	Task	Where to find more information
4	Add an Authentication Service role for OpenID and click the **Network endpoint** tab. You might need to restart the *System* task to see the endpoints. The *redirect* and *logout* endpoints are required to configure your identity provider. There are different URIs for each client type: • ***/genetec:*** Config Tool, Security Desk, and SDK • ***/<Mobile>*****OpenId:** Genetec™ Mobile • ***/<SecurityCenter>*****OpenId:** Web Client **NOTE:** *Mobile* and *SecurityCenter* are the default web addresses for the Mobile Server role and the Web Server role. Any modification to these web addresses will be reflected in the corresponding URIs. To work with role failover, separate *redirect* and *logout* URIs are needed for each server that can host the Directory, Mobile Server, and Web Server roles. Ensure that role failover is properly configured to see all the required endpoints. If any servers are added or retired after setting up the identity provider, you might need to update the configuration by adding or removing URIs. All clients must be able to resolve the endpoint URI for their type. If a public address is being used, that address must resolve to the correct server for clients connecting from your private network.	• Setting up Directory failover and load balancing on page 168 • Setting up role failover on page 164
Integrate the external identity provider		
5	Following the instructions from your identity provider, add Security Center as a relying application in that system. For successful authentication, Security Center requires the identity provider to return *claims* about the authenticated party in an access token (JWT format) or the UserInfo endpoint. At a minimum, those claims must include a username claim, and a group membership claim.	

Step	Task	Where to find more information
6	Add authorized user groups from your identity provider to Security Center and set privileges. If your identity provider can export a list of groups in CSV format, you can important that list to Security Center. Typically, identity providers use names to uniquely identify user groups. When names are used, Security Center user groups must have the same name as the corresponding group from your identity provider, and include the domain name. For example: `Operators@YourCompany.com`. If your identity provider uses an ID to uniquely identify a user group, you must perform another step before linking the group to the Authentication Service role. Add the ID to the **External unique identifier** property for the corresponding user group in Security Center. Users are automatically created and added to their assigned group, or groups when they log on for the first time.	• Creating user groups on page 429 • About privileges on page 438 • Importing user groups from a CSV file for third-party authentication on page 527
7	Configure the Authentication Service role with information about your identity provider. Open the Authentication Service role for OpenID, click the **Properties** tab, and input the required fields.	• Authentication Service - Properties tab (OpenID) on page 1348

How to integrate Security Center with Azure Active Directory using OpenID Connect

Before Security Center can use Azure Active Directory to authenticate users with OpenID Connect, setup is required in Config Tool and the Azure Portal.

This example shows the steps required to set up third-party authentication with Azure Active Directory (Azure AD) using OpenID Connect (OIDC) access tokens. The procedure is divided into the following sections:

1. Preparing Security Center
2. Preparing Azure AD
3. Integrating Security Center with Azure AD

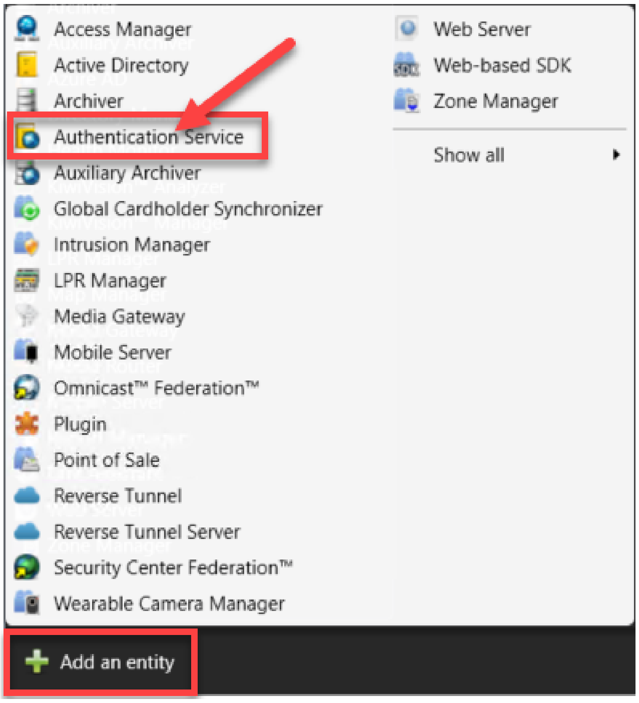
To implement third-party authentication, you must have administrator rights in Security Center and Azure AD.

IMPORTANT: This sample integration might differ from your requirements and the Azure Portal is subject to change. When setting up Azure AD, ensure that all steps are adapted to your specific situation.

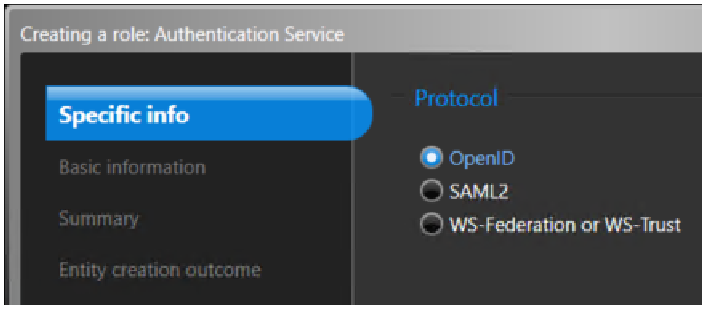
1 - Preparing Security Center

1. Open Config Tool and connect to the Security Center *main server* as an administrator.

2. In Config Tool, open **System** > **Roles** and click **Add an entity** > **Authentication Service**.



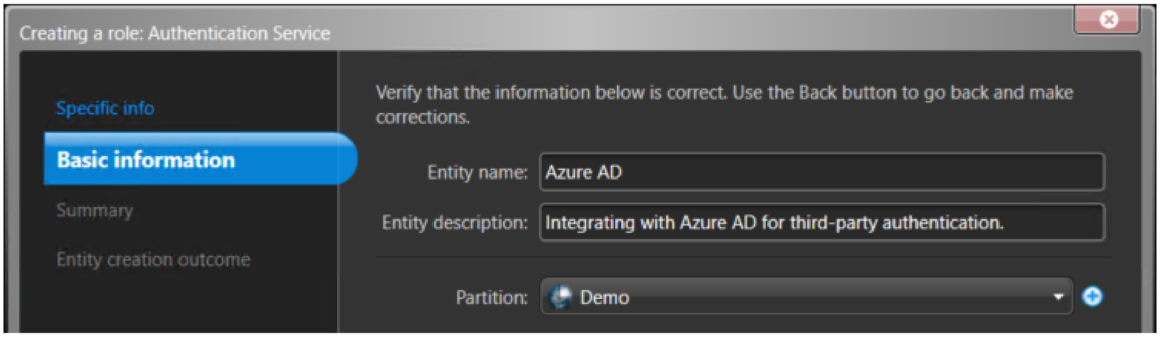
3. In the *Creating a role: Authentication Service* window, select **OpenID** and click **Next**.



Protocol

● OpenID
○ SAML2
○ WS-Federation or WS-Trust

4. Enter a name and optional description for the new Authentication Service role and click **Next**.



Verify that the information below is correct. Use the Back button to go back and make corrections.

Entity name: Azure AD

Entity description: Integrating with Azure AD for third-party authentication.

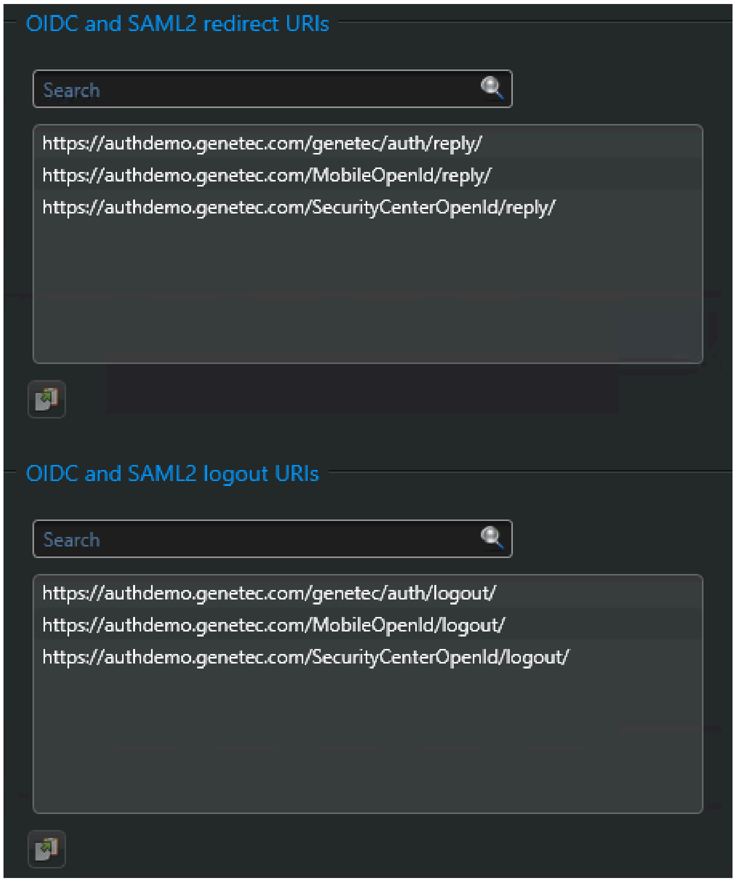
Partition: Demo

NOTE: If your system has multiple partitions, you can also add the new role to a specific partition here.

5. On the *Summary* page, ensure all the information is correct, click **Create**, and click **Close**.
6. In the newly created role, click the **Network endpoint** tab.

7. On the *Network endpoint* page, copy the OIDC *redirect* and *logout* URIs. These are needed to configure Azure AD.

   NOTE: You might need to restart the *System* task to see the endpoint URIs.



OIDC and SAML2 redirect URIs

Search

https://authdemo.genetec.com/genetec/auth/reply/
https://authdemo.genetec.com/MobileOpenId/reply/
https://authdemo.genetec.com/SecurityCenterOpenId/reply/

OIDC and SAML2 logout URIs

Search

https://authdemo.genetec.com/genetec/auth/logout/
https://authdemo.genetec.com/MobileOpenId/logout/
https://authdemo.genetec.com/SecurityCenterOpenId/logout/

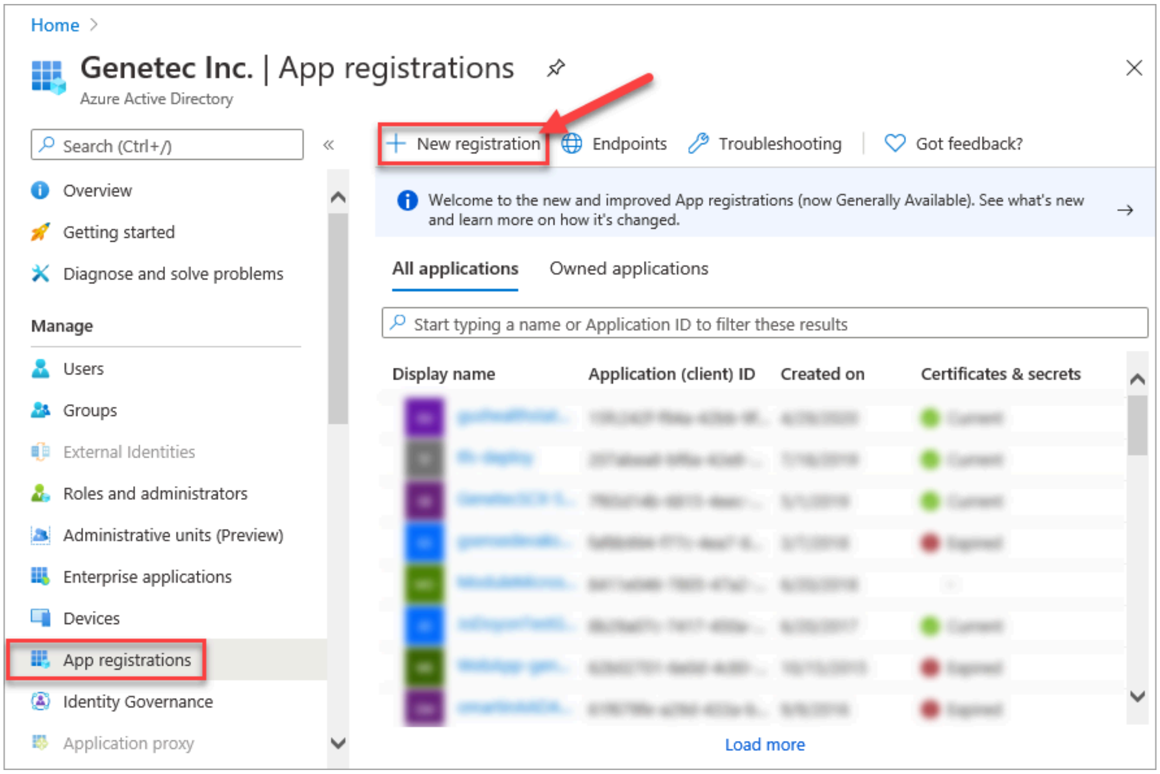
2 - Preparing Azure AD

Before completing these steps in the Azure Portal, you must meet all of the following prerequisites:

- Have an Azure AD that represents your domain.
- Have provisioned at least one user.
- Have provisioned at least one user group that contains the users you want to grant access to Security Center.

1. In the Azure Portal, open the Azure Active Directory for your tenant.

2. In the left menu, select **App registrations**, and click **New registration**.



Home >

Genetec Inc. | App registrations

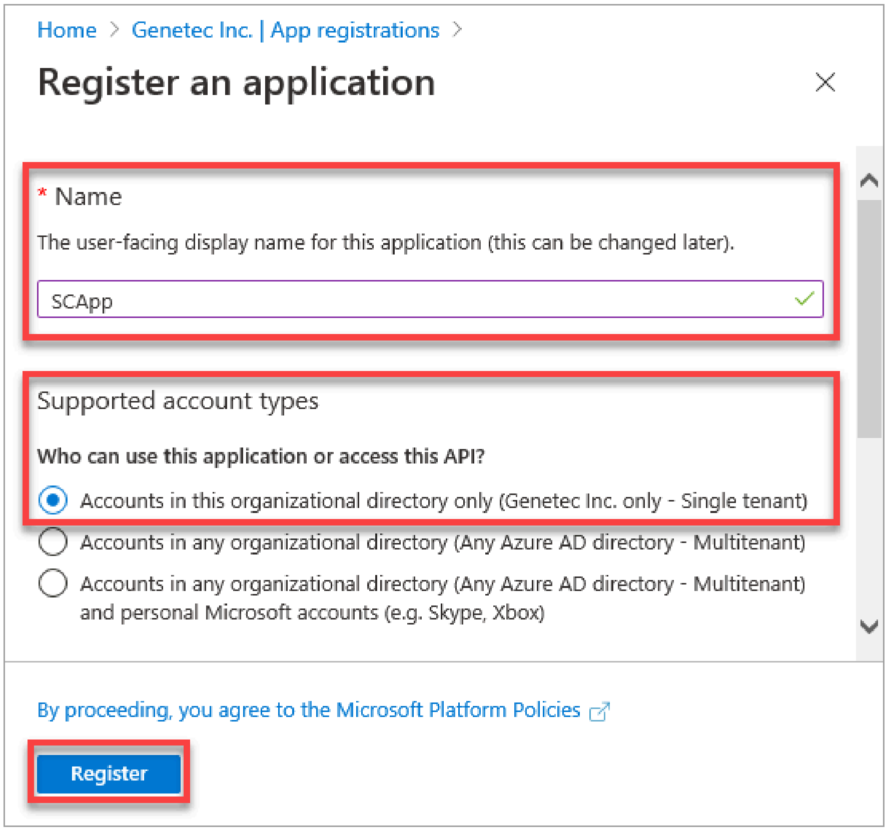
Azure Active Directory

Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed.

All applications
Owned applications
Start typing a name or Application ID to filter these results

Display name	Application (client) ID	Created on	Certificates & secrets
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

3. Enter a **Name**, select **Single tenant** under *Supported account types*, and click **Register**.



Home > Genetec Inc. | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

SCApp ✓

Supported account types

Who can use this application or access this API?

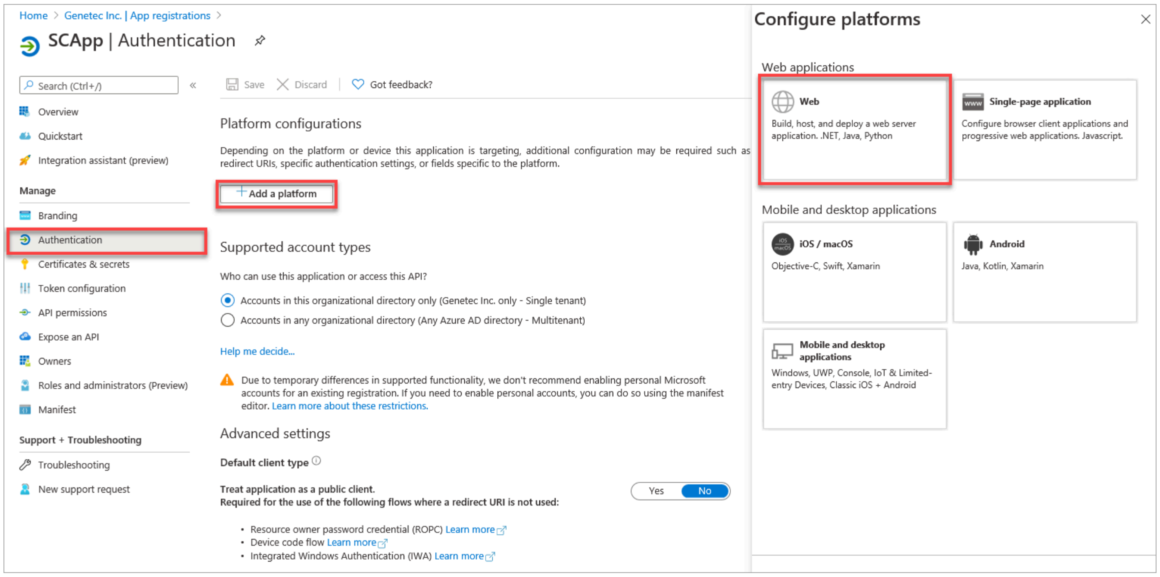
● Accounts in this organizational directory only (Genetec Inc. only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

By proceeding, you agree to the Microsoft Platform Policies

4. In the left menu for your application, select **Authentication**, click **Add a platform**, and select **Web**.



Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Genetec Inc. only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

Advanced settings

Default client type

Treat application as a public client.
Required for the use of the following flows where a redirect URI is not used: Yes [✓ No]

- Resource owner password credential (ROPC) Learn more
- Device code flow Learn more
- Integrated Windows Authentication (IWA) Learn more

Configure platforms

Web applications

Web
Build, host, and deploy a web server application. .NET, Java, Python

Single-page application
Configure browser client applications and progressive web applications. Javascript.

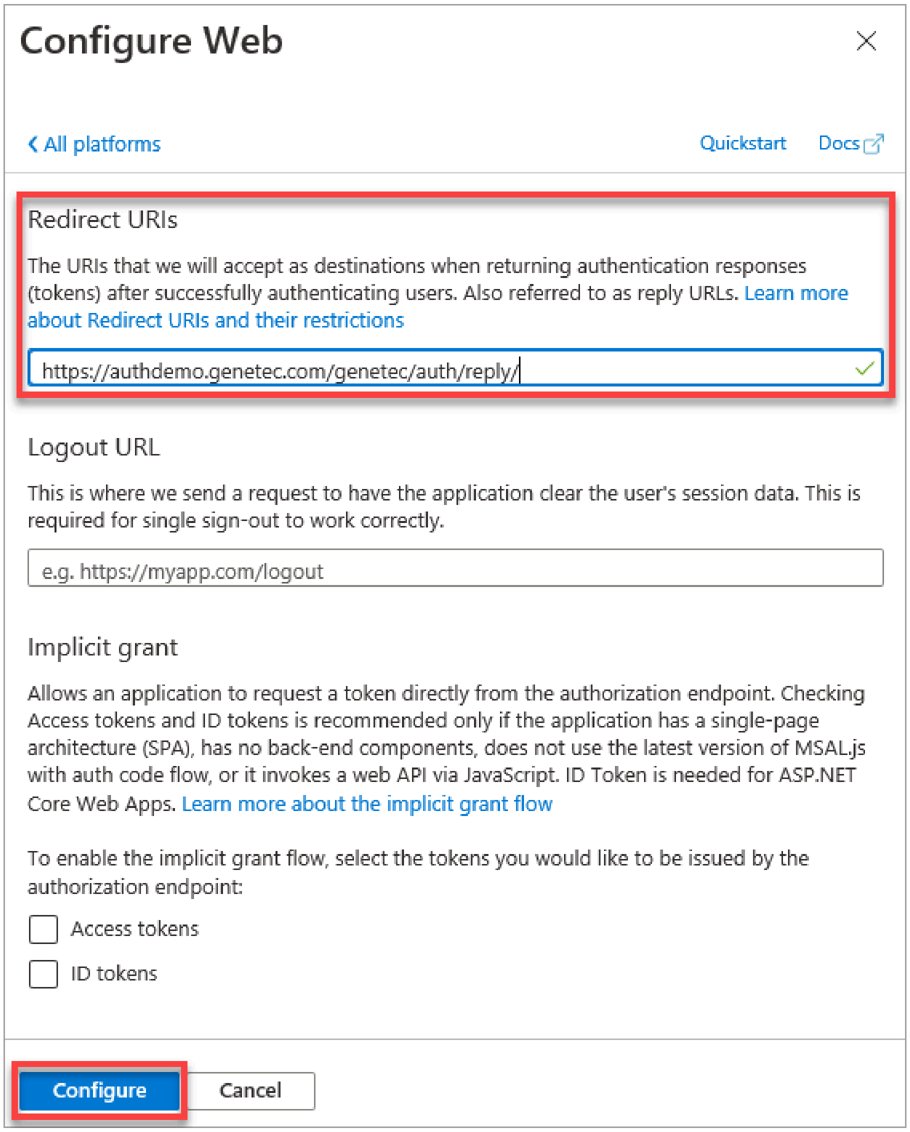
Mobile and desktop applications

iOS / macOS
Objective-C, Swift, Xamarin

Android
Java, Kotlin, Xamarin

Mobile and desktop applications
Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

5. In *Configure Web*, enter the first *redirect* URI for Security Center to **Redirect URIs** and click **Configure**.



Configure Web

Redirect URIs

The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://authdemo.genetec.com/genetec/auth/reply/ ✓

Logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://myapp.com/logout

Implicit grant

Allows an application to request a token directly from the authorization endpoint. Checking Access tokens and ID tokens is recommended only if the application has a single-page architecture (SPA), has no back-end components, does not use the latest version of MSAL.js with auth code flow, or it invokes a web API via JavaScript. ID Token is needed for ASP.NET Core Web Apps. Learn more about the implicit grant flow

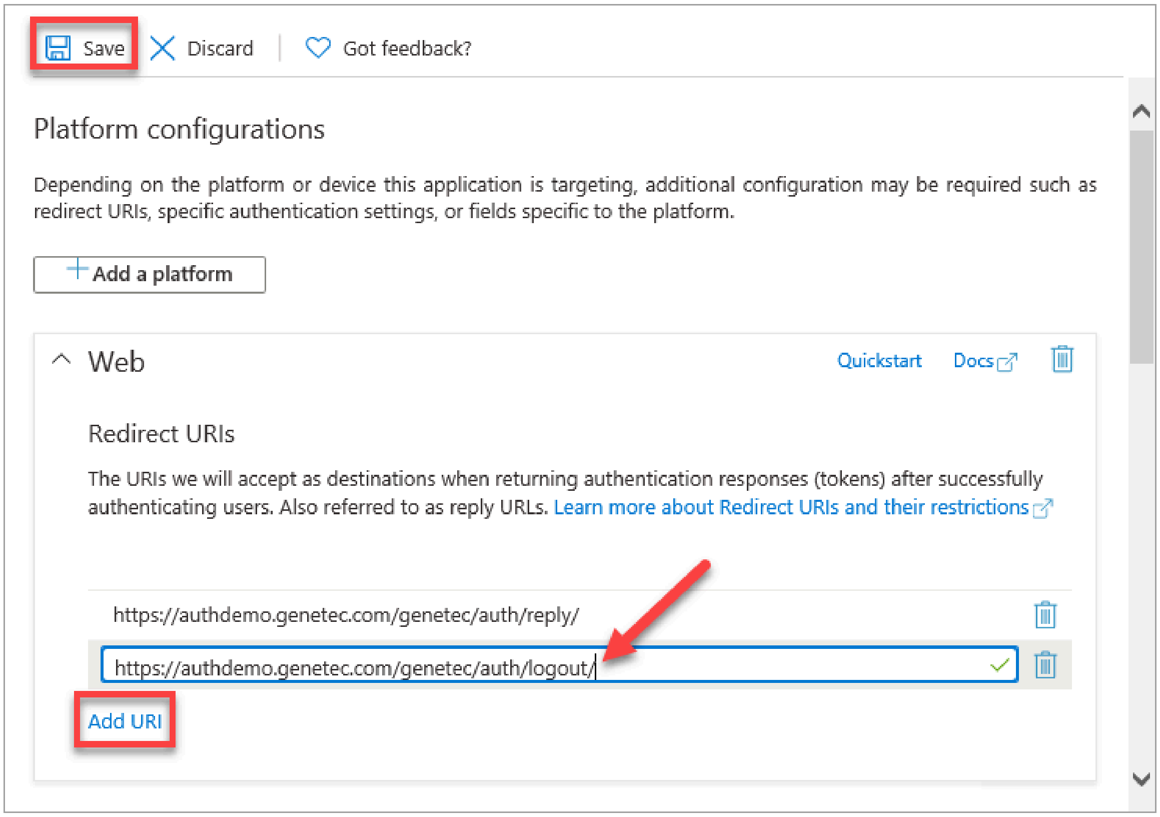
To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

□ Access tokens

□ ID tokens

NOTE: The explicit **Logout URL** is not required by OIDC.

6. Under *Redirect URIs* for the Web platform, click **Add URI** and enter the remaining *redirect* and *logout* URIs for Security Center, and click **Save**.



Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

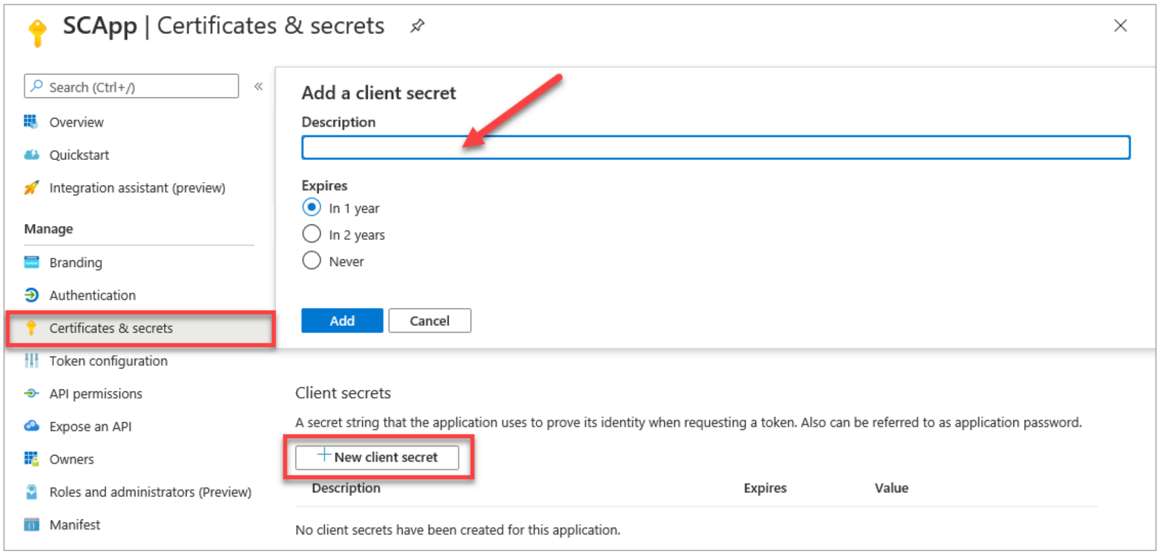
Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://authdemo.genetec.com/genetec/auth/reply/

https://authdemo.genetec.com/genetec/auth/logout/

7. In the left menu for your application, select **Certificates & secrets**, and click **New client secret** to generate a client secret for Security Center.



Add a client secret

Description

Expires
● In 1 year
○ In 2 years
○ Never

Client secrets

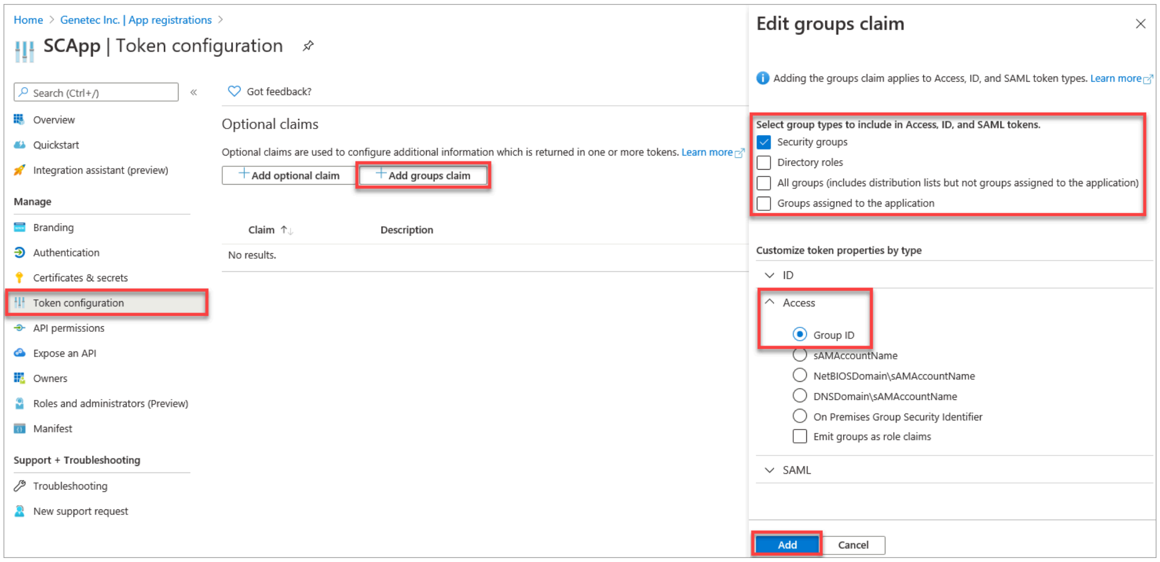
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
No client secrets have been created for this application.		

BEST PRACTICE: After generating your secret, copy it and keep it safe until the integration is complete. It is impossible to retrieve a client secret from the Azure AD configuration. If the secret is lost, you must generate a new one.

8. In the left menu for your application, select **Token configuration**.

9. Click **Add groups claim**, select the group types that you want to grant access to Security Center, select **Group ID** for the Access token type, and click **Add**.



Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim	Description
No results.	

Edit groups claim

Adding the groups claim applies to Access, ID, and SAML token types. Learn more

Select group types to include in Access, ID, and SAML tokens.

- ☑ Security groups
- ☐ Directory roles
- ☐ All groups (includes distribution lists but not groups assigned to the application)
- ☐ Groups assigned to the application

Customize token properties by type

ID

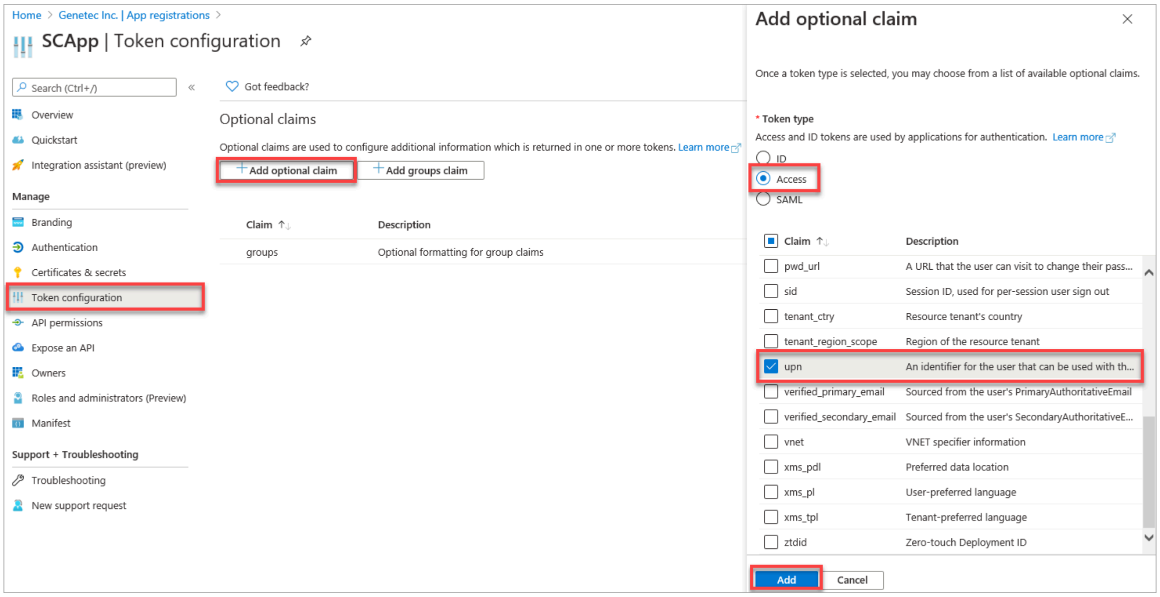
Access

- ● Group ID
- ○ sAMAccountName
- ○ NetBIOSDomain\sAMAccountName
- ○ DNSDomain\sAMAccountName
- ○ On Premises Group Security Identifier
- ☐ Emit groups as role claims

SAML

10. Click **Add optional claim**, select the **Access** token type, select the **UPN** claim, and click **Add**.

NOTE: Security Center requires a unique identifier for the user. UPN is one possibility, but other optional claims, such as email, can be used instead.



Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim	Description
groups	Optional formatting for group claims

Add optional claim

Once a token type is selected, you may choose from a list of available optional claims.

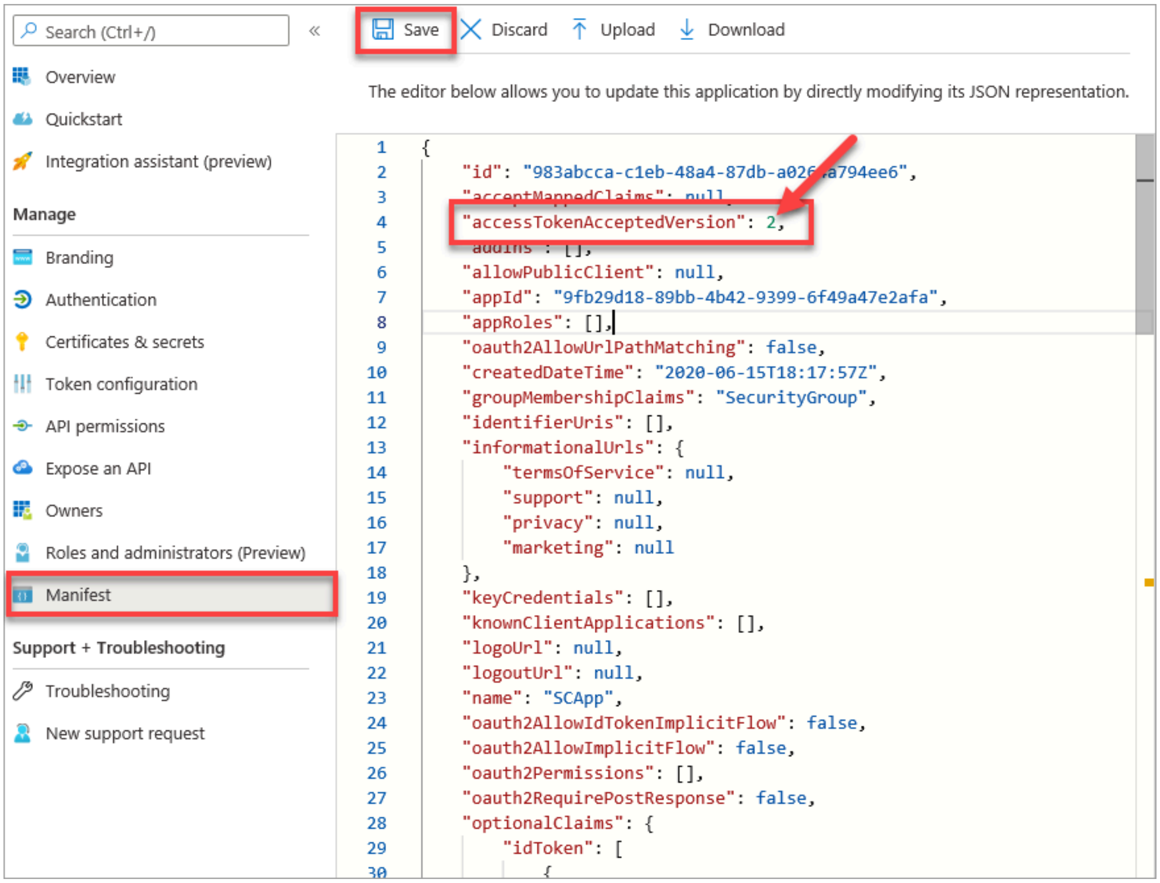
* Token type

Access and ID tokens are used by applications for authentication. Learn more

- ○ ID
- ● Access
- ○ SAML

	Claim	Description
☐	pwd_url	A URL that the user can visit to change their pass...
☐	sid	Session ID, used for per-session user sign out
☐	tenant_ctry	Resource tenant's country
☐	tenant_region_scope	Region of the resource tenant
☑	upn	An identifier for the user that can be used with th...
☐	verified_primary_email	Sourced from the user's PrimaryAuthoritativeEmail
☐	verified_secondary_email	Sourced from the user's SecondaryAuthoritativeE...
☐	vnet	VNET specifier information
☐	xms_pdl	Preferred data location
☐	xms_pl	User-preferred language
☐	xms_tpl	Tenant-preferred language
☐	ztdid	Zero-touch Deployment ID

11. In the left menu for your application, select **Manifest**, set *accessTokenAcceptedVersion* to 2, and click **Save**.

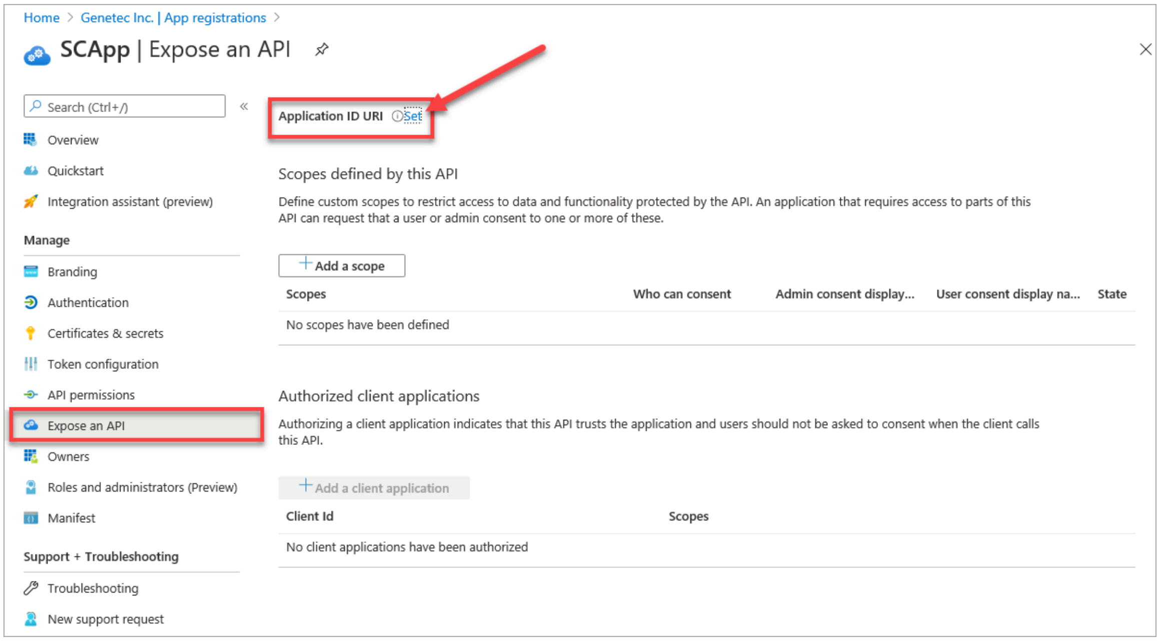


The editor below allows you to update this application by directly modifying its JSON representation.

```
{
    "id": "983abcca-c1eb-48a4-87db-a026-a794ee6",
    "acceptMappedClaims": null,
    "accessTokenAcceptedVersion": 2,
    "addIns": [],
    "allowPublicClient": null,
    "appId": "9fb29d18-89bb-4b42-9399-6f49a47e2afa",
    "appRoles": [],
    "oauth2AllowUrlPathMatching": false,
    "createdDateTime": "2020-06-15T18:17:57Z",
    "groupMembershipClaims": "SecurityGroup",
    "identifierUris": [],
    "informationalUrls": {
        "termsOfService": null,
        "support": null,
        "privacy": null,
        "marketing": null
    },
    "keyCredentials": [],
    "knownClientApplications": [],
    "logoUrl": null,
    "logoutUrl": null,
    "name": "SCApp",
    "oauth2AllowIdTokenImplicitFlow": false,
    "oauth2AllowImplicitFlow": false,
    "oauth2Permissions": [],
    "oauth2RequirePostResponse": false,
    "optionalClaims": {
        "idToken": [
            {
```

12. In the left menu for your application, select **Expose an API**.

13. Click **Set** next to *Application ID URI* to specify a globally unique URI for the Security Center application, and click **Save**.



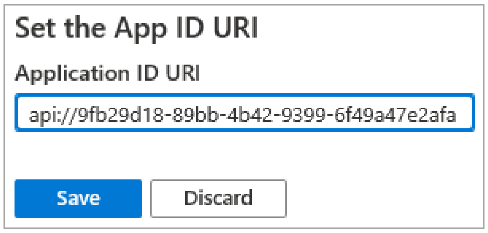
Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

No scopes have been defined

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

No client applications have been authorized

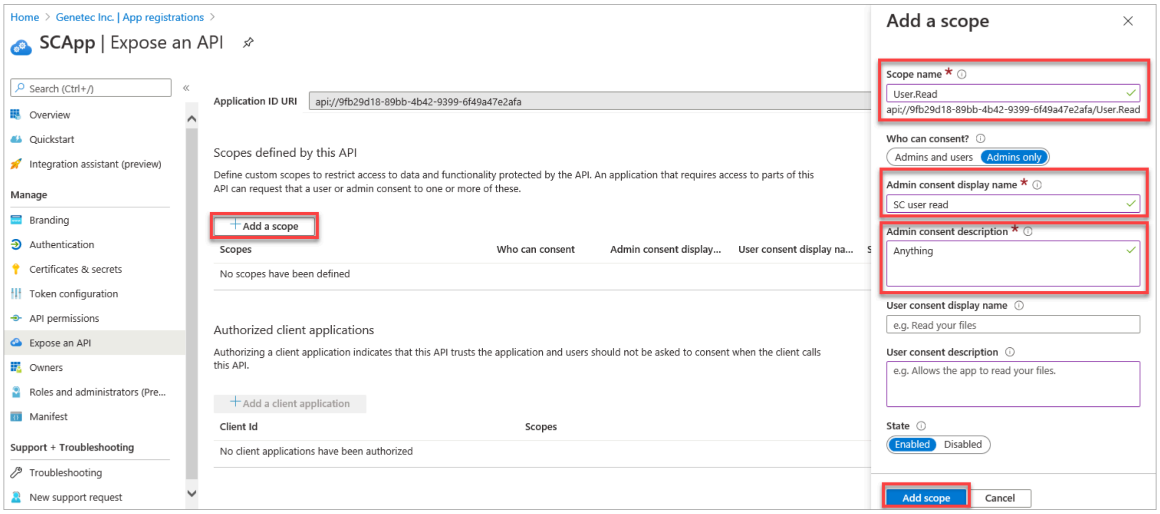
Azure AD automatically generates a usable URI. You can use the default or change it as required.



Application ID URI: api://9fb29d18-89bb-4b42-9399-6f49a47e2afa

14. Click **Add a scope**, fill in the required fields with values of your choice, and click **Add scope**.

NOTE: A custom scope ensures that Azure AD targets Security Center. The scope can specify anything.



Application ID URI: api://9fb29d18-89bb-4b42-9399-6f49a47e2afa

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

No scopes have been defined

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

No client applications have been authorized

Scope name *: User.Read
api://9fb29d18-89bb-4b42-9399-6f49a47e2afa/User.Read

Who can consent?: Admins and users [✓ Admins only]

Admin consent display name *: SC user read

Admin consent description *: Anything

User consent display name: e.g. Read your files

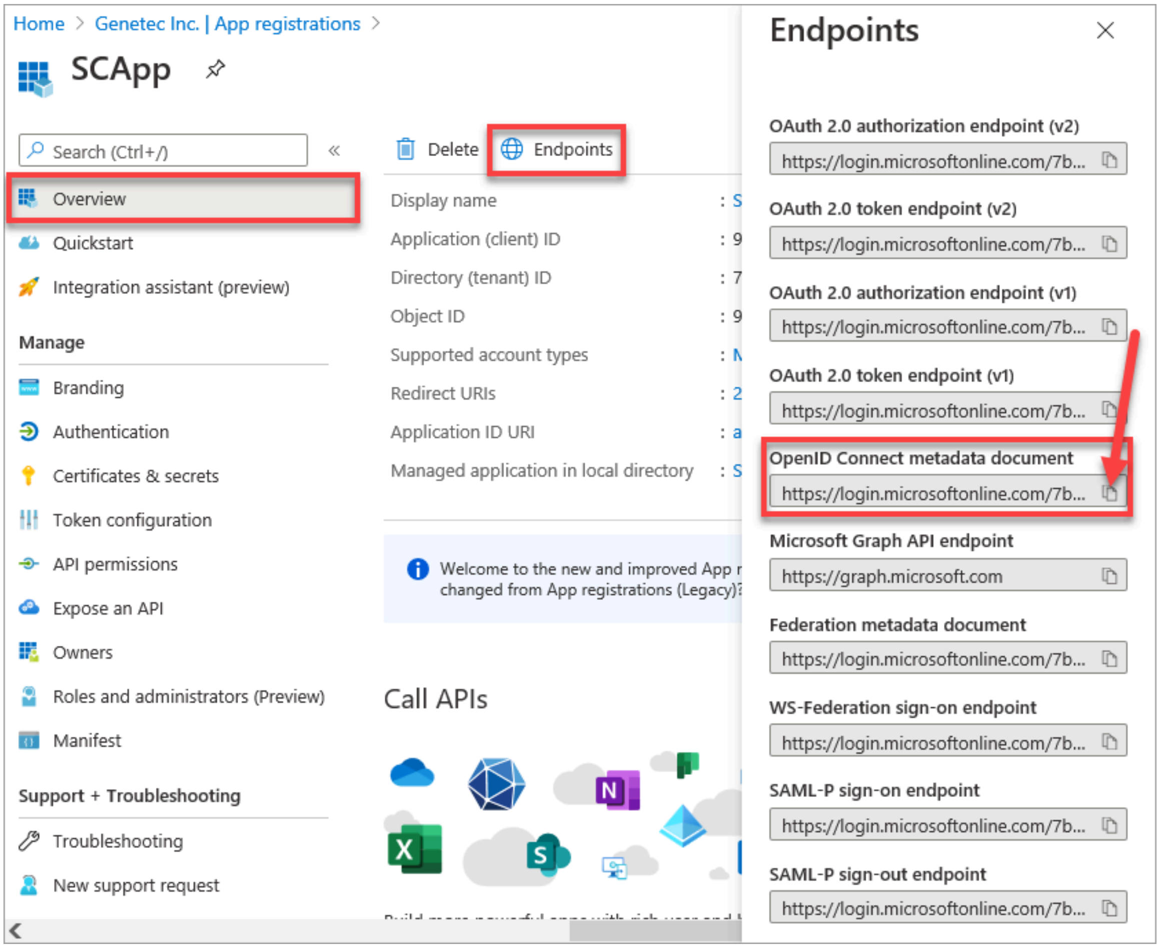
User consent description: e.g. Allows the app to read your files.

State: [✓ Enabled] Disabled

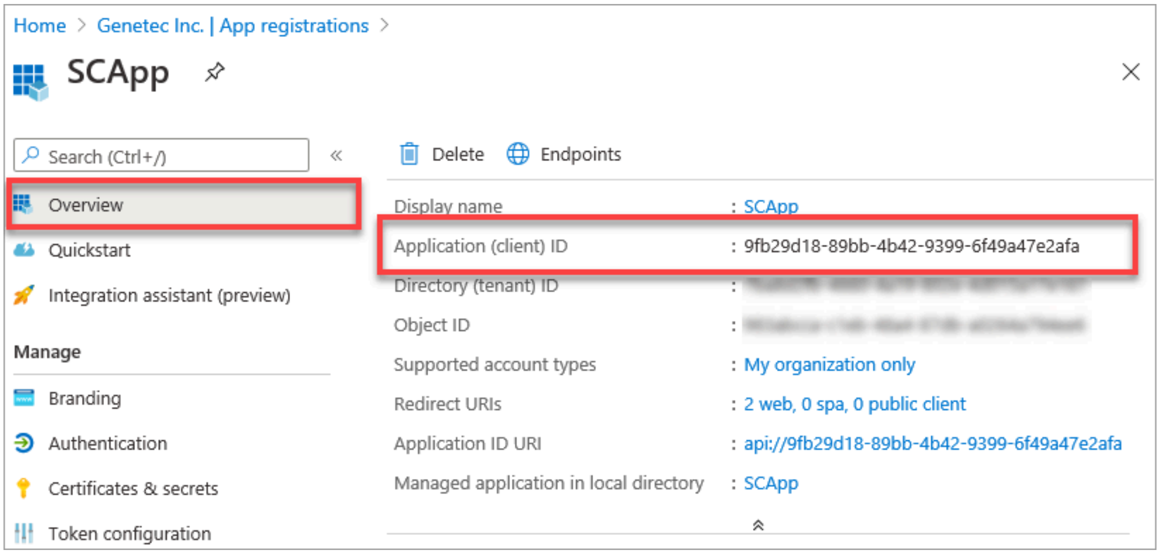
3 - Integrating Security Center with Azure AD

1. In Config Tool, open the Authentication Service role that was created earlier, and click the **Properties** tab.

2. Complete the properties as follows:
   - **Display name:** When logging on to Security Center, third-party authentication options are each presented as a button with the text "Sign in with <*display name*>".
   - **Issuer:** Secure URL (https) pointing to the *OpenID Connect metadata document*. Copy it from *Endpoints* in the Azure AD application configuration.


Home > Genetec Inc. | App registrations >
SCApp
Search (Ctrl+/)
Overview
Quickstart
Integration assistant (preview)
Manage
Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators (Preview)
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Delete
Endpoints
Display name
Application (client) ID
Directory (tenant) ID
Object ID
Supported account types
Redirect URIs
Application ID URI
Managed application in local directory
Welcome to the new and improved App r
changed from App registrations (Legacy)?
Call APIs
Endpoints
OAuth 2.0 authorization endpoint (v2)
https://login.microsoftonline.com/7b...
OAuth 2.0 token endpoint (v2)
https://login.microsoftonline.com/7b...
OAuth 2.0 authorization endpoint (v1)
https://login.microsoftonline.com/7b...
OAuth 2.0 token endpoint (v1)
https://login.microsoftonline.com/7b...
OpenID Connect metadata document
https://login.microsoftonline.com/7b...
Microsoft Graph API endpoint
https://graph.microsoft.com
Federation metadata document
https://login.microsoftonline.com/7b...
WS-Federation sign-on endpoint
https://login.microsoftonline.com/7b...
SAML-P sign-on endpoint
https://login.microsoftonline.com/7b...
SAML-P sign-out endpoint
https://login.microsoftonline.com/7b...

   - **Domain names:** The domain names of users who will authenticate using Azure AD, such as `genetec.com`. You must have at least one.
   - **Client ID:** Unique identifier that represents Security Center in Azure AD. Copy it from the *Overview* in the Azure AD application configuration.



Home > Genetec Inc. | App registrations >

SCApp

Search (Ctrl+/)

- Overview
- Quickstart
- Integration assistant (preview)

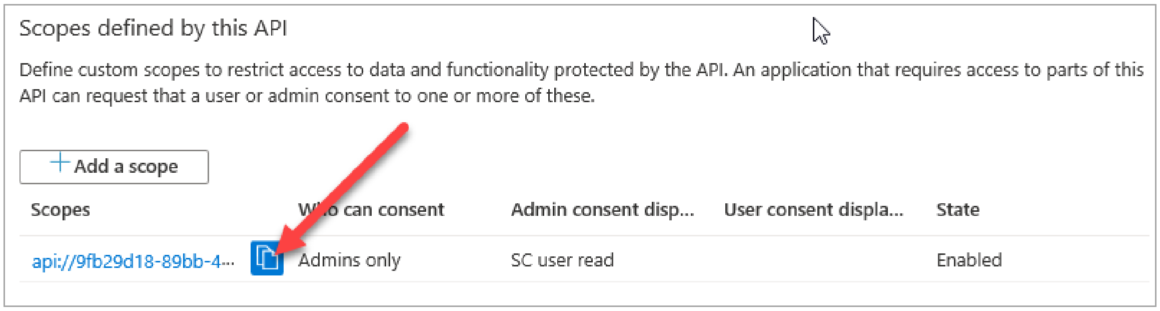
Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration

Delete   Endpoints

Display name : SCApp
Application (client) ID : 9fb29d18-89bb-4b42-9399-6f49a47e2afa
Directory (tenant) ID : [redacted]
Object ID : [redacted]
Supported account types : My organization only
Redirect URIs : 2 web, 0 spa, 0 public client
Application ID URI : api://9fb29d18-89bb-4b42-9399-6f49a47e2afa
Managed application in local directory : SCApp

- **Confidential client:** Switch to **ON** if you elected to generate a client secret in Azure AD.
- **Client secret:** Input the client secret you generated in Azure AD.
- **Username claim:** Enter: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn`
- **Group claim:** Enter: `groups`
- **Scopes (advanced setting):** The custom scope you created in Azure AD. Copy it from *Expose an API* in the Azure AD application configuration.



Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

+ Add a scope

Scopes	Who can consent	Admin consent disp...	User consent displa...	State
api://9fb29d18-89bb-4...	Admins only	SC user read		Enabled

Leave all other properties with the default value.

3. Click **Apply**.
4. Bulk download your list of groups from Azure Active Directory as a CSV file.
5. Import user groups from the downloaded CSV file to Security Center.

   NOTE: The external unique identifier of imported groups must match the *Object Id* of those groups in Azure AD.

How to integrate Security Center with Okta using OpenID Connect

Before Security Center can use Okta to authenticate users with OpenID Connect, setup is required in Config Tool and the Okta Admin Console.

This example shows the steps required to set up third-party authentication with Okta using the OpenID Connect (OIDC) UserInfo endpoint. The procedure is divided into the following sections:

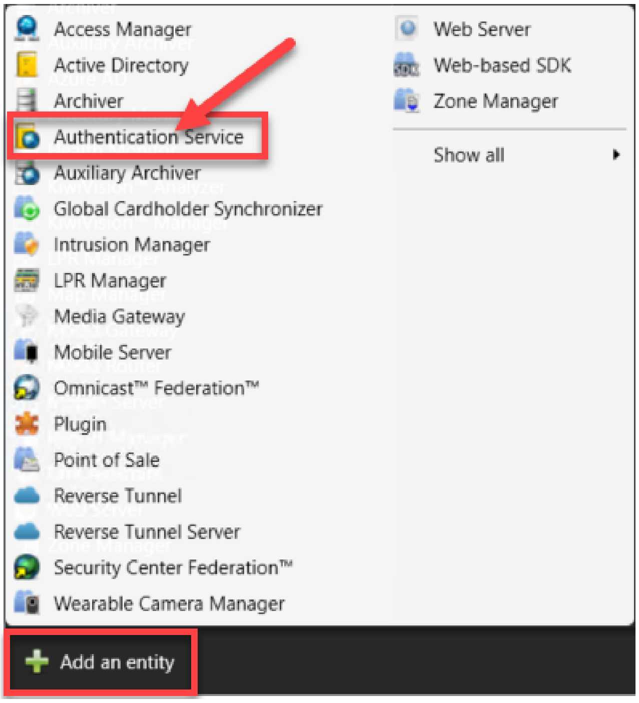
1. Preparing Security Center
2. Preparing Okta
3. Integrating Security Center with Okta

To implement third-party authentication, you must have administrator rights in Security Center and Okta.

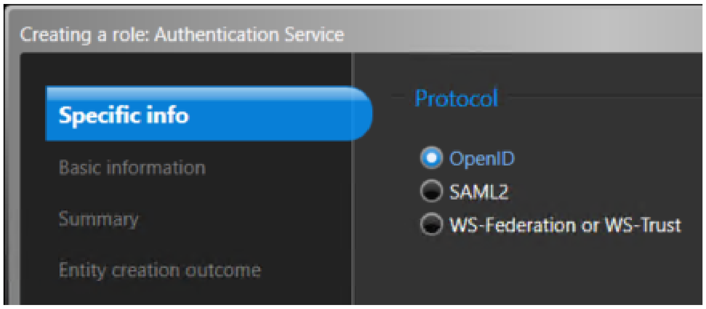
IMPORTANT: This sample integration might differ from your requirements and the Okta Admin Console is subject to change. When setting up Okta, ensure that all steps are adapted to your specific situation.

1 - Preparing Security Center

1. Open Config Tool and connect to the Security Center *main server* as an administrator.
2. In Config Tool, open **System** > **Roles** and click **Add an entity** > **Authentication Service**.



3. In the *Creating a role: Authentication Service* window, select **OpenID** and click **Next**.

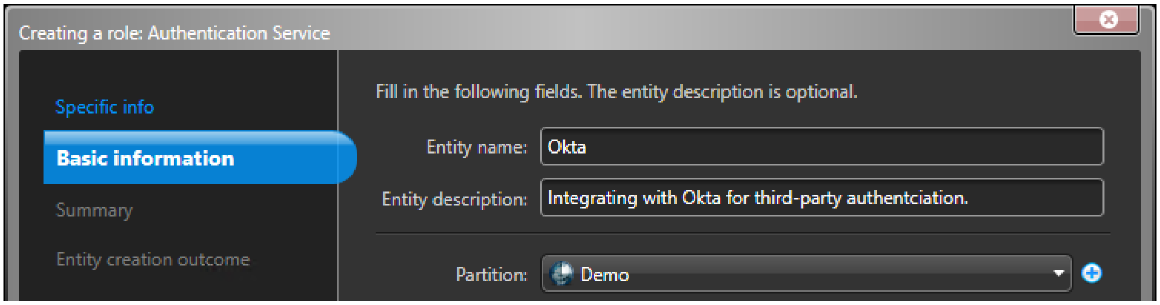


Creating a role: Authentication Service

Protocol

● OpenID
○ SAML2
○ WS-Federation or WS-Trust

4. Enter a name and optional description for the new Authentication Service role and click **Next**.



Creating a role: Authentication Service

Fill in the following fields. The entity description is optional.

Entity name: Okta

Entity description: Integrating with Okta for third-party authentciation.

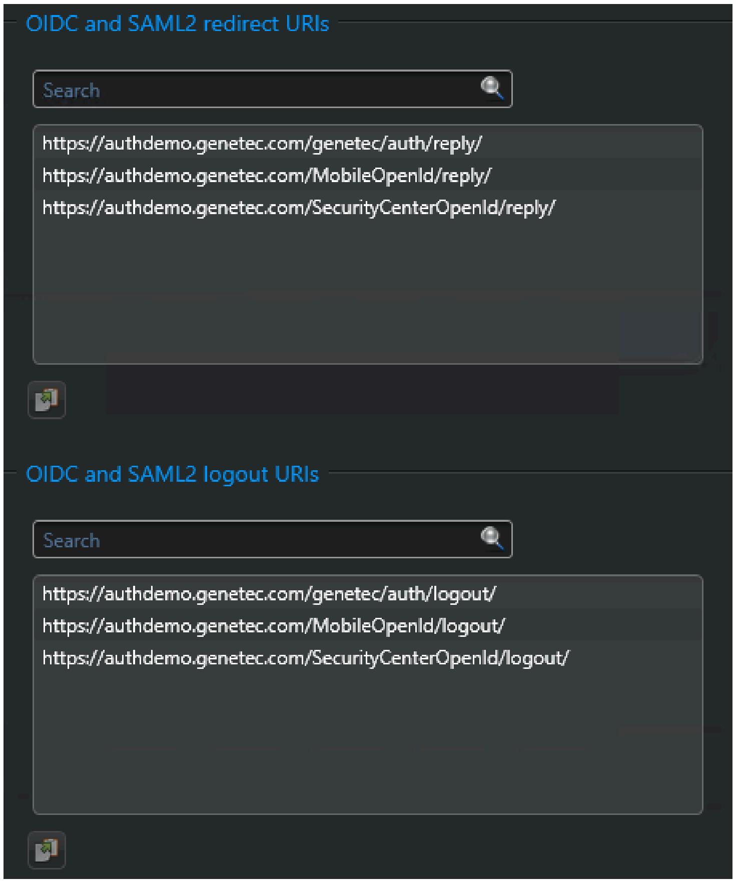
Partition: Demo

NOTE: If your system has multiple partitions, you can also add the new role to a specific partition here.

5. On the *Summary* page, ensure all the information is correct, click **Create**, and click **Close**.

6. In the newly created role, click the **Network endpoint** tab.
7. On the *Network endpoint* page, copy the OIDC *redirect* and *logout* URIs. These are needed to configure Okta **Sign-in redirect URIs** and **Sign-out redirect URIs**.

   NOTE: You might need to restart the *System* task to see the endpoint URIs.



OIDC and SAML2 redirect URIs

Search

https://authdemo.genetec.com/genetec/auth/reply/
https://authdemo.genetec.com/MobileOpenId/reply/
https://authdemo.genetec.com/SecurityCenterOpenId/reply/

OIDC and SAML2 logout URIs

Search

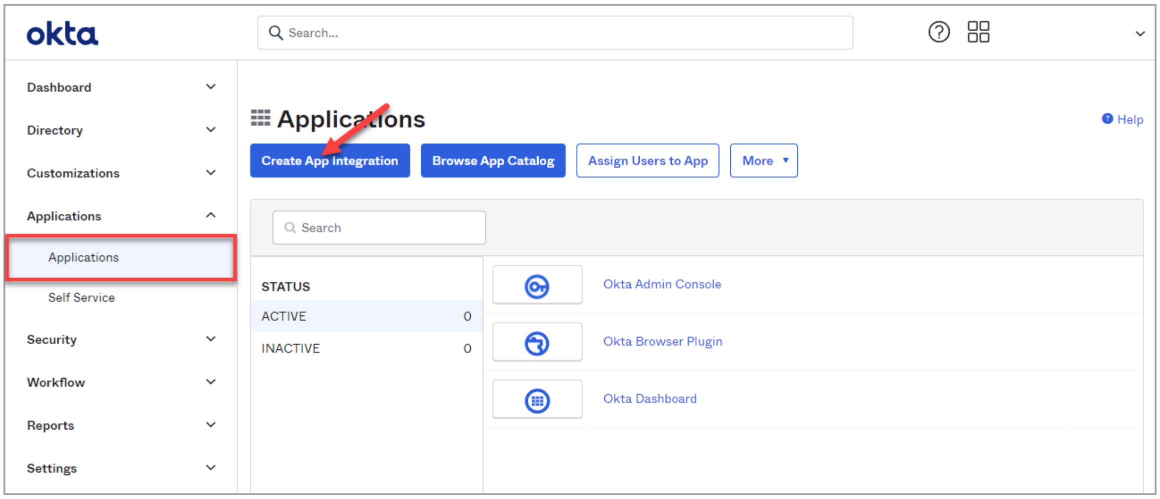
https://authdemo.genetec.com/genetec/auth/logout/
https://authdemo.genetec.com/MobileOpenId/logout/
https://authdemo.genetec.com/SecurityCenterOpenId/logout/

2 - Preparing Okta

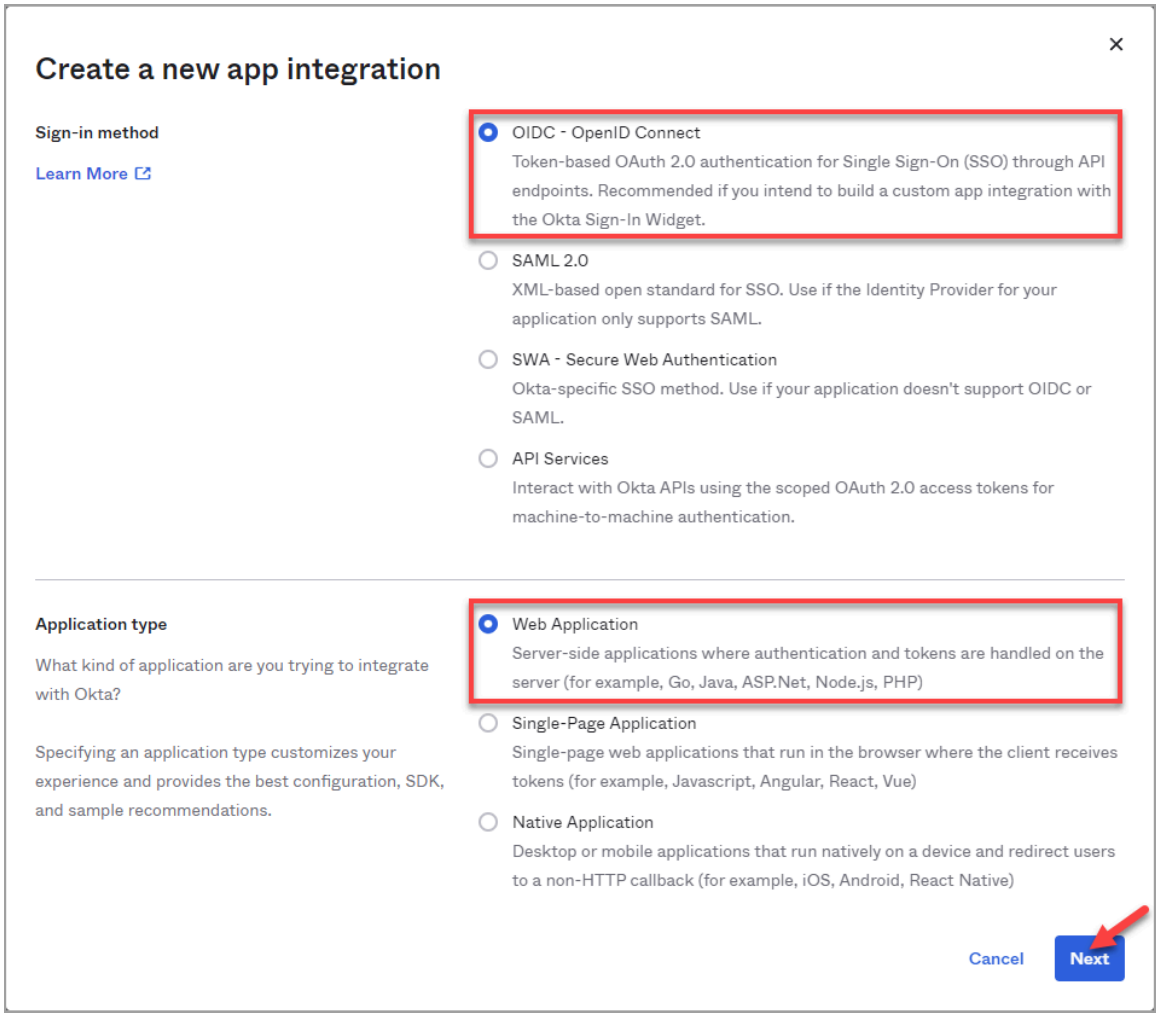
Before completing these steps in the Okta Admin Console, you must meet all of the following prerequisites:

- Have an Okta administrator account.
- Have provisioned at least one user.
- Have provisioned at least one user group that contains the users you want to grant access to Security Center.

1. In the Okta Admin Console, select **Applications** > **Applications** and then click **Create App Integration**.



2. In the *Create a new app integration* wizard, select **OIDC - OpenID Connect**, **Web Application**, and click **Next**.



Create a new app integration

Sign-in method

Learn More

● OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

○ SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

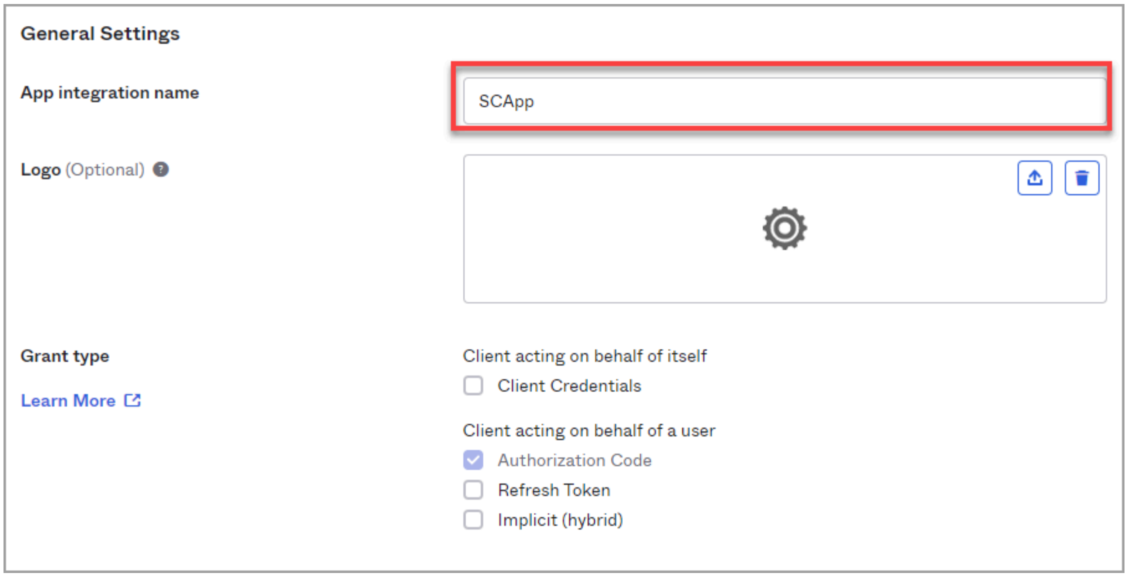
● Web Application
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

○ Single-Page Application
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)

○ Native Application
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

3. On the *New Web App Integration* page, set the following and click **Save**:

   - **App integration name**



General Settings

App integration name: SCApp

Logo (Optional)

Grant type

Client acting on behalf of itself

□ Client Credentials

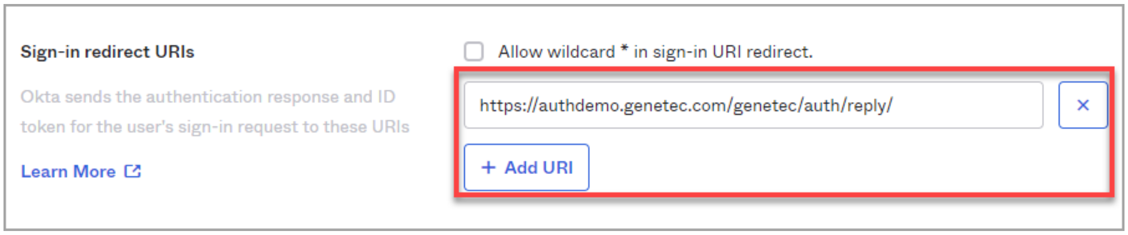
Client acting on behalf of a user

☑ Authorization Code

□ Refresh Token

□ Implicit (hybrid)

   - **Sign-in redirect URIs** copied from the *redirect* URIs in Security Center



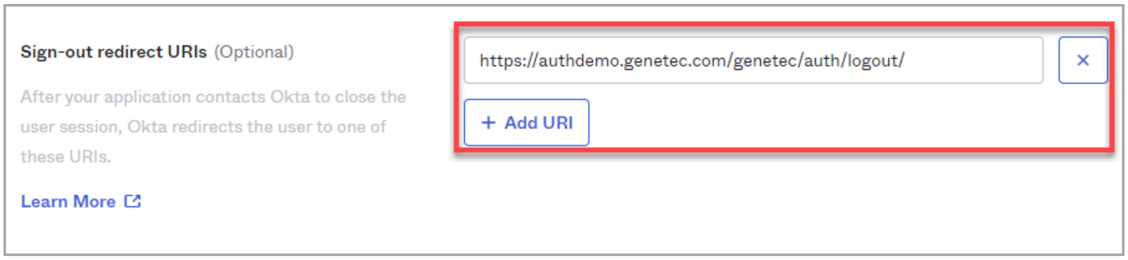
Sign-in redirect URIs

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

□ Allow wildcard * in sign-in URI redirect.

https://authdemo.genetec.com/genetec/auth/reply/

   - **Sign-out redirect URIs** copied from the *logout* URIs in Security Center

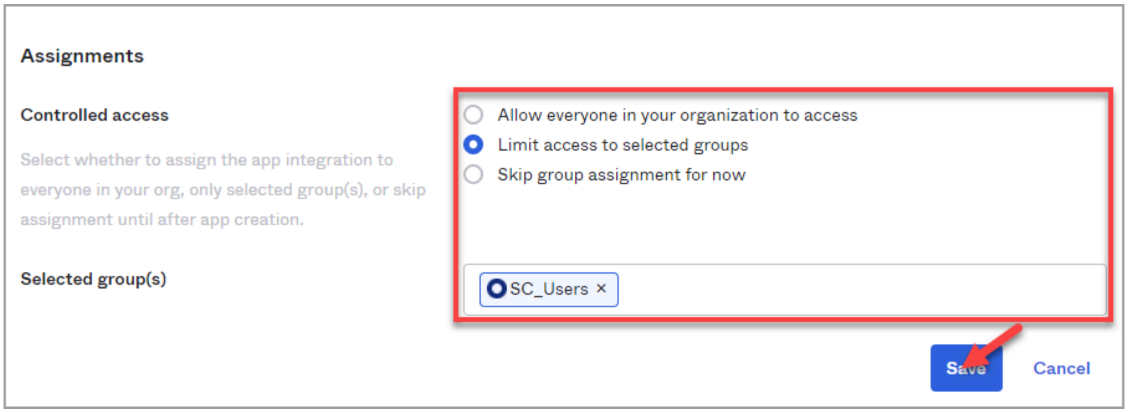


Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

https://authdemo.genetec.com/genetec/auth/logout/

   - **Controlled access** select **Limit access to selected groups** and add the required groups



Assignments

Controlled access

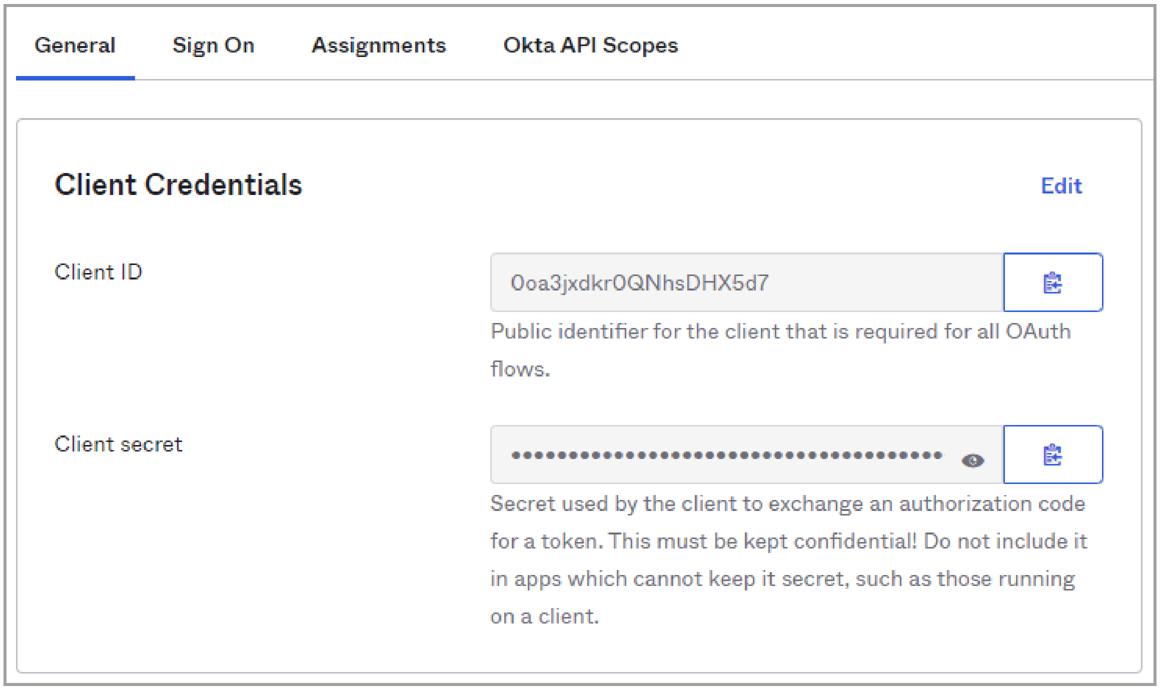
Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

○ Allow everyone in your organization to access
● Limit access to selected groups
○ Skip group assignment for now

Selected group(s)

SC_Users ×

4. On the *General* page for your application, copy the default **Client ID** and **Client secret**. These are needed to configure Security Center. If required, you can click **Edit** to generate a new client secret.



Client Credentials

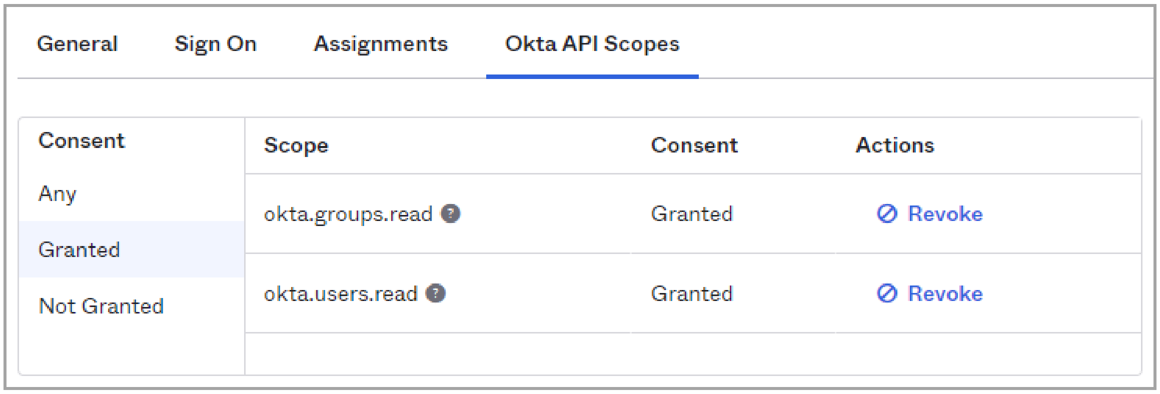
Client ID: 0oa3jxdkr0QNhsDHX5d7

Public identifier for the client that is required for all OAuth flows.

Client secret: ••

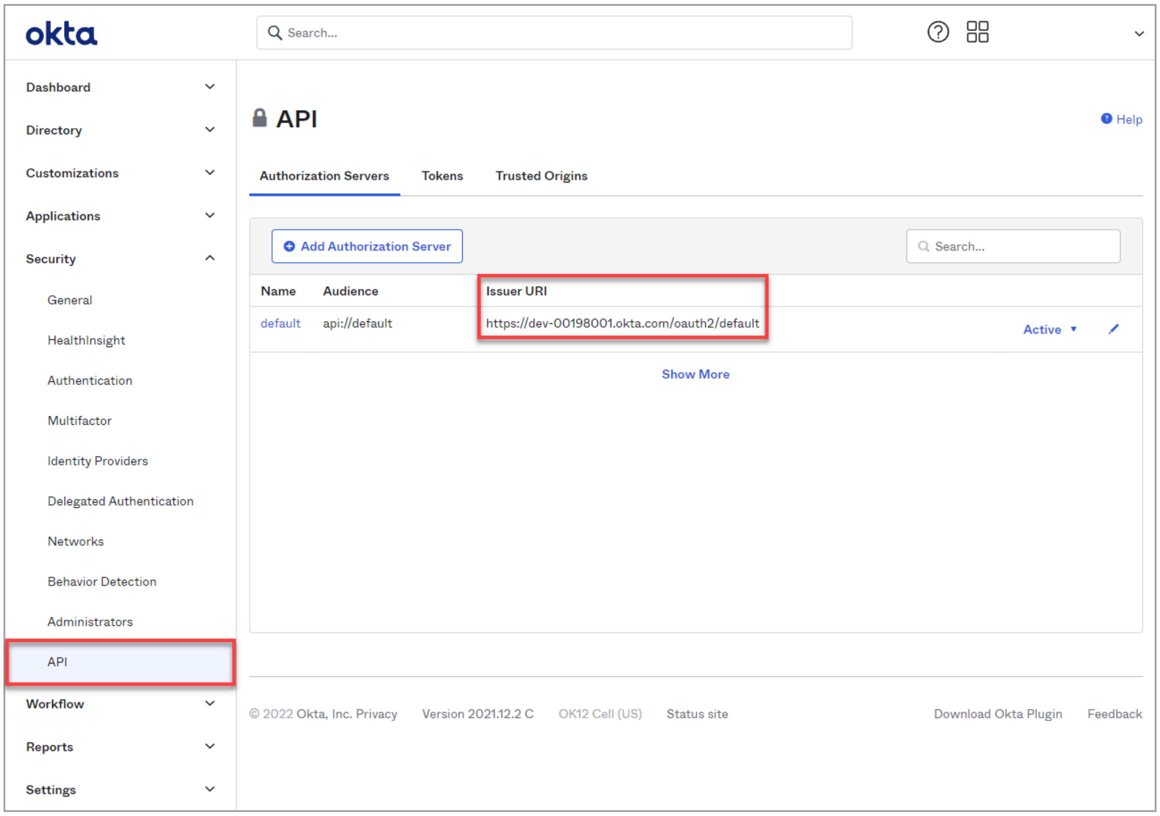
Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

5. Click the **Okta API Scopes** tab for your Security Center application and grant the okta.groups.read and okta.users.read operations.



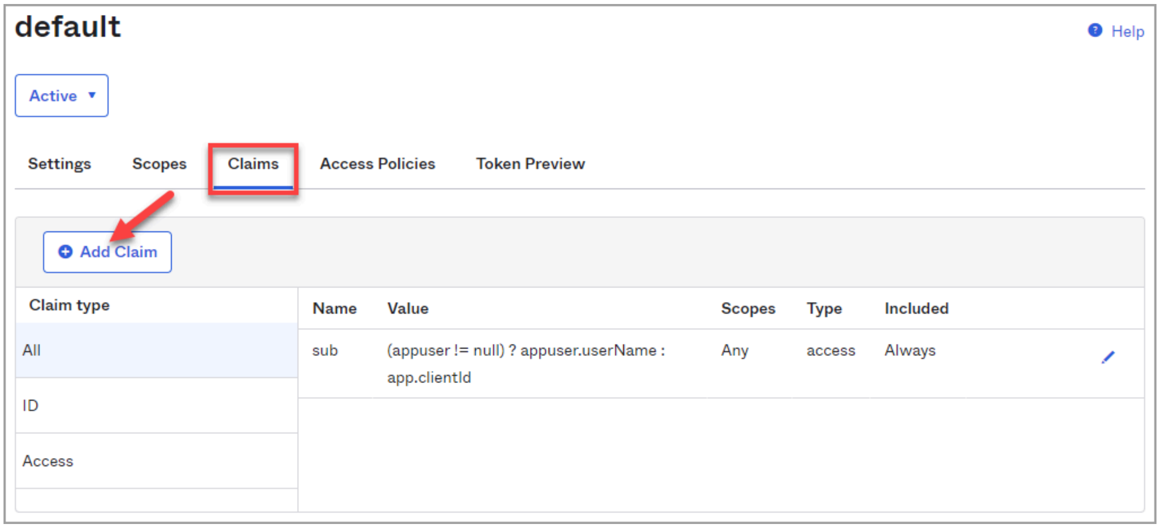
Scope	Consent	Actions
okta.groups.read	Granted	Revoke
okta.users.read	Granted	Revoke

6. Click **Security** > **API** and copy the *Issuer URI* for the default authorization server. This URI is needed to configure Security Center.



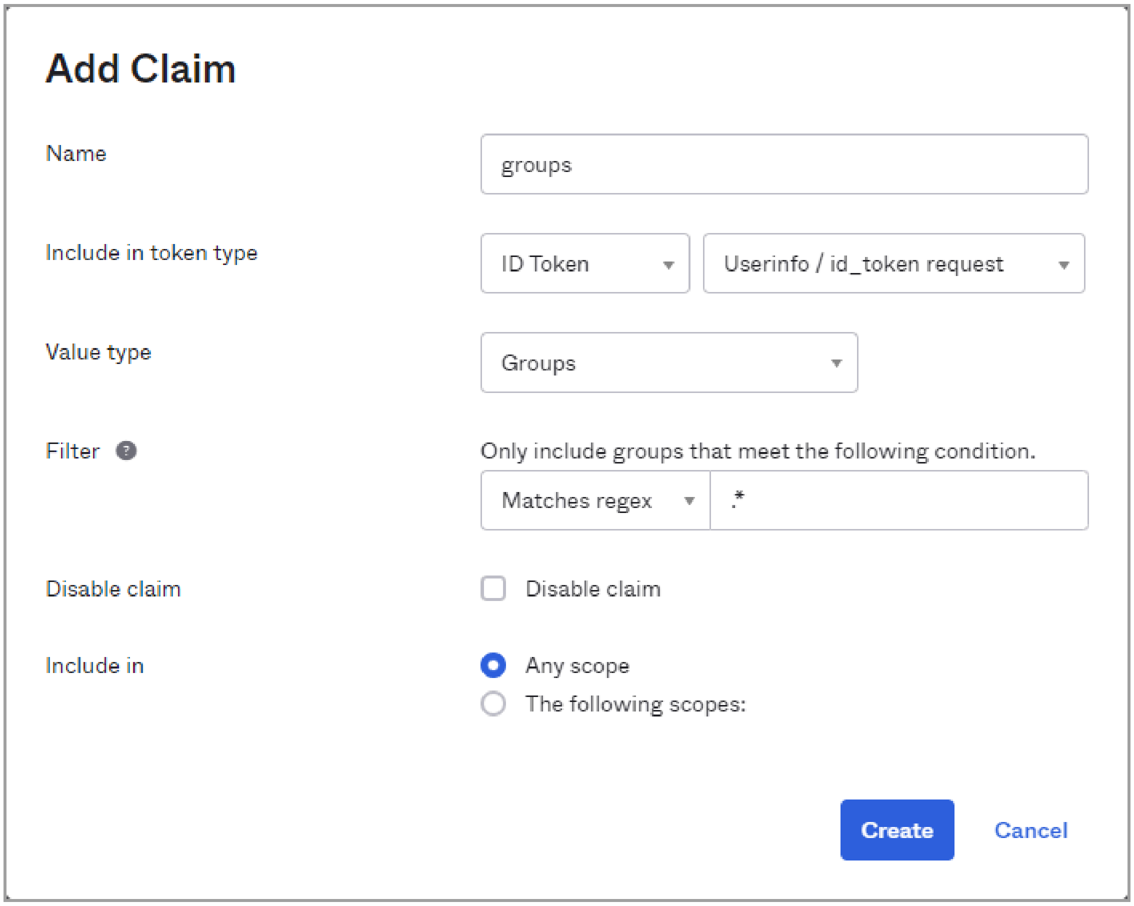
Name	Audience	Issuer URI	
default	api://default	https://dev-00198001.okta.com/oauth2/default	Active ▾

7. Open the default authorization server, click the **Claims** tab, and click **Add Claim**.



Name	Value	Scopes	Type	Included
sub	(appuser != null) ? appuser.userName : app.clientId	Any	access	Always

8. Add a groups claim as follows and click **Create**:



Add Claim

Name: groups

Include in token type: ID Token ▾ | Userinfo / id_token request ▾

Value type: Groups ▾

Filter: Only include groups that meet the following condition. Matches regex ▾ | .*

Disable claim: □ Disable claim

Include in: ● Any scope ○ The following scopes:

NOTE: The *Matches regex* filter with .* returns all groups to which the authenticated user belongs.

If required, the filter can also be used to exclude certain groups from the claim. At least one group assigned to Security Center must be included with the claim to grant access.

3 - Integrating Security Center with Okta

1. In Config Tool, open the Authentication Service role that was created earlier, and click the **Properties** tab.
2. Complete the properties as follows:
   - **Display name:** When logging on to Security Center, third-party authentication options are each presented as a button with the text "Sign in with <*display name*>".
   - **Issuer:** Enter the *Issuer URI* that was copied from the default authorization server in Okta.
   - **Domain names:** The domain names of users who will authenticate using Okta, such as `genetec.com`. You must have at least one.
   - **Client ID:** Enter the *Client ID* that you copied from the Security Center application in Okta.
   - **Confidential client:** Switch to **ON**.
   - **Client secret:** Enter the *Client secret* that you copied from the Security Center application in Okta.
   - **Username claim:** Enter: `preferred_username`
   - **Group claim:** Enter: `groups`
   - **Obtain claims from (advanced setting):**
     - Switch **Access token** to **OFF**.
     - Switch **User info endpoint** to **ON**.

   Leave all other properties with the default value.

3. Click **Apply**.
4. Create one or more user groups with the exact same name as the groups assigned to the Security Center application in Okta.
5. Add groups authorized to connect using Okta to the *User groups* list in Authentication Service role.

SAML 2.0 Integration overview

Before users can log on to Security Center using an external identity provider with SAML 2.0, you must follow a sequence of steps.

The following table lists the tasks required to deploy third-party authentication using SAML 2.0:

Step	Task	Where to find more information
Understand prerequisites and key issues before integrating		
1	Learn about the different components and how they connect.	• OpenID Connect and SAML2.0 integration.
2	Ensure all Security Center clients trust the connection to your identity provider. To establish trust, a trusted Certificate Authority must sign the public key certificate for the identity provider on the computer or mobile device connecting to Security Center.	
3	Verify that your Security Center license includes SAML2 integrations. Go to the Config Tool homepage, click **About** > **Security Center**, and confirm that Number of SAML2 integrations is one or more.	• License options in Security Center on page 1447
Prepare Security Center		

Step	Task	Where to find more information
4	Add an Authentication Service role for SAML2 and click the **Network endpoint** tab. You might need to restart the *System* task to see the endpoints. The *redirect* and *logout* endpoints are required to configure your identity provider. There are different URIs for each client type: • ***/genetec:*** Config Tool, Security Desk, and SDK • ***/<Mobile>*OpenId:** Genetec™ Mobile • ***/<SecurityCenter>*OpenId:** Web Client **NOTE:** *Mobile* and *SecurityCenter* are the default web addresses for the Mobile Server role and the Web Server role. Any modification to these web addresses is reflected in the corresponding URIs. To work with role failover, separate *redirect* and *logout* URIs are needed for each server that can host the Directory, Mobile Server, and Web Server roles. Ensure that role failover is properly configured to see all the required endpoints. If any servers are added or retired after setting up the identity provider, you might need to update the configuration by adding or removing URIs. All clients must be able to resolve the endpoint URI for their type. If a public address is being used, that address must resolve to the correct server for clients connecting from your private network. Security Center also provides a SAML2 metadata document that includes all required endpoints. You can point to this endpoint from your identity provider to accelerate the setup and ensure that the latest configuration is always available.	• Setting up Directory failover and load balancing on page 168 • Setting up role failover on page 164
Integrate the external identity provider		
5	Following the instructions from your identity provider, add Security Center as a relying application in that system. For successful authentication, Security Center requires the identity provider to return assertions about the authenticated party in an access token. At a minimum, those assertions must include a username assertion, a name identifier assertion, and a group membership assertion. The Security Center SAML2 metadata document outlines the expected format of the name identifier.	

Step	Task	Where to find more information
6	Add authorized user groups from your identity provider to Security Center and set privileges. If your identity provider can export a list of groups in CSV format, that list can be imported to Security Center. Typically, identity providers use names to uniquely identify user groups. When names are used, Security Center user groups must have the same name as the corresponding group from your identity provider, and include the domain name. For example: `Operators@YourCompany.com`. If your identity provider uses an ID to uniquely identify a user group, you must perform another step before linking the group to the Authentication Service role. Add the ID to the **External unique identifier** property for the corresponding user group in Security Center. Users are automatically created and added to their assigned group, or groups when they log on for the first time.	• Creating user groups on page 429 • About privileges on page 438 • Importing user groups from a CSV file for third-party authentication on page 527
7	Configure the Authentication Service role with information about your identity provider. Open the Authentication Service role for SAML2, click the **Properties** tab, and input the required fields.	• Authentication Service - Properties tab (SAML2) on page 1349

How to integrate Security Center with Okta using SAML 2.0

Before Security Center can use Okta to authenticate users with SAML 2.0, setup is required in Config Tool and the Okta Admin Console.

This example shows the steps required to set up third-party authentication with Okta using SAML 2.0. The procedure is divided into the following sections:

1. Preparing Security Center
2. Preparing Okta
3. Integrating Security Center with Okta

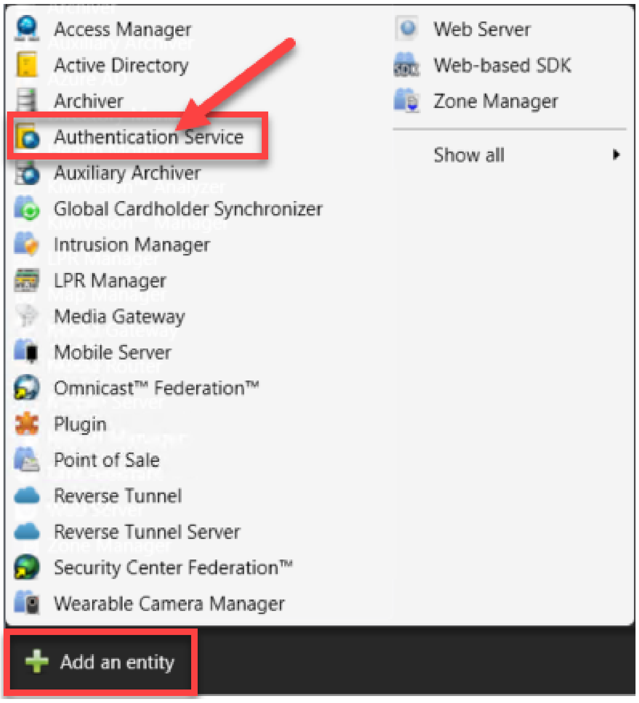
To implement third-party authentication, you must have administrator rights in Security Center and Okta.

IMPORTANT: This sample integration might differ from your requirements and the Okta Admin Console is subject to change. When setting up Okta, ensure that all steps are adapted to your specific situation.

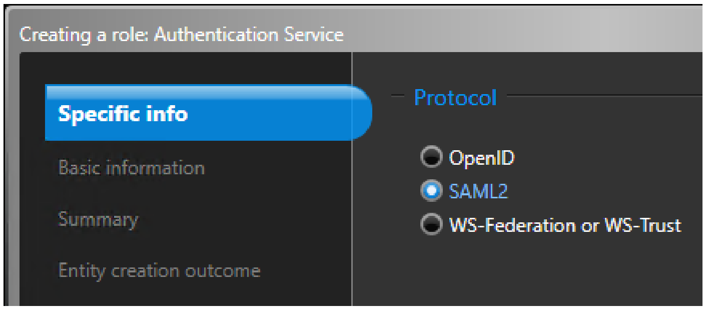
1 - Preparing Security Center

1. Open Config Tool and connect to the Security Center *main server* as an administrator.

2. In Config Tool, open **System** > **Roles** and click **Add an entity** > **Authentication Service**.



3. In the *Creating a role: Authentication Service* window, select **SAML2** and click **Next**.

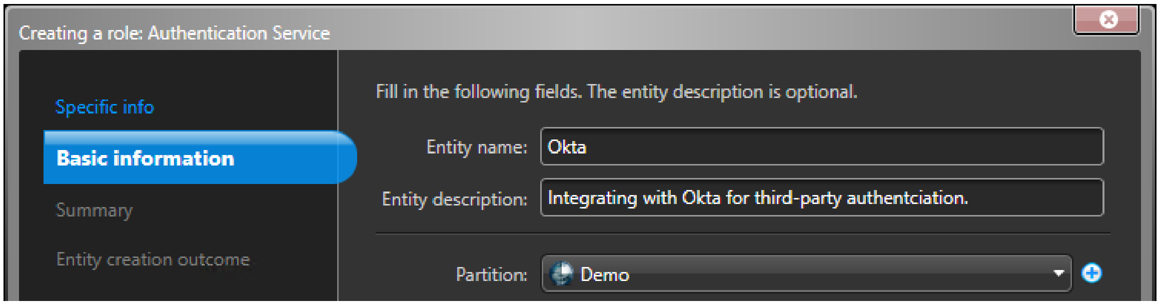


Creating a role: Authentication Service

Protocol

○ OpenID
● SAML2
○ WS-Federation or WS-Trust

4. Enter a name and optional description for the new Authentication Service role and click **Next**.



Creating a role: Authentication Service

Fill in the following fields. The entity description is optional.

Entity name: Okta

Entity description: Integrating with Okta for third-party authentciation.

Partition: Demo

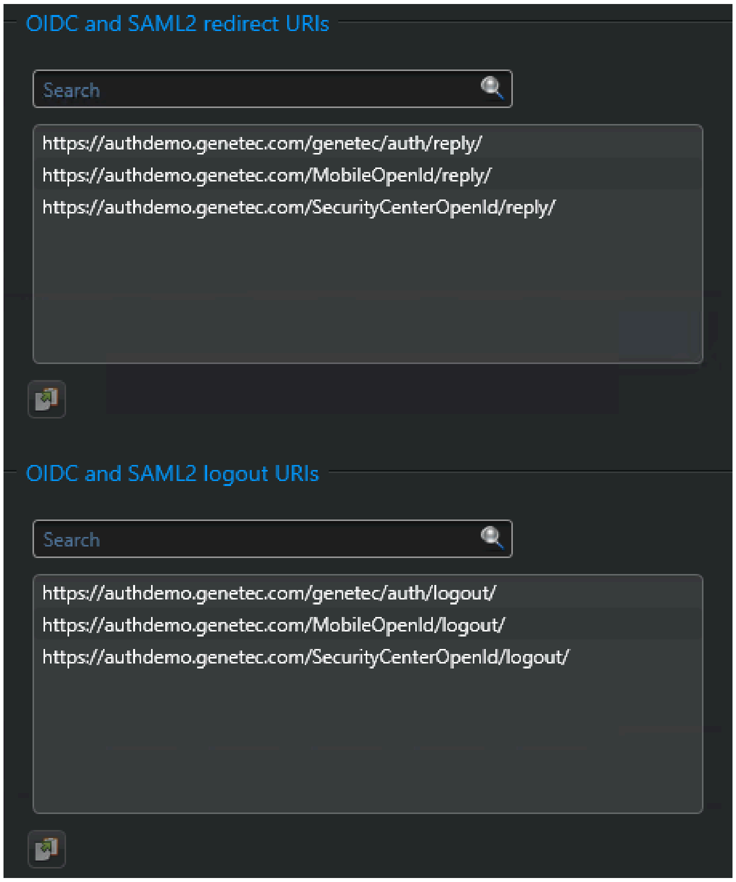
NOTE: If your system has multiple partitions, you can also add the new role to a specific partition here.

5. On the *Summary* page, ensure all the information is correct, click **Create**, and click **Close**.
6. In the newly created role, click the **Network endpoint** tab.

7. On the *Network endpoint* page, copy the *redirect* and *logout* URIs. These are needed to configure the Okta **Single sign on URL** and **Single Logout URL**.

   NOTE: You might need to restart the *System* task to see the endpoint URIs.

   The same URIs are used for OIDC and SAML 2.0. These URIs must be reachable from all clients using Single Sign-On.



OIDC and SAML2 redirect URIs

https://authdemo.genetec.com/genetec/auth/reply/
https://authdemo.genetec.com/MobileOpenId/reply/
https://authdemo.genetec.com/SecurityCenterOpenId/reply/

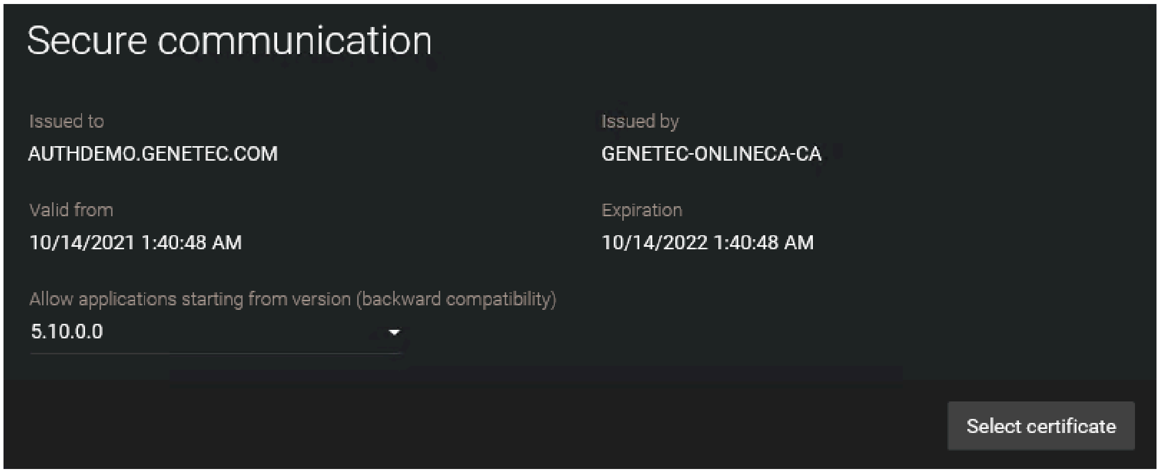
OIDC and SAML2 logout URIs

https://authdemo.genetec.com/genetec/auth/logout/
https://authdemo.genetec.com/MobileOpenId/logout/
https://authdemo.genetec.com/SecurityCenterOpenId/logout/

8. On the Security Center main server, follow the instructions for your operating system to export the public key certificate used by the Security Center main server in X.509 format.

   NOTE: The certificate Common Name (CN) or Subject Alternative Name (SAN) must match the hostname, IP address, or Fully Qualified Domain Name (FQDN) that is used in the *redirect* and *logout* URIs.

   This public key is required by Okta to enable Single Logout. The Security Center certificate is shown in the *Secure communication* section on the Server Admin - *Main server* page.



Secure communication

Issued to: AUTHDEMO.GENETEC.COM

Issued by: GENETEC-ONLINECA-CA

Valid from: 10/14/2021 1:40:48 AM

Expiration: 10/14/2022 1:40:48 AM

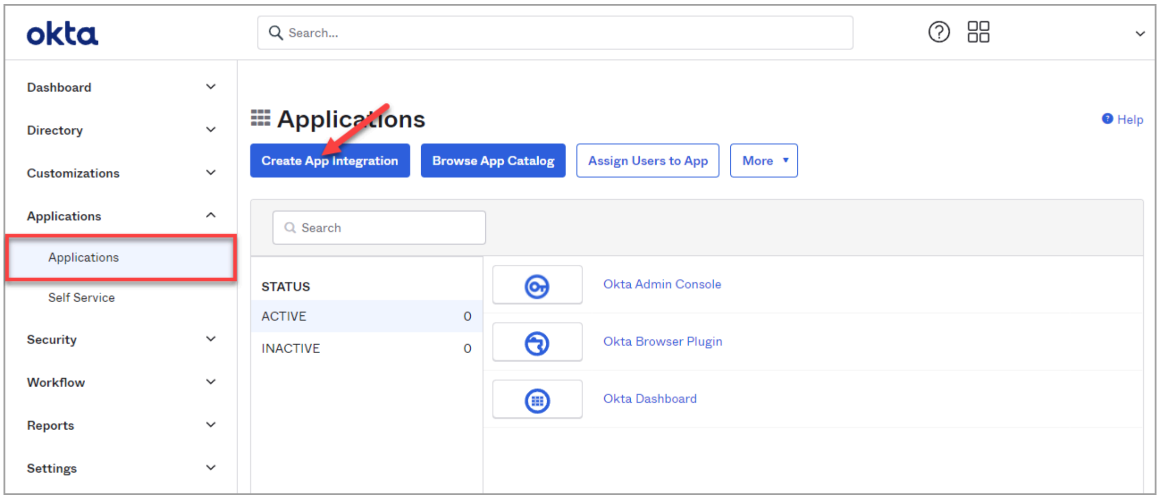
Allow applications starting from version (backward compatibility): 5.10.0.0

2 - Preparing Okta

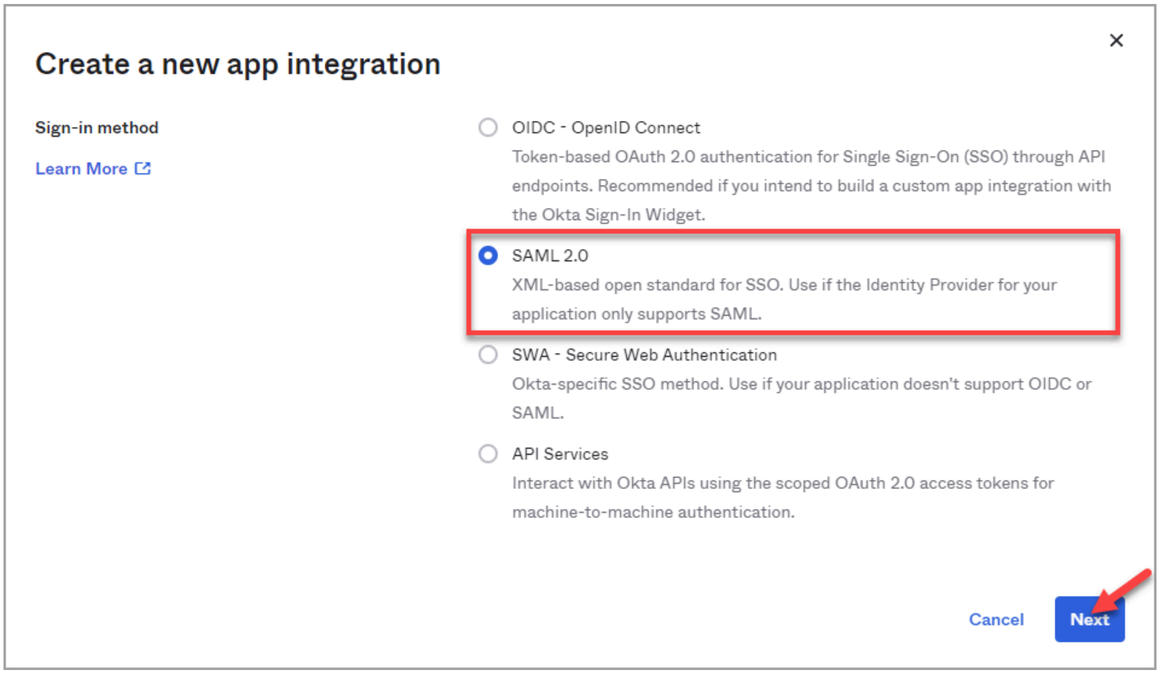
Before completing these steps in the Okta Admin Console, you must meet all of the following prerequisites:

- Have an Okta administrator account.
- Have provisioned at least one user.
- Have provisioned at least one user group that contains the users you want to grant access to Security Center.

1. In the Okta Admin Console, select **Applications** > **Applications** and then click **Create App Integration**.



2. In the *Create a new app integration* wizard, select **SAML 2.0** and click **Next**.



Create a new app integration

Sign-in method

Learn More

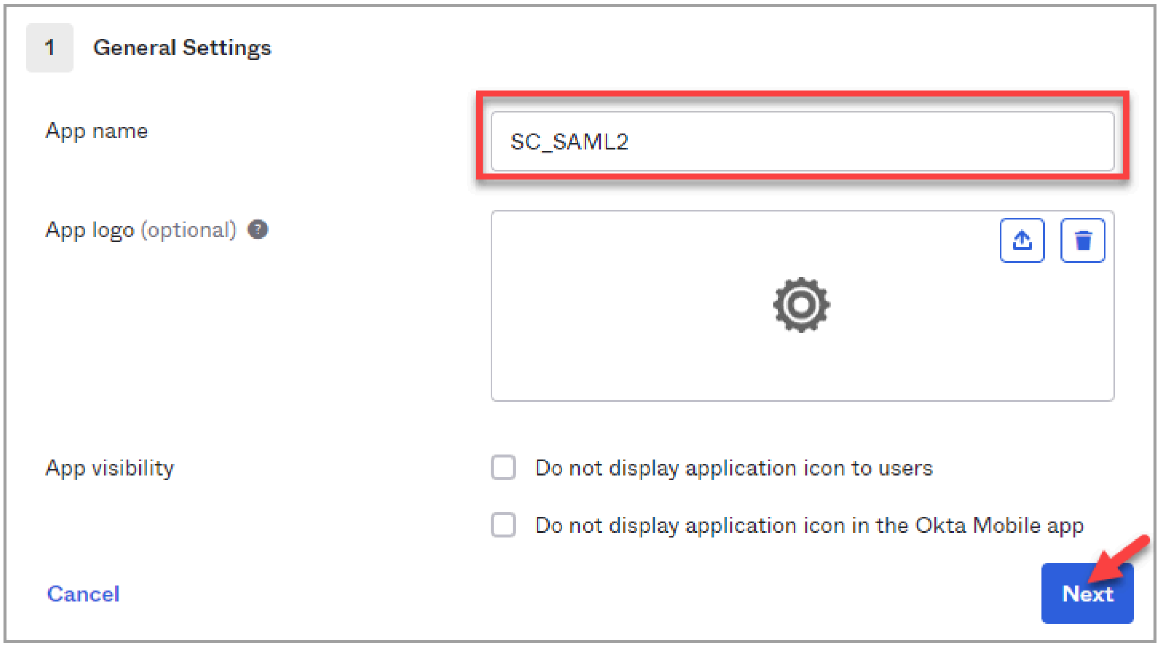
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

3. In the *Create SAML Integration* wizard, enter the **App name** and click **Next**.



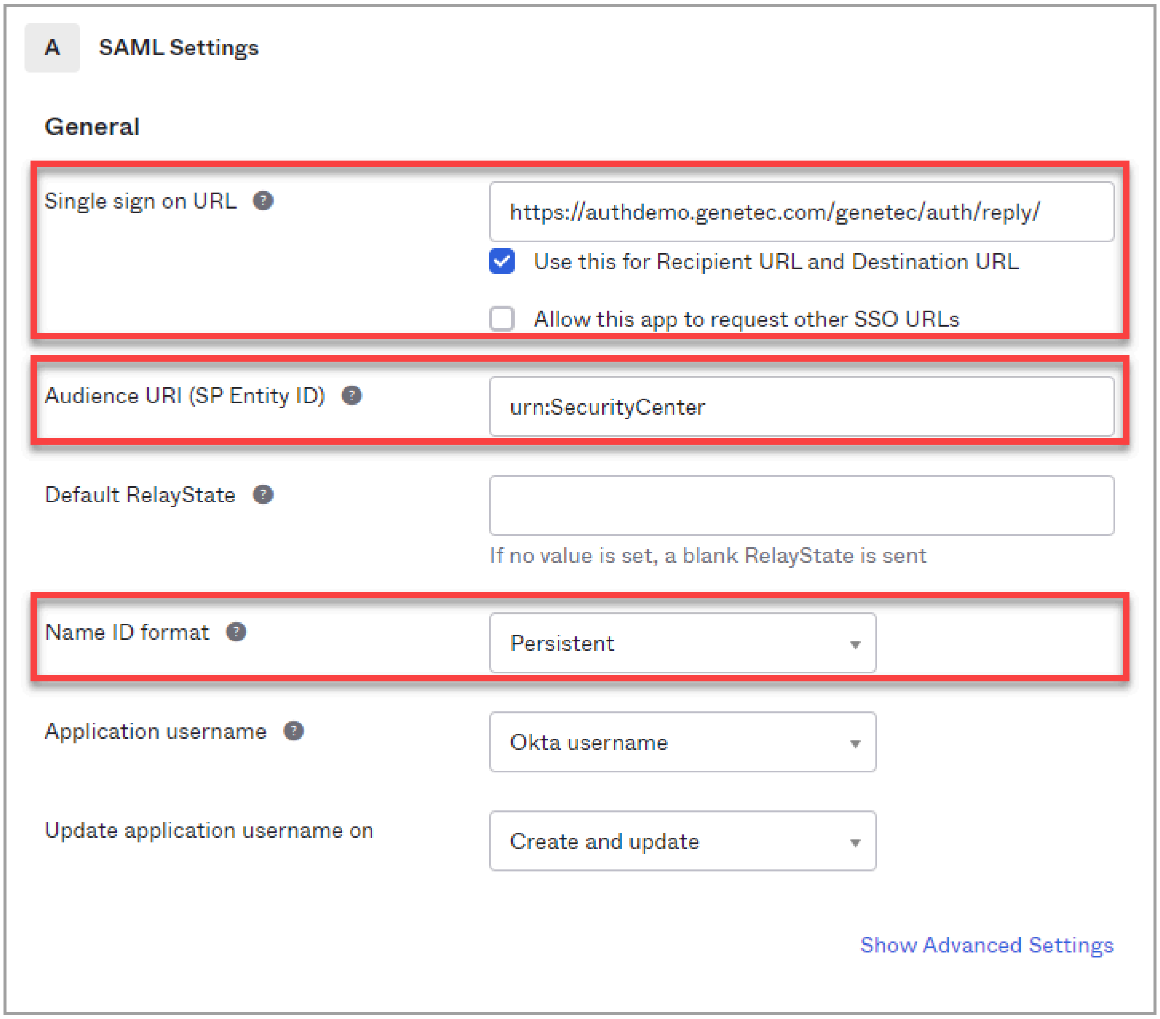
1 General Settings

App name: SC_SAML2

App logo (optional)

App visibility
□ Do not display application icon to users
□ Do not display application icon in the Okta Mobile app

4. On the *Configure SAML* page, set the following:
   - **Single sign on URL** copied from the *redirect* URIs in Security Center

     NOTE: If more than one URI is required, select **Allow this app to request other SSO URLs** and enter the additional URIs as needed.
   - **Audience URI (SP Entity ID)** enter `urn:SecurityCenter`
   - **Name ID format** select **Persistent**
   - 

A SAML Settings

General

Single sign on URL: https://authdemo.genetec.com/genetec/auth/reply/

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): urn:SecurityCenter

Default RelayState:

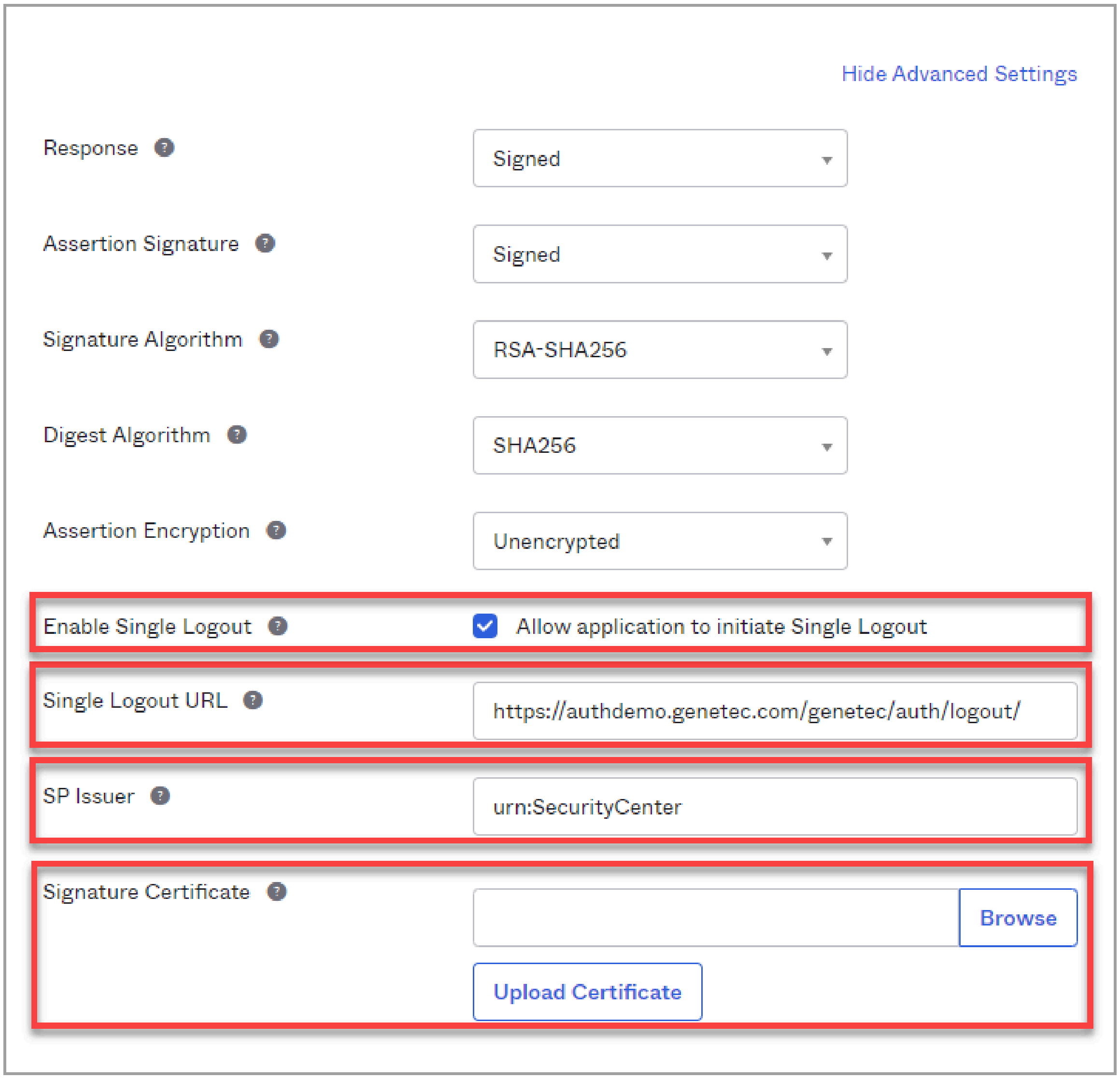
If no value is set, a blank RelayState is sent

Name ID format: Persistent

Application username: Okta username

Update application username on: Create and update

5. Still in the *SAML Settings* section, click **Show Advanced Settings** and set the following:
   - **Enable Single Logout**
   - **Single Logout URL** the */genetec* endpoint copied from the *logout* URIs in Security Center
   - **SP Issuer** enter `urn:SecurityCenter`
   - **Signature Certificate** upload the public key certificate exported from Security Center



Response: Signed

Assertion Signature: Signed

Signature Algorithm: RSA-SHA256

Digest Algorithm: SHA256

Assertion Encryption: Unencrypted

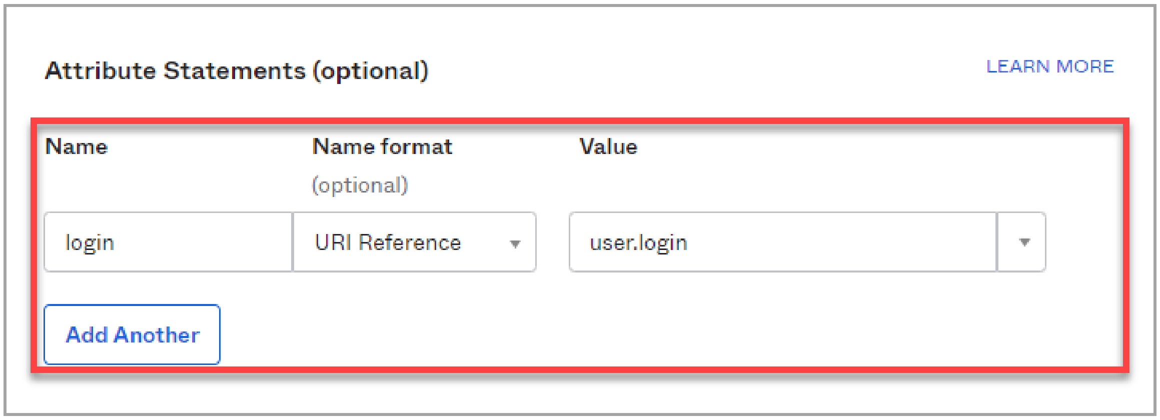
Enable Single Logout: ☑ Allow application to initiate Single Logout

Single Logout URL: https://authdemo.genetec.com/genetec/auth/logout/

SP Issuer: urn:SecurityCenter

Signature Certificate:

6. In the *Attribute Statements* section, set the following:
   - **Name:** `login`
   - **Name format: URI Reference**
   - **Value:** `user.login`



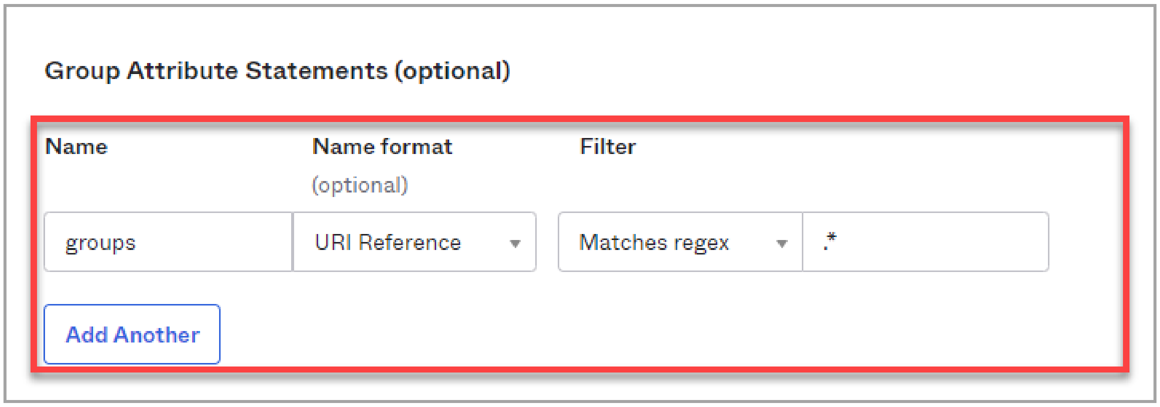
Attribute Statements (optional)

Name	Name format (optional)	Value
login	URI Reference	user.login

7. In the *Group Attribute Statements* section, set the following:
   - **Name:** `groups`
   - **Name format: URI Reference**
   - **Filter: Matches regex** `.*`

     NOTE: The *Matches regex* filter with .* returns all groups to which the authenticated user belongs.

     If required, the filter can also be used to exclude certain groups. At least one group assigned to Security Center must be included to grant access.

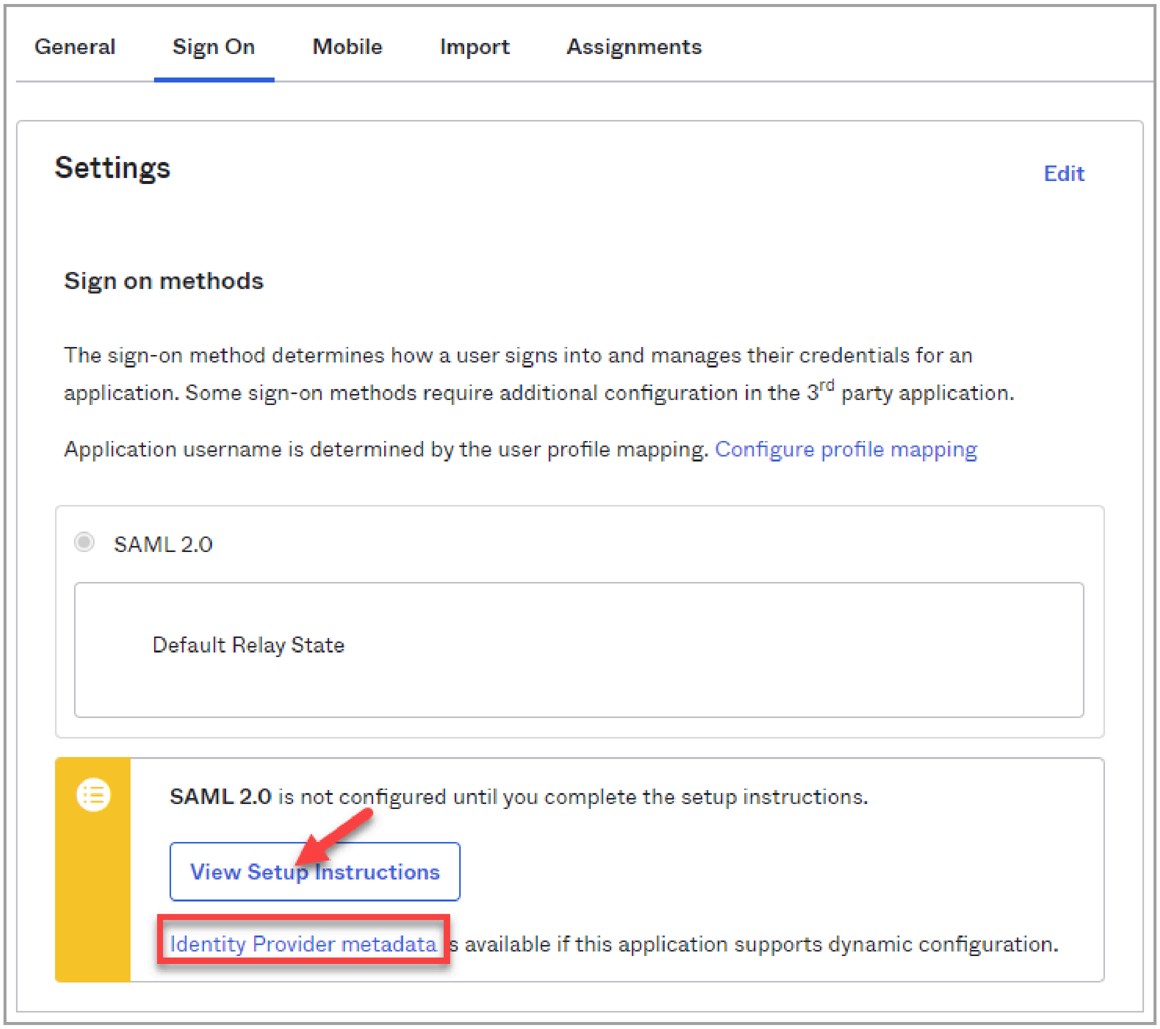


Group Attribute Statements (optional)

Name	Name format (optional)	Filter	
groups	URI Reference	Matches regex	.*

8. Click **Next**.
9. On the *Feedback* page, select **I'm an Okta customer adding an internal app**, provide optional feedback, and click **Finish**.

10. On the *Sign On* page for your application, do the following:
    a. Copy the **Identity Provider metadata** URL. This is the **Metadata URL** required by the Authentication Service role in Security Center.
    b. Click **View Setup Instructions**.



Settings

Sign on methods

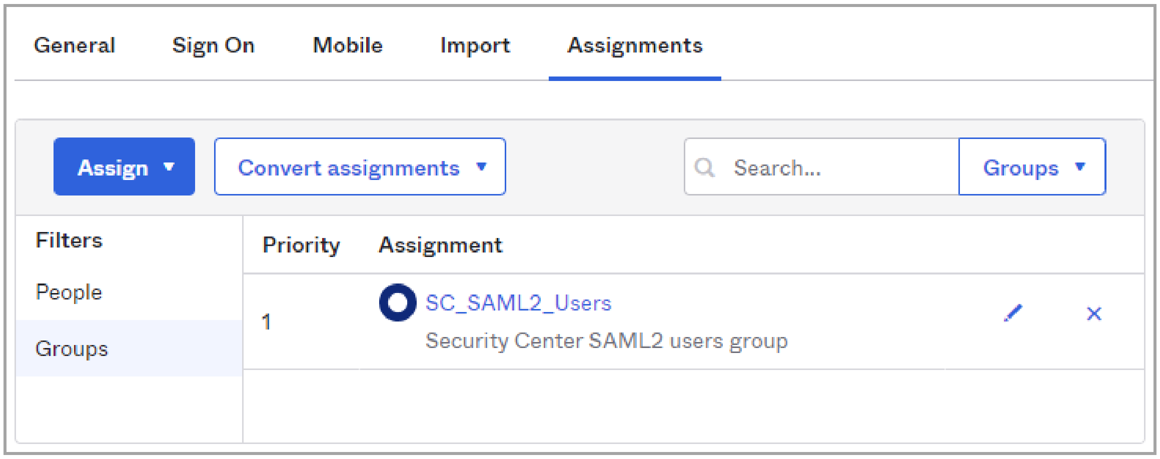
The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

11. On the *How to Configure SAML 2.0 for <application>* page, download the **X.509 Certificate**.
12. On the *Assignments* page for your application, assign the Security Center user groups to the application.



Priority	Assignment
1	SC_SAML2_Users Security Center SAML2 users group

3 - Integrating Security Center with Okta

1. On the Security Center main server, follow the instructions for your operating system to import the Okta certificate.

   NOTE: You might need to restart Windows for the certificate to take effect.
2. In Config Tool, open the Authentication Service role that was created earlier, and click the **Properties** tab.
3. Complete the properties as follows:
   - **Display name:** When logging on to Security Center, third-party authentication options are each presented as a button with the text "Sign in with <*display name*>".
   - **Metadata URL:** Enter the *Identity Provider metadata* URL that was copied from Okta.
   - **Audience:** `urn:SecurityCenter`
   - **Domain names:** The domain names of users who will authenticate using Okta, such as `genetec.com`. You must have at least one.
   - **Username assertion:** `login`
   - **Group assertion:** `groups`

   Leave all other properties with the default value.
4. Click **Apply**.
5. Create one or more user groups with the exact same name as the groups assigned to the Security Center application in Okta.
6. Add groups authorized to connect using Okta to the *User groups* list in Authentication Service role.

Importing user groups from a CSV file for third-party authentication

Importing user groups from a CSV file simplifies the process of creating Security Center user groups for third-party authentication

Before you begin

The user groups that interact with Security Center have been defined in the external identity provider.

What you should know

Some identity providers, such as Azure Active Directory, can export user groups in CSV format. Security Center can import data from these files to ensure accuracy and save time.

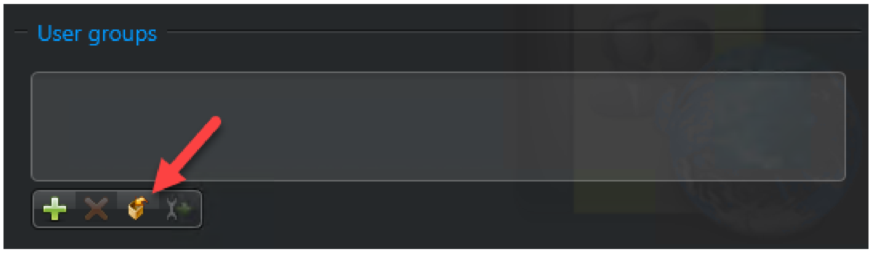
Compatible CSV files must be formatted as follows:

- First row includes only headers.
- All headers must be unique.
- At least one column must be for group name. It is the only mandatory field.

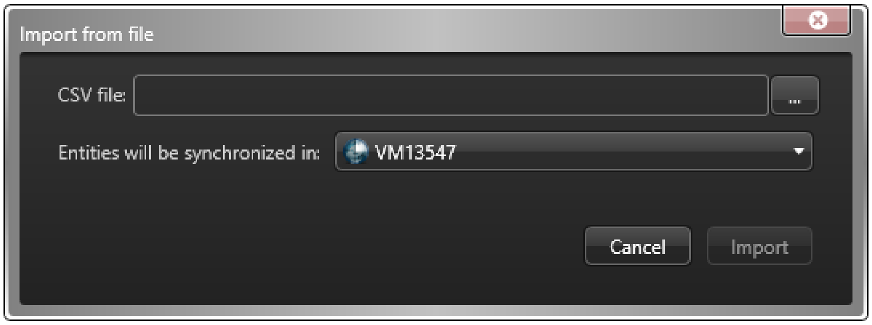
To import user groups from a CSV file:

1 From the Config Tool home page, open **System** > **Roles** and select an Authentication Service role that uses the OpenID or SAML2 protocols.

2 Click the **Properties** tab, and then click the **Import** button under *User groups*.



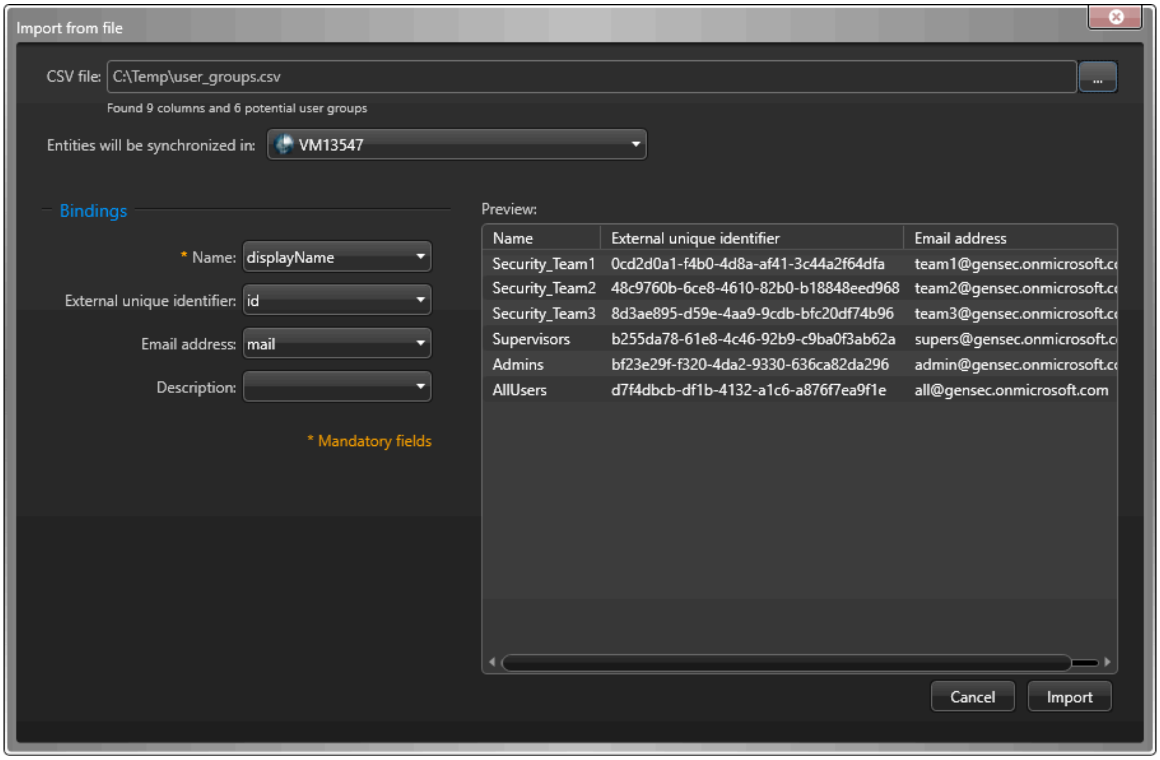
The *Import from file* window opens.



NOTE: If multiple partitions are defined in Security Center, new user groups imported from the CSV file are created in the partition specified under *Entities will be synchronized in*.

3 Select a CSV file to import.

The CSV is parsed immediately and any detected rows, columns, errors, and warnings are displayed.



Import from file

CSV file: C:\Temp\user_groups.csv

Found 9 columns and 6 potential user groups

Entities will be synchronized in: VM13547

Bindings

* Name: displayName

External unique identifier: id

Email address: mail

Description:

* Mandatory fields

Preview:

Name	External unique identifier	Email address
Security_Team1	0cd2d0a1-f4b0-4d8a-af41-3c44a2f64dfa	team1@gensec.onmicrosoft.c
Security_Team2	48c9760b-6ce8-4610-82b0-b18848eed968	team2@gensec.onmicrosoft.c
Security_Team3	8d3ae895-d59e-4aa9-9cdb-bfc20df74b96	team3@gensec.onmicrosoft.c
Supervisors	b255da78-61e8-4c46-92b9-c9ba0f3ab62a	supers@gensec.onmicrosoft.c
Admins	bf23e29f-f320-4da2-9330-636ca82da296	admin@gensec.onmicrosoft.c
AllUsers	d7f4dbcb-df1b-4132-a1c6-a876f7ea9f1e	all@gensec.onmicrosoft.com

By default, user group fields are bound to CSV headers as follows:

- **Name** is bound to the displayName header.
- **External unique identifier** is bound to the id header.
- **Email address** is bound to the mail header.
- **Description** is bound to the description header.

NOTE: A warning is displayed if the columns bound to **Name** or **External unique identifier** have duplicate or empty values. These rows are skipped during the import process.

4 If required, specify a different partition for new user groups.

NOTE: This selection is only available if multiple partitions are defined in Security Center. Only user groups created by the CSV import are placed in the selected partition. Existing user groups are not affected by this setting.

5 If required, modify the field bindings.

You cannot bind the same header to multiple fields.

6 Click **Import**.

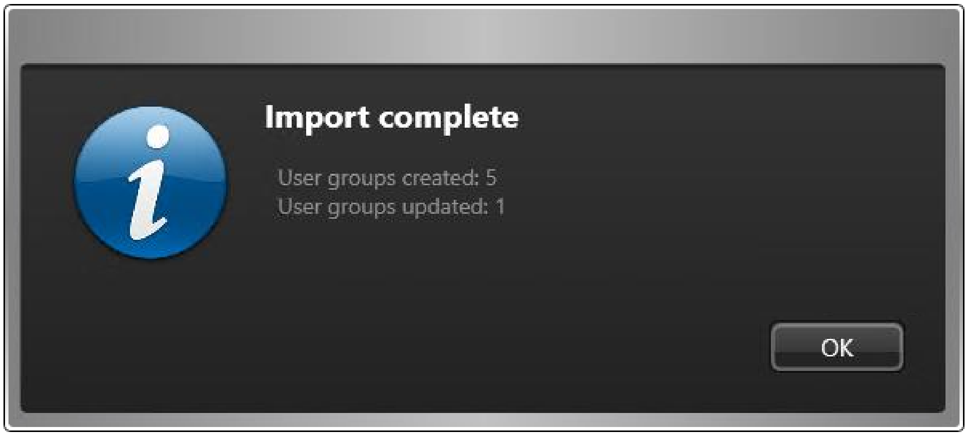
The user groups specified in the CSV file are imported to Security Center.

During the import, the system looks for an existing user groups with a matching Name that is not associated with another Authentication Service role. User groups are then processed as follows:

- If a matching group is not found, a new user group is created with data from the CSV.
- If a matching group is found, and that group is not associated with another Authentication Service role, it is updated with data from the CSV.
- If a matching group is found, and that group is associated with another Authentication Service role, a new group is created with data from the CSV.
- If a group that is already associated with this Authentication Service role has the same external identifier as a CSV row, the matching CSV row is skipped.

Depending on the number of groups to process, it can take few seconds for the import to complete.

The CSV file is imported and results are displayed.



Import complete

User groups created: 5
User groups updated: 1

All imported groups are automatically added to the **User groups** list in the Authentication Service role.

7 Click **OK**.

Related Topics

OpenID Connect Integration overview on page 493
SAML 2.0 Integration overview on page 515

Deploying third-party authentication through ADFS using WS-Federation or WS-Trust

You can use an Active Directory Federation Services (ADFS) server as an identity provider for Security Center, and allow users outside your company to log on by establishing a trust chain from third-party ADFS servers to the Security Center main server.

Before you begin

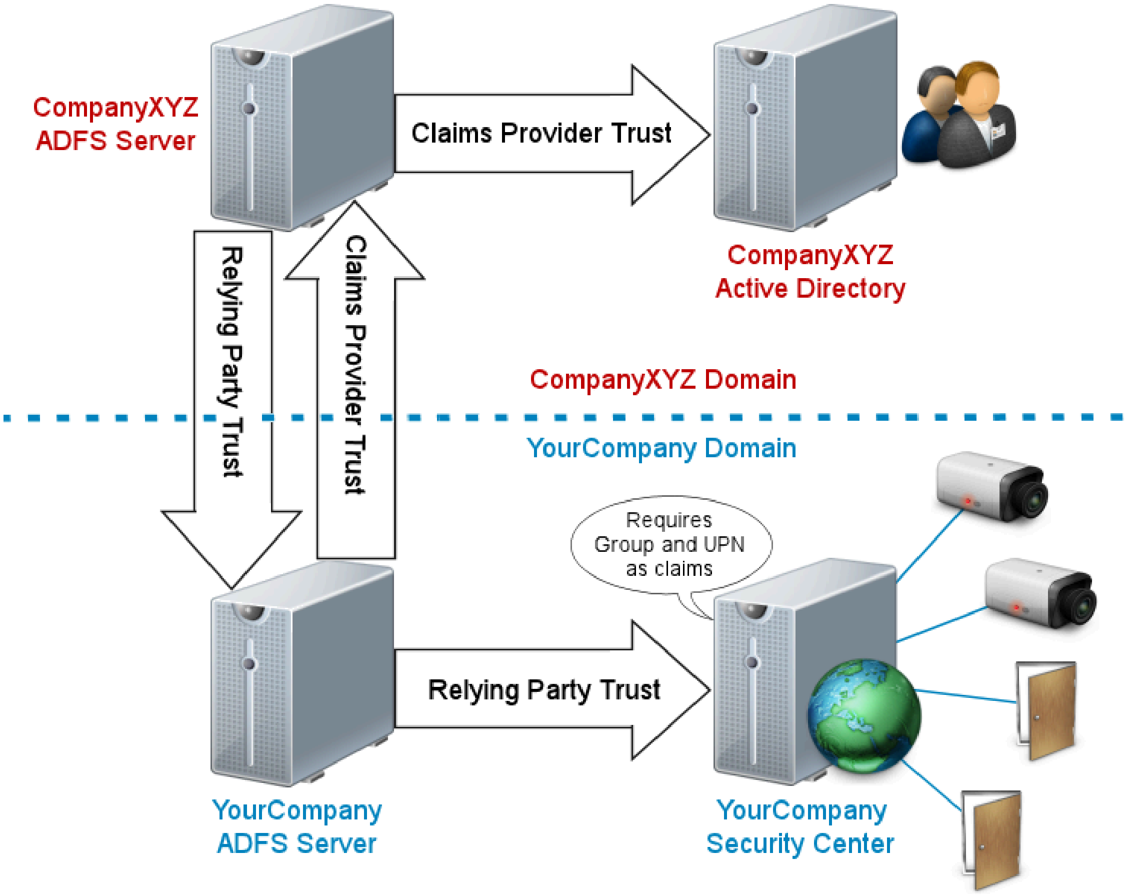
- Be familiar with the concepts of third-party authentication.
- Ensure that your *ADFS* server is operational. For general information on ADFS installation and configuration, refer to the documentation for your version of the product software.

What you should know

This deployment process uses the following a sample scenario:

- Users from Company XYZ must access your Security Center system.
- Company XYZ servers are not on the same domain as your servers.
- Company XYZ has an ADFS server using WS-Trust or WS-Federation that relies on Active Directory as the *identity provider*.

For external users from Company XYZ to access Security Center, a chain of trusts must be established from the Active Directory of Company XYZ to the main server of your Security Center system, as follows:



NOTE: Security Center requires specific attributes as *claims*: *Group* and *UPN (User Principal Name)*.

BEST PRACTICE: If you want to use security groups from your local Active Directory as Security Center user groups, do not federate them through an Authentication Service role, but import them from Active Directory instead. Importing from Active Directory offers more functionality, such as synchronizing all standard fields (first name, last name, email address, and so on), custom field mapping, and the option to create all users during role synchronization.

To deploy third-party authentication through ADFS using WS-Trust or WS-Federation:

1. Company XYZ must add a relying party trust to their ADFS server for your ADFS server.
2. Configure your local ADFS server as follows:
   a) Add a claims provider trust for the third-party ADFS server.
   b) Configure the claim rules for the third-party claims provider.
   c) Add a relying party trust for Security Center.
   d) Configure the claim rules for Security Center.
3. Configure Security Center to perform third-party authentication through ADFS.
   a) Connect to your Security Center system with Config Tool.
   b) Create a user group for each ADFS group you accept as Security Center user group.
   c) Create an Authentication Service role for third-party authentication using WS-Trust or WS-Federation.

Incoming users can now be authenticated by ADFS.

NOTE: External users who must be authenticated by ADFS using the WS-Trust protocol must append their domain name to the end of their username, such as `Username@CompanyXYZ.com`, on the Security Center logon screen.

IMPORTANT: There is currently a known issue regarding the use of a local Active Directory and ADFS. When you have external users authenticated through ADFS in your system, all users imported from your local Active Directory must also use fully qualified user names, even though they belong to the same domain as your Security Center system.

Configuring claim rules for a third-party claims provider

Claim rules specify which claims must be forwarded to your ADFS server for use by local applications.

Before you begin

A claims provider trust for the third-party ADFS server has been added to your ADFS server.

NOTE: Adding a claims provider trust is outside the scope of this document. For more information on working with ADFS, refer to the documentation for your version of the product software.

What you should know

This task is part of the deployment process for third-party authentication using ADFS based on a sample scenario. The instructions and screen captures are based on Windows Server 2016. If you are using a different version, your procedure might be different.

NOTE: Security Center requires specific attributes as *claims*: *Group* and *UPN (User Principal Name)*.

To configure claim rules:

1. In the *AD FS* window, click **Trust Relationships** > **Claims Provider Trusts**, select the claims provider that corresponds to the third-party ADFS, and click **Edit Claim Rules** in the *Actions* pane.

   The *Edit Claims Rules* window opens.

2 If no claim rule exists for **UPN**, add one.
   a) Click **Add Rule**.
   b) In the **Claim rule template** list, select **Pass Through or Filter an Incoming Claim**, and click **Next**.
   c) Configure the rule and click **Finish**.
      - **Claim rule name:** Enter a name that helps you remember the rule.
      - **Incoming claim type:** Select **UPN**.
      - **Pass through only claim values that match a specific email suffix value:** Select this option, and enter an email suffix value. For example: `CompanyXYZ.com`.

        BEST PRACTICE: It is recommended to filter the claims coming from a third-party claims provider as a security precaution, so that the third-party claims provider cannot send unexpected values. This is done, for example, to prevent Company XYZ from pretending that its users are from your company, and get elevated privileges. **Pass through all claim values** should be avoided when dealing with third-party claims providers.

3 If no claim rule exists for **Group**, add one.
   a) Click **Add Rule**.
   b) In the **Claim rule template** list, select **Pass Through or Filter an Incoming Claim**, and click **Next**.
   c) Configure the rule and click **Finish**.
      - **Claim rule name:** Enter a name that helps you remember the rule.
      - **Incoming claim type:** Select **Group**.
      - **Pass through only claim values that start with a specific value:** Select this option, and enter a start value. For example: `CompanyXYZ\` or `CompanyXYZ.com\`. Ask your IT department which form should be used.

4 Click **Apply**.

After you finish

Add a relying party trust for Security Center.

Adding a relying party trust for Security Center

For an ADFS server to act as the claims provider for your Security Center system, you must add Security Center to the relying party trusts of the ADFS server.

Before you begin

- The *AD FS Management* window must be open on your ADFS server.
- If Directory failover is configured on your system, know the hostname of each Directory server.

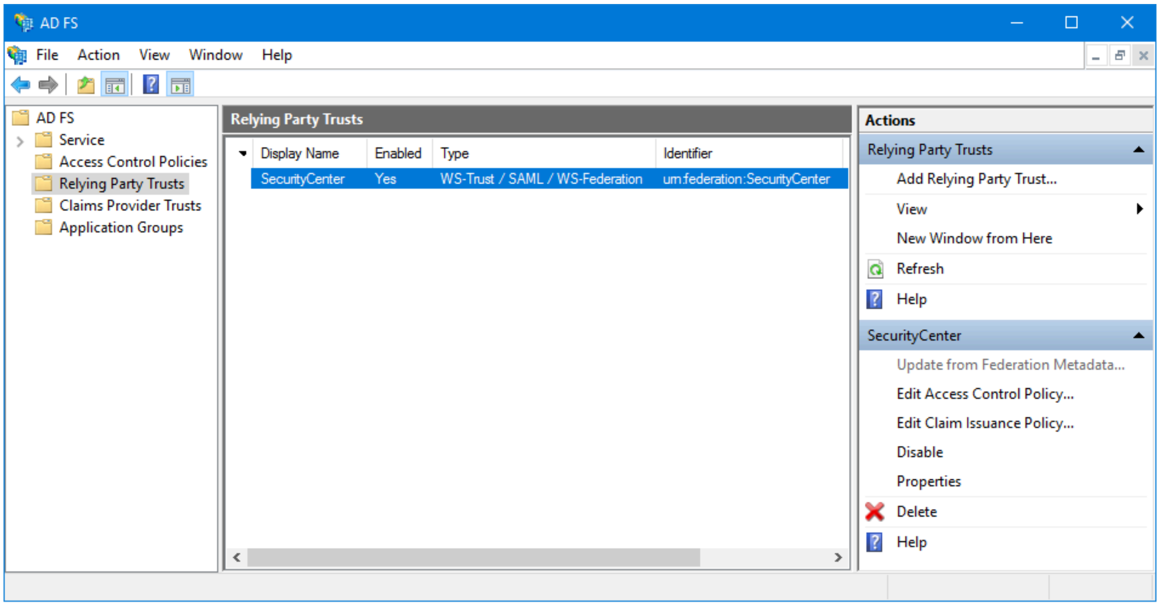
What you should know

This task is part of the deployment process for third-party authentication using ADFS based on a sample scenario. The instructions and screen captures are based on Windows Server 2016. If you are using a different version, your procedure might be different.

NOTE: If you are not enabling *web-based authentication*, click **Next** instead of executing the steps that are marked "(WbA only)".

To add a relying party trust to your ADFS server for Security Center:

1 In the *AD FS* window, click **Relying Party Trusts** > **Add Relying Party Trust**.



The *Add Relying Party Trust Wizard* window opens

2 On the *Welcome* page, click **Start** > **Enter data about the relying party manually** > **Next**.

You can leave **Claims aware** selected.

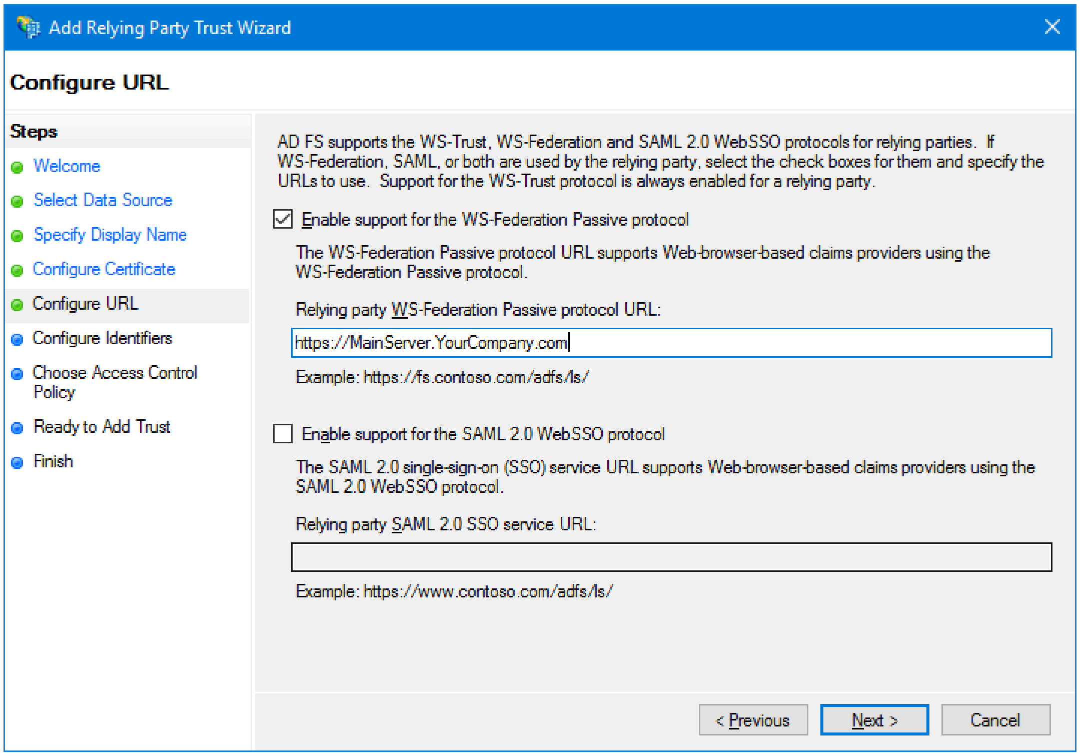
3 On the *Specify Display Name* page, enter in the **Display name** field, a name that represents your Security Center system, and click **Next**.

For example, `YourCompany Security Center`.

4 (Optional) On the *Configure Certificate* page, specify a token encryption certificate and click **Next**.

5 (WbA only) On the *Configure URL* page, select **Enable support for the WS-Federation Passive protocol** and enter the URL of your Security Center *main server*, and then click **Next**.

For example: `https://MainServer.YourCompany.com`



AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☑ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

https://MainServer.YourCompany.com

Example: https://fs.contoso.com/adfs/ls/

☐ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

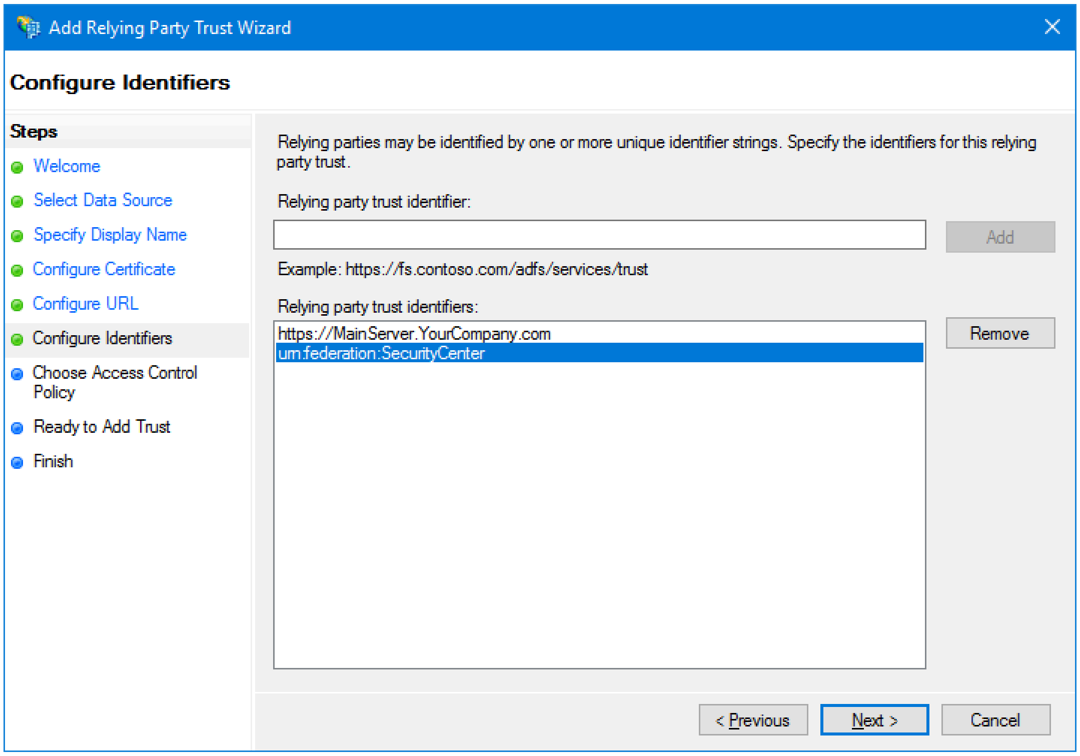
Relying party SAML 2.0 SSO service URL:

Example: https://www.contoso.com/adfs/ls/

6 (WbA only) On the *Configure Identifiers* page, enter in the **Relying party trust identifier** field, a string that identifies your Security Center main server, and click **Add**.

IMPORTANT: An example would be to use the URL of your main server: `https://MainServer.YourCompany.com`. Write this value down. You need to enter this identifier in a subsequent step, when you configure the Authentication Service role on the Security Center server.

BEST PRACTICE: We recommend using the default value configured for the Authentication Service role, `urn:federation:SecurityCenter`, so you have one less thing to remember.



Add Relying Party Trust Wizard

Configure Identifiers

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

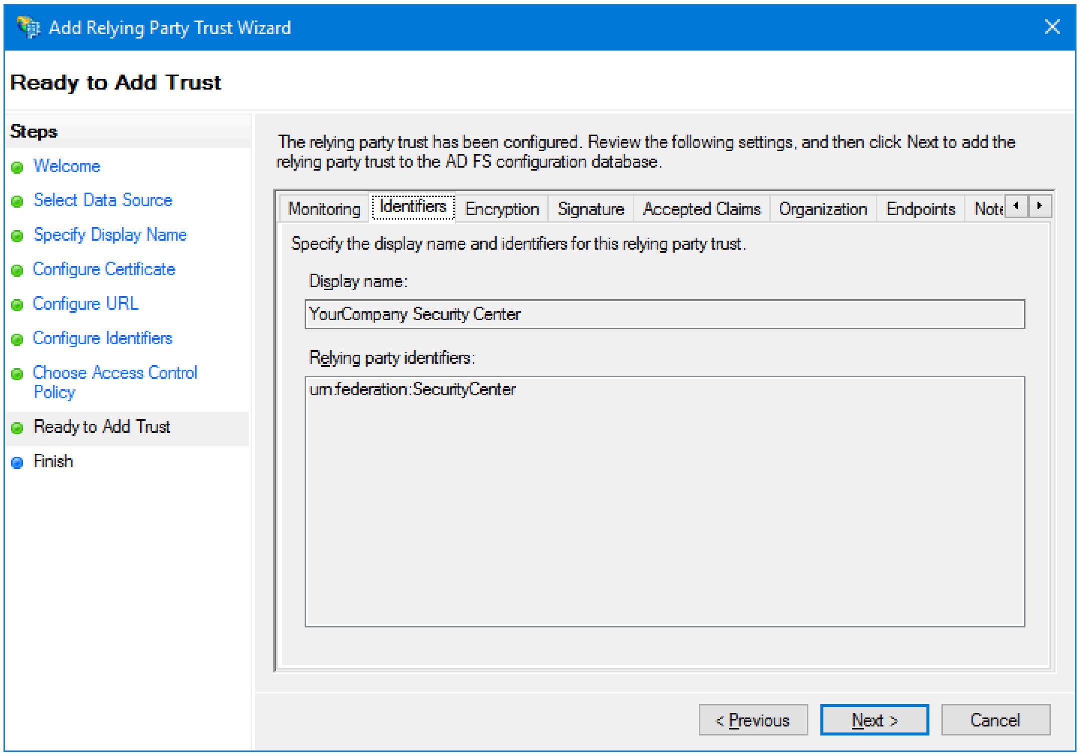
Relying party trust identifiers:

https://MainServer.YourCompany.com
urn:federation:SecurityCenter

7 (WbA only) In the **Relying party trust identifiers** list, select the row that corresponds to your main server URL and click **Remove** > **Next**.

8 In the *Choose Access Control Policy* page, select **Permit everyone** and click **Next**.

9 In the *Ready to Add Trust* page, click **Identifiers**, and verify the identifiers you entered.



The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the display name and identifiers for this relying party trust.

Display name:

YourCompany Security Center

Relying party identifiers:

urn:federation:SecurityCenter

10 Click **Next**, leave **Configure claims issuance policy for this application** selected, and click **Close**.

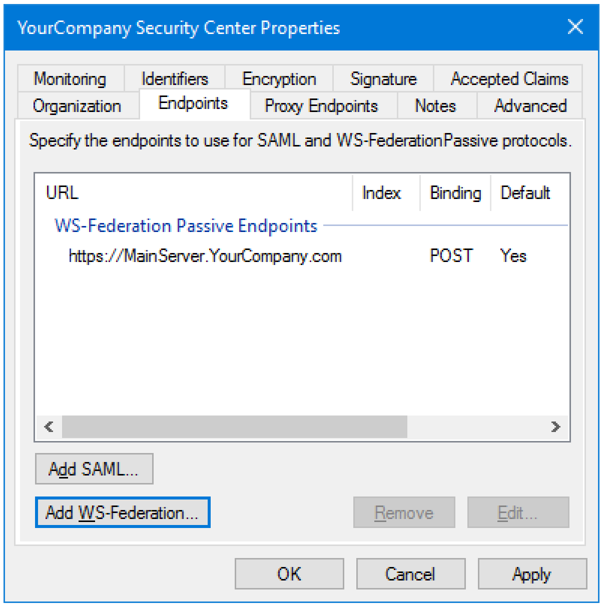
The Security Center main server is added to the relying party trusts of your ADFS server.

11 If Directory failover is configured on your system, you must add the URL of each Directory server as endpoints to the Security Center relying party trust of your ADFS server.

NOTE: The Authentication Service role runs on the same server as the Directory role. When the Directory role fails over to the next server in line, the Authentication Service role also fails over to the same server.

For this reason, the ADFS server must know the URL of every Directory server you have in your system. For the server URL, enter `https://` followed by the fully qualified hostname.

a) In the *AD FS* window, select the Security Center relying party trust, and click **Properties** > **Endpoints**.

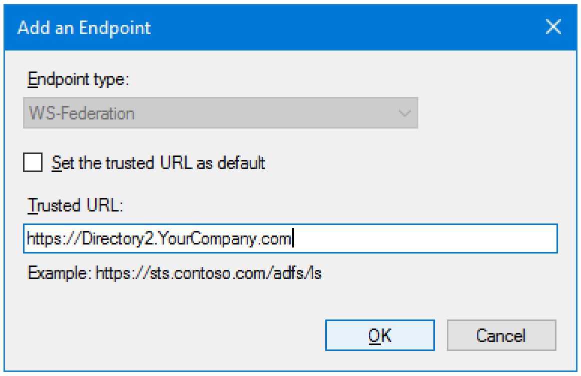


YourCompany Security Center Properties

Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default
WS-Federation Passive Endpoints			
https://MainServer.YourCompany.com		POST	Yes

b) Click **Add WS-Federation**, enter the URL for each of a Directory server, and click **OK**.



Add an Endpoint

Endpoint type: WS-Federation

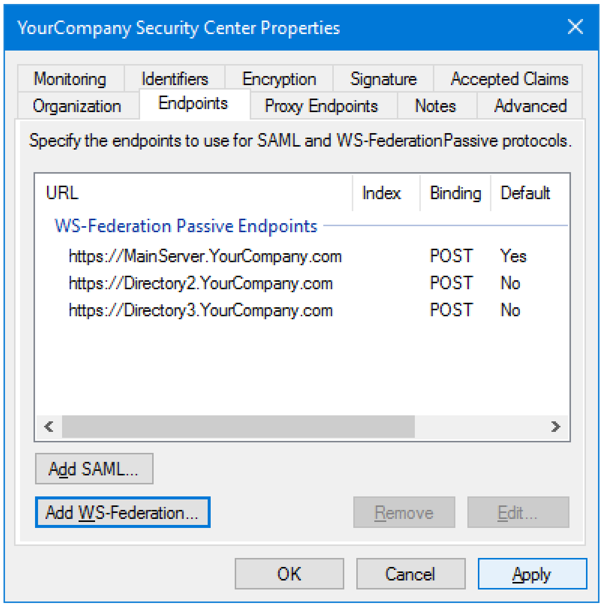
☐ Set the trusted URL as default

Trusted URL: https://Directory2.YourCompany.com

Example: https://sts.contoso.com/adfs/ls

c) Repeat the previous step for all Directory servers on your system.

d) Click **Apply** > **OK**.



Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default
WS-Federation Passive Endpoints			
https://MainServer.YourCompany.com		POST	Yes
https://Directory2.YourCompany.com		POST	No
https://Directory3.YourCompany.com		POST	No

After you finish

Configure claim rules for Security Center.

Configuring claim rules for Security Center

Claim rules for the Security Center relying party trust specify which claims Security Center requires.

Before you begin

- The *AD FS Management* window must be open on your ADFS server.
- A relying party trust for Security Center must be added to the ADFS server.
- This task is part of the deployment process for third-party authentication using ADFS based on a sample scenario. The instructions and screen captures are based on Windows Server 2016. If you are using a different version, your procedure might be different.

To configure claim rules for Security Center:

1 In the *AD FS* window, click **Relying Party Trusts**, select the relying party that corresponds to your Security Center system, and click **Edit Claim Issuance Policy** in the *Actions* pane.

The *Edit Claim Issuance Policy* window opens.

2 If no claim rule exists for **UPN**, add one.

a) Click **Add Rule**.

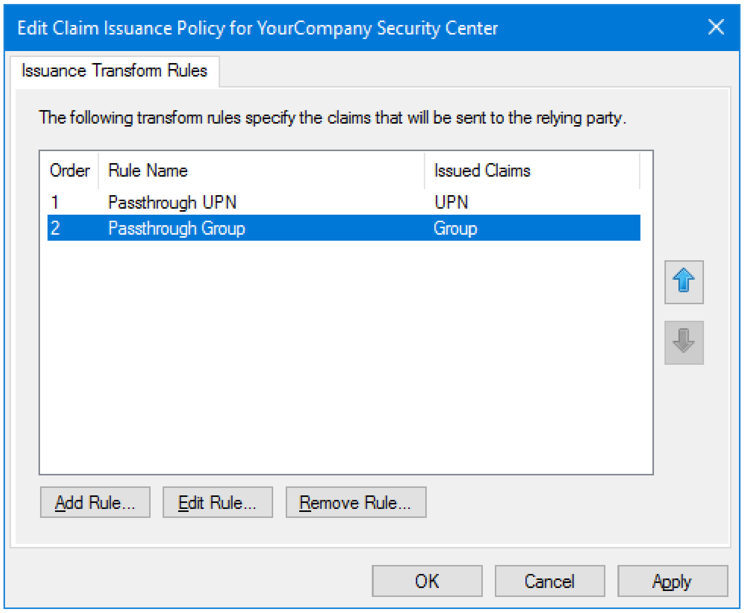
b) In the **Claim rule template** list, select **Pass Through or Filer an Incoming Claim**, and click **Next**.

c) Configure the rule and click **Finish**.

- **Claim rule name:** Enter a name that helps you remember the rule.
- **Incoming claim type:** Select **UPN**.
- **Pass through all claim values:** Select this option.

3 If no claim rule exists for **Group**, add one.

Follow the instructions for UPN claim rule. Only this time, change **UPN** to **Group**.



Edit Claim Issuance Policy for YourCompany Security Center

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Passthrough UPN	UPN
2	Passthrough Group	Group

4 Click **Apply** > **OK**.

After you finish

Map remote ADFS groups to user groups in Security Center.

Mapping remote ADFS groups to Security Center

To accept remote ADFS groups as valid user groups in Security Center, you must create a Security Center user group for each of them.

Before you begin

All ADFS servers involved in the trust chain must be fully configured.

To map accepted ADFS groups to Security Center:

1 Create a user group for each ADFS group you want to accept in Security Center.

The Security Center user groups must have the exact same name as the groups defined in the remote Active Directory, followed by the remote ADFS domain name.

For example, if the company XYZ domain has a user group called *Operators*, the user group in Security Center must be named *Operators@CompanyXYZ.com*.

2 Apply the required access rights and privileges to these user groups.

After you finish

Add the mapped user groups to the list of Accepted user groups in the Authentication Service role.

Creating Authentication Service roles for WS-Federation or WS-Trust

For Security Center to receive claims from an ADFS server using the WS-Trust or WS-Federation protocols, you must create and configure an Authentication Service role.

Before you begin

- All ADFS servers involved in the trust chain are fully configured.
- ADFS groups have been mapped to Security Center user groups.

What you should know

The Authentication Service role connects Security Center to an external identity provider for third-party authentication.

You must create one Authentication Service role for WS-Trust or WS-Federation in Security Center for each root ADFS. In our sample scenario, the local ADFS server is the root ADFS, therefore only one Authentication Service role is needed.

If you do not have a local ADFS server, but multiple independent third-party ADFS servers acting as identity providers for Security Center, then you need to create one Authentication Service role for each of them.

To create an Authentication Service role:

1 From the Config Tool homepage, open the *System* task and click the **Roles** view.

2 Click **Add an entity** (➕) > **Authentication Service**.

3 On the *Specific info* page, select **WS-Federation or WS-Trust**, and click **Next**Test.
NOTE: These protocols can only be selected at role creation.

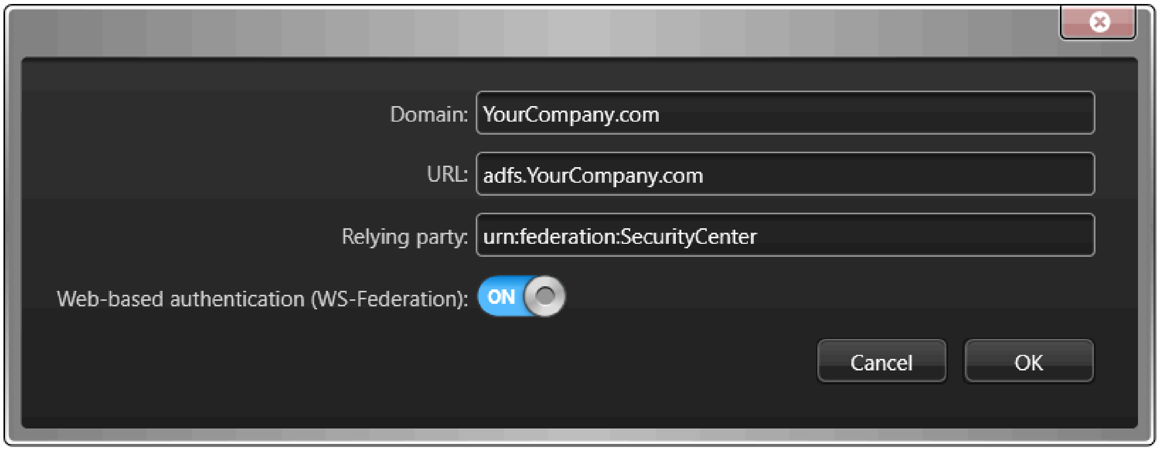
4 In the *Basic information* page, enter a name and description for the role.

5 Select a **Partition** this role is a member of, and click **Next**.
Partitions determine which Security Center users have access to this entity. Only users who have been granted access to the partition can see the ADFS role.

6 Click **Next** > **Create** > **Close**.
A new Authentication Service role (🌐) is created.

7 Click the **Properties** tab, and configure the **Trust chain (domains)**.

a) Click **Add an item** (➕), configure the local ADFS server, and click **OK**.



Domain: YourCompany.com

URL: adfs.YourCompany.com

Relying party: urn:federation:SecurityCenter

Web-based authentication (WS-Federation): ON

- **Domain:** This is the domain of your local ADFS server. Example: `YourDomain.com`.
- **URL:** This is the address of the metadata document for your ADFS server. It is always in the following format: `adfs.YourCompany.com`

Replace `YourCompany.com` with the name of your ADFS server.

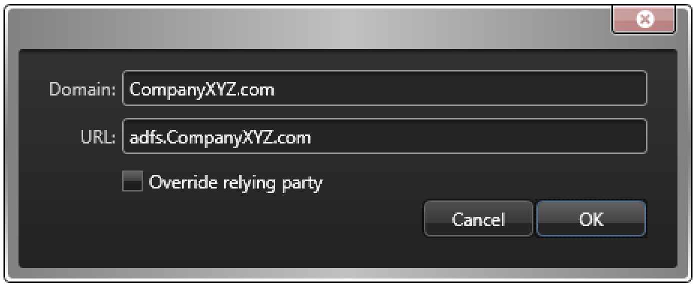
Security Center

- **Relying party:** This is the identifier that was entered as the **Relying party identifier** when you added the relying party trust for Security Center.

  The relying party identifier is how Security Center identifies itself to the ADFS server, even when the role fails over to another server.
- **Web-based authentication (WS-Federation):** Select this option to enable *web-based authentication* (default=OFF).

  IMPORTANT: Supervised user logon does not work if you enable web-based authentication, because the user authentication is handled outside of .

b) Click **Add an item** (➕), configure the remote ADFS server, and click **OK**.



Domain: CompanyXYZ.com

URL: adfs.CompanyXYZ.com

□ Override relying party

- **Domain:** This is the domain of the remote ADFS server. Example: `CompanyXYZ.com`. Users from that domain must append the domain to their usernames when they log on to Security Center. Example: `johnny@CompanyXYZ.com`.
- **URL:** This is the address of the remote ADFS server's metadata document. It is always in the following format: `adfs.CompanyXYZ.com`

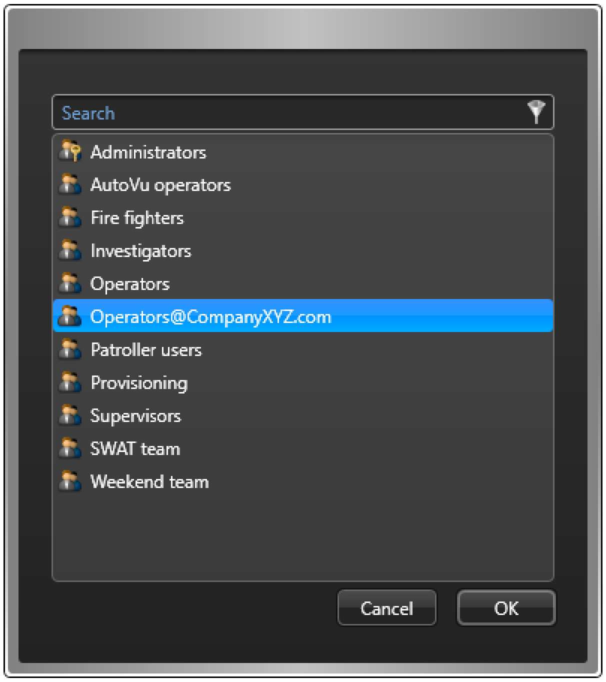
  Replace `CompanyXYZ.com` with the name of the remote ADFS server.
- **Override relying party:** (Advanced setting) Select this option if the claims provider on this domain expects a different audience in the token request made by the relying party, and enter the value it expects.

c) If you configured more than one remote ADFS servers as claims providers to your local ADFS server, add them now.

8 Configure the external user groups that Security Center is going to accept.

a) In the *Accepted user groups* section, click **Add an item** (➕).

b) In the dialog box that opens, select the user groups mapped to the remote ADFS groups, and click **OK**.



Users who are members of the accepted user groups can log on to your system. Security Center does not keep nor validate their passwords. The ADFS server does. Security Center simply trusts them as authentic users if the ADFS accepts them.

NOTE: External users who must be authenticated by ADFS using the WS-Trust protocol must append their domain name to the end of their username, such as `Username@CompanyXYZ.com`, on the Security Center logon screen.

9 Click **Apply**.

25

Fusion stream encryption

This section includes the following topics:

What is fusion stream encryption?

Fusion stream encryption is a proprietary technology of Genetec Inc. used to protect the privacy of your video archives. The Archiver uses a two-level encryption strategy to ensure that only authorized client machines or users with the proper certificates on smart cards can access your private data.

What is a fusion stream?

Fusion stream is a proprietary data structure of Genetec Inc. for streaming multimedia. Each fusion stream is a bundle of data (video, audio, and metadata) streams and key streams related to a single camera. Fusion streams are generated on specific client requests. The key streams are included only if the data streams are encrypted.

Benefits of fusion stream encryption

The benefits of fusion stream encryption are as follows:

- No data captured by Security Center is stored or transmitted as *plaintext*. This means that the privacy of your data is protected even if you outsource the management of your data center.
- Data streams are encrypted using the US government approved AES 128-bit encryption standard.
- The keys used to encrypt the data streams change every minute, discouraging any kind of brute-force attack.
- Each data stream is encrypted with a different key stream, reducing the attack surface.
- The key streams are encrypted using *public-key encryption*, ensuring that only authorized client machines (with a valid *private key*) can view the protected data. The private key can be installed on the machine or accessed from a smart card reader.
- If a private key is compromised (leaked out), you can prevent it from ever being used again on your system.
- Encryption overhead is kept to a minimum by encrypting the data stream only once. Redirectors and Auxiliary Archivers do not have to re-encrypt the data.

Limitations

The limitations of fusion stream encryption are as follows:

- Multicast from the video unit is supported only if the unit supports encryption and is connected through HTTPS.
- Recordings on the edge cannot be encrypted. Turn edge recording off if you want encryption.
- Video encrypted in version 5.8 and later cannot be decrypted in version 5.7 and earlier..
- Encrypted video cannot be viewed on Security Center Mobile devices.
- Motion detection by the Archiver is not supported when encryption is on.
- Thumbnails cannot be generated for encrypted video.
- Encryption cannot be added after the video has been archived.

  However, you can still encrypt your exported video files. For more information, see the *Security Center User Guide*.
- New encryption keys cannot be added to archived data, which means that authorization to view archived data cannot be granted to new machines.
- Encryption certificates are only validated for expiration dates. This means that any certificate you enroll takes effect immediately, regardless of its activation date.

  CAUTION: If a certificate expires it is no longer used for encryption. When there are no valid certificates left, video recording is stopped.

- Encryption cannot be removed from the video archives.

  The workaround is to export your video in ASF format.
- Encrypted video cannot be exported in legacy G64 format.

  When you export encrypted video in G64x format, the video is exported with encryption. All information necessary for the decryption of the video are found in the G64x file.
- Encrypted video cannot be recovered if you lose all your private keys.

  See Best practices for managing private keys on page 548.

How does fusion stream encryption work?

The application of fusion stream encryption requires that all client machines authorized to view encrypted data have a private key installed. The private key must match one of the encryption certificates configured on the Archiver.

Two-level encryption

The Archiver uses a two-level encryption strategy to protect the privacy of your data.

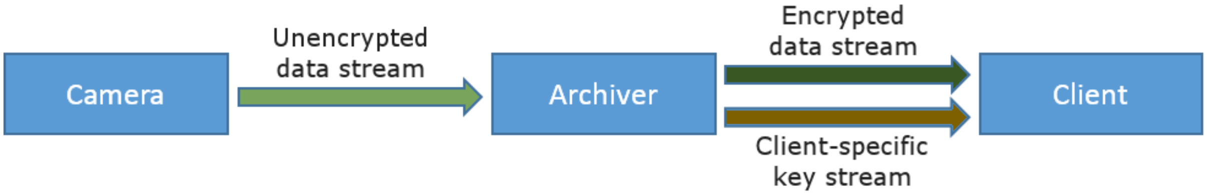
- First-level encryption: The Archiver receives the data stream as *plaintext* from the camera. Then the Archiver encrypts the data stream using randomly generated *symmetric keys* that change every minute. The stream of symmetric keys is called the *master key stream*. The master key stream is the *first key* needed to unlock the private data. It is shared by all client machines.
- Second-level encryption: To ensure that only authorized clients can access the master key stream, the Archiver protects it using *public-key encryption* (see RSA). The Archiver encrypts the master key stream individually for each authorized client, using a *public key*. Only the client that has the *private key* (matching the public key) installed can unlock the master key stream (the *first key*). The private key is the *second key* needed to unlock the private data. This private key must be kept on the client machine.

The public and private keys are part of an *encryption certificate* that is created for a specific client. The certificate also identifies the client. To enable encryption, the certificate must be stripped of its private key and handed to the Archiver. The Archiver then takes the public key from the certificate to encrypt the master key stream for that client. For this reason, the encrypted master key stream is called the *client-specific key stream*.

When the client requests encrypted data, it identifies itself to the Archiver by sending its certificate along with the data request. Based on the certificate, the Archiver knows which client is requesting the data, and sends the corresponding client-specific key stream with the encrypted data stream to the client. Since only the intended client has the matching private key, only the intended client can decrypt the information.

Summary

All video that must be protected must first go through the Archiver before it is sent to the requesting client. The Archiver encrypts the video, and sends the requested information bundled in a composite stream called the *fusion stream*. The fusion stream contains both the encrypted data streams, and their corresponding client-specific key streams.



If the fusion stream is intercepted by an unauthorized party on its way to the intended client, it remains protected because the unauthorized party does not have the private key, and thus cannot decrypt the data contained within.

BEST PRACTICE: It is recommended to create the encryption certificate on the client machine that will be requesting to view the video. This limits the exposure of the private key.

Related Topics

Preventing users from viewing encrypted data on a specific machine on page 554

Authorizing a new client to view all data from an encrypted camera on page 557

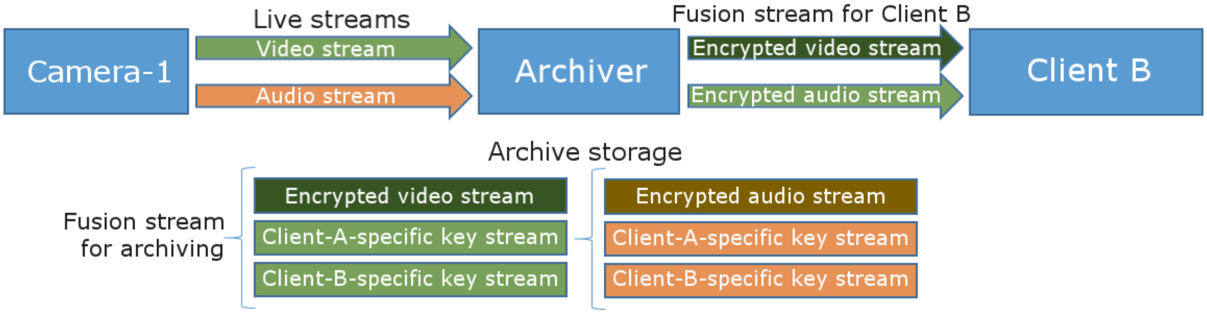
Fusion stream encryption scenarios

When a client machine requests a data stream (video, audio, metadata) from an encrypted camera, the Archiver sends a fusion stream containing all the information the client needs, and only what it needs.

Scenario setup

You want all video and audio from Camera-1 to be encrypted. You want Client A and Client B (workstations) to have access. First you request and install an *encryption certificate* on each of them. Then, you enable the encryption on the Archiver in charge of Camera-1, using the certificates you obtained for Client A and Client B.

The following diagram illustrates your setup with Client B requesting video from Camera-1.


Live streams
Camera-1
Video stream
Audio stream
Archiver
Fusion stream for Client B
Encrypted video stream
Encrypted audio stream
Client B
Archive storage
Fusion stream for archiving
Encrypted video stream
Client-A-specific key stream
Client-B-specific key stream
Encrypted audio stream
Client-A-specific key stream
Client-B-specific key stream

What happens when encryption is enabled

- Motion detection by Archiver on Camera-1 is disabled.
- Multicast from Camera-1 is disabled.
- The Archiver generates a fusion stream for archiving, which includes (see illustration):
  - One encrypted video stream.
  - One *client-specific key stream* so Client A can decrypt the video stream.
  - One client-specific key stream so Client B can decrypt the video stream.
  - One encrypted audio stream.
  - One client-specific key stream so Client A can decrypt the audio stream.
  - One client-specific key stream so Client B can decrypt the audio stream.

Scenario: Client B requests only video from Camera-1

- Client B sends a request for video from Camera-1 to Archiver, with its encryption certificate.
- The Archiver responds by sending a fusion stream to Client B, which includes (see illustration):
  - Encrypted video stream.
  - Client-specific key stream for Client B to decrypt the video.

Scenario: Client B requests both video and audio from Camera-1

- Client B sends a request for video and audio from Camera-1 to Archiver, with its encryption certificate.
- The Archiver responds by sending a fusion stream to Client B, which includes:
  - Encrypted video stream.
  - Client-specific key stream for Client B to decrypt the video.
  - Encrypted audio stream.
  - Client-specific key stream for Client B to decrypt the audio.

Performance impact of fusion stream encryption

Fusion stream encryption impacts the performance of the Archiver and the Security Desk workstations. You may need to reevaluate the type and number of machines you need if you plan on enabling this feature.

Fusion Stream Encryption impact on Archiver performance

The first encryption certificate enabled on the Archiver reduces the capacity of the Archiver by 30%. Each additional encryption certificate applied to all cameras further reduces the Archiver capacity by 4%.

For example, on an Archiver that supports 300 cameras without encryption:

Number of certificates enabled	Number of supported cameras
0 encryption certificates (no encryption)	300 cameras
1 encryption certificate	210 cameras
5 encryption certificates	178 cameras
10 encryption certificates	145 cameras
20 encryption certificates	96 cameras

BEST PRACTICE: Do not exceed 20 encryption certificates per Archiver.

Encryption impact on workstation performance

Video encryption can increase the CPU usage by up to 40% when viewing low-resolution video (CIF). The impact becomes less noticeable as the resolution of the video increases, because much more processing power is spent on decoding the video than on decrypting the video. The impact on performance becomes unnoticeable when viewing HD and Ultra-HD video.

Best practices for managing private keys

The effectiveness of fusion stream encryption relies on an external public-key infrastructure to manage the private keys. The entire security of the system is based on the fact that the private keys remain secret. Hence, the transfer and handling of the private keys must be done in a secure manner.

Safeguarding the private keys

The safest way to handle a public-private key pair is to generate the *encryption certificates* directly on the client machine, then assign this certificate (only the public key part) to the Archiver responsible for performing the encryption. This way, you reduce the attack surface by ensuring that the private key never leaves the client machine where it is used.

If you want to use the same private key on multiple client machines, make sure you distribute it in a secure way. Use a strong password to encrypt the private key while in transit. To learn how to do this, see Export a certificate with the private key.

After all copies of the private key are installed on the client machines, you can safely delete the temporary files that were used to distribute the private key.

BEST PRACTICE: If your company uses Active Directory Domain Services (ADDS), it is recommended to use the Credential Roaming mechanism, where private keys are associated to user group profiles instead of specific machines.

Preventing private key disclosure

You might worry about users exporting the private keys from their client machines. To reduce this risk, you can follow any of these *defense in depth* best practices.

- **Mark private keys as non-exportable:** To prevent Windows clients from extracting private keys, you can mark private keys as non-exportable.

  You set the non-exportable flag when you import a certificate.

  This is how:

  1. Create a certificate and export the public and private keys in PFX format. Use a strong password to encrypt the private key.
  2. Import only the public key for the Archiver servers.
  3. Import the private key for each individual machine, and set the private key as non-exportable.

     ```
     certutil -importPFX [PFXfile] NoExport
     ```
  4. When the private key has been imported for all machines, destroy the original PFX file.

  IMPORTANT: There are third-party applications that do not enforce the non-exportable flag. Because it is possible to export private keys by using these third-party applications, marking private keys as non-exportable is not entirely foolproof.
- **Run the operator account in unprivileged mode:** You can prevent your Security Desk users from exporting the private keys by installing the certificates on the local computer store instead of the users' personal stores, and by denying them administrator privileges. However, Security Desk still needs to have access to the private keys. This means that you need to run Security Desk as an administrator, and enter the password for the Security Desk users.
- **Restrict the use of applications through Windows Group Policy:** You can prevent the Security Desk users from accessing the private keys by blocking the tools used to manipulate the certificates, such as *certmgr.msi*, through Windows Group Policy.

Creating a private key backup

If you lose your private keys, you cannot recover your encrypted data. It is recommended that you use of a secured backup client machine to create an extra encryption certificate for all of the data that you encrypt. The private key corresponding to this certificate must not be used on any other client machine. The sole purpose of this backup machine is so that you have a backup solution in case all private keys used on your client machines are lost.

Setting up fusion stream encryption

To set up fusion stream encryption, you need to request and install encryption certificates on the machines that are authorized to view encrypted cameras, and then use those certificates to enable this feature on the Archiver.

What you should know

Fusion stream encryption is for the protection of your data privacy. To protect your data against tampering, see Protecting video files against tampering on page 680.

To set up fusion stream encryption:

1 Request and install the encryption certificates on the client machines that are authorized to access your company's private data.

2 Enable encryption on your Archiver or individual cameras.

Requesting and installing encryption certificates

To authorize a client machine to view encrypted data, you must request an encryption certificate from the client machine. You then install the certificate with the private key locally, and transfer the public portion of the certificate to the Archiver responsible for encryption.

Before you begin

There are many ways to request and manage *digital certificates*. Before you proceed, consult your IT department about your company's policies and standard procedures.

What you should know

The encryption certificate contains a pair of public and private keys. The public key is used by the Archiver to encrypt the private data for a specific client machine. The private key is used by the client machine to decrypt the private data.

BEST PRACTICE: The private key should never leave the machine on which it is needed.

To request and install an encryption certificate on a client machine:

1 Log on as a local administrator of the client machine.

2 Add the Certificates snap-in to your local computer account.

Installing the certificates in the local computer store gives you more control over the management of private keys.

3 Follow your company's procedure for requesting and installing the certificate.

4 If the client is supposed to have access to encrypted data for a limited time, set the certificate's expiry date accordingly.

5 If you do not plan to run Config Tool from this computer, export the certificate with only the public key to a certificate (.cer) file.

Save the certificate file to a location that can be accessed from the workstation from which you plan to run Config Tool.

After you finish

Enable encryption on your Archiver or individual cameras.

Related Topics

Best practices for managing private keys on page 548

Enabling fusion stream encryption

To protect the privacy of your data, you can enable fusion stream encryption.

Before you begin

Request and install the encryption certificates on the client machines authorized to access your company's private data.

What you should know

Only the public portion of the certificate must be installed on the Archiver.

Encryption certificates are applied through Config Tool. It is not necessary to install certificates on the Archiver server. To apply certificates, Config Tool must have access to the required certificates in the certificate store on the local machine, or exported certificate (.cer) files.

IMPORTANT: To enable encryption, you must add at least one certificate to the Archiver.

To enable fusion stream encryption:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Do one of the following:

- To enable encryption for all cameras connected to an Archiver, select an Archiver role to configure, and click the **Camera default settings** tab.
- To enable encryption for a specific a camera, select the camera, click the **Recording** tab, and then ensure **Recording settings** is set to **Custom settings**.

3 Click **Show advanced settings** and set **Encryption** to **In transit and at rest**.

4 Under the *Certificates* table, click **Add an item** (➕).

The *Select certificate* dialog box opens.

5 If the encryption certificates are already installed to the certificate store on the local machine, select them from the *Installed certificates* table, and click **OK**.

6 If the encryption certificates are not installed, find and install them:

a) Select **Browse certificate file**, and click **Browse certificate file** (....

The *Open* dialog box opens.

b) Navigate to the folder where the certificates files are saved.

The browser looks for **X.509 Certificates** files by default. If you do not find the required files, set it to look for **Personal Information Exchange** files instead.

c) Select the certificates to install, and click **Open**.

d) If a certificate file is password-protected, click the advanced show icon (⊕) and enter the password.

e) (Optional) Click **Validate file** to ensure the selected certificate is capable of encrypting and decrypting video.

NOTE: To validate decryption, the private key must be accessible to Config Tool during the test.

f) Click **OK**.

7 Click **Apply**.

The Archivers start encrypting all data streamed from the selected cameras. Only client workstations with one or more of the configured certificates are able to view the encrypted streams from now on.

Related Topics

Disabling fusion stream encryption on page 553
Preventing users from viewing encrypted data on a specific machine on page 554
Preventing compromised certificates from being used in your system on page 555
Authorizing a client to view new data from an encrypted camera on page 556
Authorizing a new client to view all data from an encrypted camera on page 557

Disabling fusion stream encryption

You can disable fusion stream encryption on the Archiver role or on individual cameras.

What you should know

You can disable fusion stream encryption by turning the **Encryption** switch off on either the Archiver or a camera.

BEST PRACTICE: Do not remove the *encryption certificates* from the Archiver in case you want to turn encryption back on.

To disable fusion stream encryption:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Do one of the following:

- To disable encryption on the Archiver, select the Archiver role to configure, and click the **Camera default settings** tab.
- To disable encryption on a camera, select the camera to configure, click the **Recording** tab, and then click **Custom settings**.

3 Click **Show advanced settings**, and turn **Encryption** off.

4 Click **Apply**.

The Archiver stops encrypting all future data streamed from the selected cameras. Video archives that were encrypted in the past remain encrypted.

Related Topics

Removing encryption from video archives on page 558

Preventing users from viewing encrypted data on a specific machine

If you no longer want people to use a specific client machine to access the data from an encrypted camera, you can remove the encryption certificate used to enable fusion stream encryption on that camera, from that machine.

What you should know

Access to data from encrypted cameras is controlled through the encryption certificates installed on the machine used to access the data, as opposed to through user privileges. Only follow this procedure if you are changing the configuration of a machine, not because an encryption certificate is compromised. If you think the distribution of an encryption certificate has been compromised, you can prevent it from ever being used again on your system.

IMPORTANT: If this client is the only machine that can access the encrypted camera, make sure you do not lose its encryption certificate (containing the *private key*). If you lose the certificate, you cannot recover the encrypted archives for that camera. If you have only one machine that can view the encrypted camera, follow the recommended best practices for managing private keys.

To stop a client machine from viewing data from an encrypted camera:

1. Log on to the client machine as a local administrator.
2. Add the Certificates snap-in to your local computer account.
3. Delete the certificates corresponding to the encrypted cameras that you no longer want people to view on this machine.
4. If this client is the only one using this certificate, also remove the certificate from the Archiver.

   This prevents the Archiver from performing unnecessary encryption. For information on how to remove a certificate from the Archiver, see Preventing compromised certificates from being used in your system on page 555.

The client will no longer be able to view new or archived data from the camera, so long as the camera remains encrypted.

Related Topics

How does fusion stream encryption work? on page 545

Preventing compromised certificates from being used in your system on page 555

Authorizing a client to view new data from an encrypted camera on page 556

Preventing compromised certificates from being used in your system

If you suspect that a fusion stream encryption certificate has been compromised, you can prevent that certificate from being used to access your encrypted video by removing it from the Archiver and deleting all key streams that were generated with that certificate.

Before you begin

IMPORTANT: Ensure that all archiving roles are online. These include Archiver, Auxiliary Archiver, and Cloud Playback roles. Key streams cannot be deleted if any archiving role associated with an encrypted camera is offline.

What you should know

The encryption certificate contains a *private key* that allows the client machine to query the Archiver for encrypted data, and to decrypt the key stream and data when they are received. For more information, see How does fusion stream encryption work? on page 545

CAUTION: If you remove the last certificate used to encrypt a camera from the Archiver, the camera ceases to be encrypted and all future data from that camera becomes accessible to all machines in your system. However, data that was previously encrypted remains encrypted.

To prevent a fusion stream encryption certificate from being used in your system:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Do one of the following:
   - If encryption is configured at the Archiver level, select the Archiver and click the **Camera default settings** tab.
   - If encryption is configured at the camera level, select the camera and click the **Recording** tab.
3. From the **Certificates** list, select the compromised certificate, and click **Remove the item** (✖).

   NOTE: You cannot enable **In transit and at rest** encryption if there are no configured certificates.
4. Click **Apply**.
5. In the message box that appears, do one of the following:
   - Click **Yes** to delete the selected certificate and the associated key streams (*client-specific key streams*).

     This option is highly recommended if your certificate has been compromised. It prevents client machines from accessing any encrypted data with the associated certificate.

     CAUTION: If you remove the only certificate used to generate key streams, you will permanently loose access to the encrypted data.
   - Click **No** to only delete the selected certificate from the Archiver, not the associated key streams.

     This option stops video encryption with the selected certificate. New video cannot be decrypted with the compromised certificate. However, all data that was encrypted before removing this certificate remains available to client machines that have the certificate installed.
6. Click **Apply**.

Related Topics

Preventing users from viewing encrypted data on a specific machine on page 554

Authorizing a new client to view all data from an encrypted camera on page 557

Authorizing a client to view new data from an encrypted camera

You can grant a new client machine the rights to access the future data from an encrypted camera by adding a new encryption certificate (public key) for that client to the Archiver in charge of that camera.

Before you begin

Adding more encryption certificates to an Archiver impacts its performance. See Performance impact of fusion stream encryption on page 547.

What you should know

A client machine has access to encrypted data because the Archiver transmits both the encrypted data stream and the key stream to the client. The key stream gives the client its first key to unlock the encrypted data. The client needs a *second key* to decrypt the *first key*, which is its *private key*. When you add the client's certificate to the Archiver, you are asking the Archiver to create a new *first key* that the client is able to unlock.

IMPORTANT: If this client is the last machine that has access to the data from the encrypted camera, make sure you do not lose its private key. If you do, you will not be able to recover the encrypted archives for that camera. If you are in that situation, follow the recommended best practices for managing private keys.

To authorize a new client to view the new data from an encrypted camera:

1 Request and install an encryption certificate for the new client machine.

2 Add the new certificate (public key) to the Archiver in charge of the camera.
For information on how to do this, see Enabling fusion stream encryption on page 551.

The new client machine can access any new data from the encrypted camera from this point on, but cannot access the data archived prior to this operation.

Related Topics

Preventing users from viewing encrypted data on a specific machine on page 554

Authorizing a new client to view all data from an encrypted camera on page 557

Authorizing a new client to view all data from an encrypted camera

You can grant a new client access to all the data of an encrypted camera by importing the encryption certificate (private key) of another client that does have access.

Before you begin

IMPORTANT: Private keys must be handled with care. See Best practices for managing private keys on page 548.

To authorize a new client to view all data from an encrypted camera:

1 Export the certificate of an authorized client machine with the private key.

2 Import the certificate with the private key to the new client machine.

The new client now has all the access rights granted to the original client through the imported encryption certificate. If the original client has access to more than one encrypted camera through this certificate, the new client now has access as well.

Related Topics

How does fusion stream encryption work? on page 545

Preventing compromised certificates from being used in your system on page 555

Authorizing a client to view new data from an encrypted camera on page 556

Removing encryption from video archives

You cannot remove the encryption from your video archives. However, you can export your video archives without encryption, using the ASF format.

Before you begin

You need a client machine authorized to access the encrypted camera, and a Security Center user account that has both the *Use ASF format* and *Remove encryption* privileges.

To export video from an encrypted camera without the encryption:

1. Open Security Desk from the authorized client workstation.
2. Export the video you want in ASF format.
   For information on exporting video, see the *Security Center User Guide*.

Part IV

Video

This part includes the following chapters:

26

Video at a glance

This section includes the following topics:

About Security Center Omnicast

Security Center Omnicast™ is the IP video management system (VMS) that provides organizations of all sizes the ability to deploy a surveillance system adapted to their needs. Supporting a wide range of IP cameras, it addresses the growing demand for HD video and analytics, all the while protecting individual privacy.

Omnicast™ main features include:

- View live and playback video from all *cameras*
- View up to 64 video streams side-by-side on a single workstation
- View all cameras on independent timelines or on synchronized timelines
- Full PTZ control, using a PC or CCTV keyboard or on screen using the mouse
- Digital zoom
- Motion detection
- Visual tracking: follow individuals or moving objects across different cameras
- Search video by *bookmark*, motion, or date and time
- Export video
- Protect video against accidental deletion
- Protect video against tampering by using digital signatures
- Protect privacy of individuals in video

Omnicast also provides video support for *events* tracked by other systems unified under Security Center.

- Enhance all event reporting with live and playback video
- Enhance alarm monitoring with live and playback video
- Enhance intrusion detection with live and playback video
- Enhance Synergis™ access control system with live and playback video
  - Video verification: compare *cardholder* picture with live and playback video
  - Consolidate all access events with live and playback video
- Enhance AutoVu™ automatic license plate recognition system with live and playback video

Entities related to video surveillance

The video surveillance system supports many of the entities in Security Center.

Icon	Entity	Description
	Archiver (role)	Controls the video units and manages the video archive.
	Auxiliary Archiver (role)	Supplements the video archive produced by the Archiver. It can archive any camera on the system.
	Media Router (role)	Manages the routing of all audio and video streams on the network.
	Media Gateway (role)	Transcodes Security Center video for Genetec™ Mobile, the Web Client, and the Genetec™ Web App and supports the Real Time Streaming Protocol (RTSP), which external applications can use to request raw video streams fromSecurity Center.
	Unit Assistant (role)	Manages system-wide operations on video units.
	Wearable Camera Manager (role)	Manages manage body-worn camera (BWC) devices in Security Center.
	Network	Network (with specific streaming capabilities) that the Media Router takes into account while making routing decisions.
	Server	Server on your network. Used to host the roles needed on your system.
	Area	Logical grouping of cameras and camera sequences.
	Analog monitor	Represents a physical analog monitor connected to a video decoder.
	Body-worn camera	Video recording system that is typically used by law enforcement to record their interactions with the public or gather video evidence at crime scenes.
	Camera	Single video source on the system. Might support audio.
	Camera (PTZ enabled)	PTZ camera (dome camera).
	Camera sequence	Prearranged order for the display of video sequences in a rotating fashion within a single tile in Security Desk.
	Monitor group	Group of analog monitors sharing common characteristics.
	Schedule	Date and time range, might support daytime and nighttime.
	Video unit	IP unit incorporating one or more video encoders.
	Partition	Group of entities on the system visible only to a group of users.
	User	Individual who uses Security Center applications.
	User group	Group of users sharing common characteristics.

27

Video deployment

This section includes the following topics:

Preparing to deploy your video surveillance system

To ensure easy video surveillance deployment, you need to perform a series of pre-configuration steps.

What you should know

It is recommended to connect the Security Center servers to a gigabit link because video traffic consumes bandwidth and can easily exceed 100 Mbps. In all cases, the best practice is to never go over 60% of network utilization on any given network link.

Before deploying your video system:

1. Have a network diagram showing all public and private networks used within your organization, their IP address range, their video transmission capabilities (Multicast, Unicast UDP, and Unicast TCP).

   For public networks, you also need the name and public IP address of their proxy servers. Ask your IT department for this information.
2. Open the ports used by Security Center for communication and video streaming, and make sure they are redirected for firewall and NAT purposes.
3. Install the following Security Center software components:

   a) Security Center Server software on your main server.

   The main server is the computer hosting the Directory role.

   b) (Optional) Security Center Server software on expansion servers.

   An expansion server is any other server on the system that does not host the Directory role. You can add expansion servers at any time.

   c) Security Center Client software on at least one workstation.

   For more information about installing Security Center, see the *Security Center Installation and Upgrade Guide*.
4. Have a list of *partitions* (if any).

   Partitions are used to organize your system into manageable subsystems. This is especially important in a multi-tenant environment. If, for example, you are installing one large system in a shopping center or, office tower, you might want to give local administration privileges to the tenants. By using partitions, you can group the tenants so that they can only see and manage the contents of their store or office, but not the others.
5. Have a list of all known users with their names and responsibilities.

   To save time, identify users who have the same roles and responsibilities, and organize them into user groups.

   NOTE: For large installations, users and user groups can be imported from a Windows Active Directory.
6. Install and connect all video equipment (video units, fixed and PTZ cameras) on your company's IP network, with the following information:

   - Manufacturer, model, and IP address of each video unit.
   - Login credentials (username and password) if applicable.
   - Communication protocol used (HTTP or HTTPS).

   TIP: A site map or floor plans showing where the cameras are located would be helpful.
7. If you have cameras connected to a conventional CCTV matrix (*hardware matrix* in Omnicast), you need the following:

   - An Omnicast™ 4.x system to manage the video encoders connected to the CCTV matrix outputs.
   - An Omnicast 4.x system federated in Security Center.

After you finish

Deploy your video surveillance system.

Related Topics

Importing security groups from an Active Directory on page 481
Setting up an Omnicast Federation on page 278

Deployment overview for your video management system

After completing the pre-configuration steps, you can integrate various video capabilities into your video management system deployment.

The following steps describe a typical video installation. Depending on your specific installation requirements, your process might be different.

Step	Task	Where to find more information
1	Complete the pre-configuration steps.	• Preparing to deploy your video surveillance system on page 564.
2	Use the Admin account in Config Tool to connect your system.	• Logging on to Security Center through Config Tool on page 7.
3	Create a partition for each independent group of entities. **TIP:** By defining the partitions first, you avoid having to move entities around after you have created them.	• Creating partitions on page 424.
4	To organize the entities in your system (such as areas, doors, and so on), configure the area view.	• Organizing the area view on page 26.
6	Configure your networking environment.	• About the Network view on page 154.
5	Configure the Archiver role.	• Configuring Archiver roles on page 568.
7	Configure the Auxiliary Archiver roles. If necessary, set up extra Archiver roles.	• Creating Auxiliary Archiver roles on page 590.
8	Configure the Media Router role.	• Configuring the Media Router role on page 597.
9	If you want to support web and mobile clients on your system, configure the Media Gateway role.	• Configuring Media Gateway roles on page 607. • About Security Center Web Client on page 410. • About Genetec Mobile on page 401.
10	(Optional) Define custom fields for your system entities.	• Creating custom fields on page 93.
11	Create user groups and create users.	• Creating user groups on page 429. • Creating users on page 433.
12	If necessary, federate remote Omnicast™ systems.	• Setting up an Omnicast Federation on page 278.
13	Create alarms.	• Creating alarms on page 1176.

About the Archiver role

The Archiver role is responsible for the discovery, status polling, and control of video units. The Archiver also manages the video archive and performs motion detection if it is not done on the unit itself.

All communications between the system and the video units are established through the Archiver role. All events generated by the units (motion, *video analytics*, and so on) are forwarded by the Archiver to the concerned parties on the system. Multiple instances of the Archiver role can be created on the system.

Configuring Archiver roles

To have your Security Center system manage your cameras, video archive, and motion detection, you must configure the Archiver role.

What you should know

When Omnicast™ is enabled in your license, an Archiver role is created by default and assigned to the *main server*.

To configure the Archiver role:

1 From the Config Tool home page, open the *Video* task.

2 Select the Archiver role to configure, and then click the **Resources** tab.

3 Configure the archive database.

4 Configure the archive storage settings.

5 (Optional) Change the role's host server.

6 To keep viewing video even if the server hosting the Archiver role goes offline, set up Archiver failover.

7 Add the video units that you want this Archiver role to control.

8 Click the **Extensions** tab and finish configuring the extensions that were created when you added the video units.

For a list of settings in the **Extensions** tab, see Archiver: Extensions tab on page 1341.

9 Click the **Camera default settings** tab and configure the default camera settings for all cameras recorded by this Archiver role.

For a list of settings in the **Camera default settings** tab, see Configuring default camera settings on page 579.

10 Configure the cameras associated to the video units you just added.

11 If recording is performed on edge units, set up video archive transfer.

After you finish

If you have a large system, you can distribute the load by creating more Archiver roles and hosting them on separate servers.

Related Topics

About the Archiver role on page 567

Moving the Archiver role to another server

In Security Center, if the server hosting the Archiver role breaks, is too slow, or has limited disk space, you can move the role to another server without installing any additional software.

Before you begin

Make sure you have another server configured and ready to accept a new role.

What you should know

Each Archiver is responsible for the *video archives* of the *cameras* it controls. The video archives include the archive database and the archive storage which can be hosted on the server hosting the Archiver, or on a different server. When moving the Archiver to another server, ensure that the new server also has access to these video archives.

To move the Archiver role to another server:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the Archiver role to configure, and then click the **Resources** tab.
3. If your current server is still running, and both the archive database and archive storage are local to your current server, back up the entire content of its video archives.
   a) In the *Backup configuration* section, temporarily set the backup folder to a location that is accessible by the new server. Make sure that the location you choose has enough disk space to store the video archives of your Archiver role.
   b) Using the following options, perform a manual backup:
      - For the type of backup, select **Backup**.
      - For the source, select the current Archiver role.
      - For the time range, select a range wide enough to include all of the video archives.
      - For the data, select **Everything since last transfer**.

   c) In the *Video* task, click the **Roles and units** view.
4. In the **Server** list, select the new server.
5. Based on the characteristics of the new server, make the necessary adjustments to the following:
   - The archive database
   - The archive storage settings

   IMPORTANT: If the new server is the same physical server as the old one, for example, same server but different GUID in Security Center, you do not need to make these adjustments.
6. Click **Apply**.
7. To restore video archives belonging to this Archiver role, consider the following:
   - If you performed a full backup, restore it with the following options:
     - For the restore type, select **Archiver**.
     - For the Archiver, select your current Archiver.
     - For the time range, select the same start and end time used for the backup.
     - For the cameras you want to restore, select all.
     - Turn off the option **Protect video from deletion**.
   - If your previous server broke and all your backups precede the server failure, restore all the video archives up to the archive retention period of the Archiver.
   - If both the archive database and the archive storage remained at the same location, such as on a third server, you do not need to restore the video archives.

8 If you temporarily changed the **Backup folder** location, set the folder back to its original location.

9 Click **Apply**.

About video units

A video unit is a video encoding or decoding device that is capable of communicating over an IP network and that can incorporate one or more video encoders. The high-end encoding models also include their own recording and video analytics capabilities. Cameras (IP or analog), video encoders, and video decoders are all examples of video units. In Security Center, a video unit refers to an entity that represents a video encoding or decoding device.

Video units are created manually, or automatically by the Archiver if the unit supports *automatic discovery*.

Related Topics

About the Unit enrollment tool on page 226
About the Unit Assistant role on page 233
Viewing unit properties on page 229

Adding video units manually

To monitor video in Security Center, you must add video units to an Archiver.

Before you begin

You must know the manufacturer, the product type (model or series), the IP address or hostname, and the logon credentials (username and password) for the units you plan to add.

TIP: If you do not know the IP address nor the hostname of your unit, *use the Unit enrollment tool* to discover it.

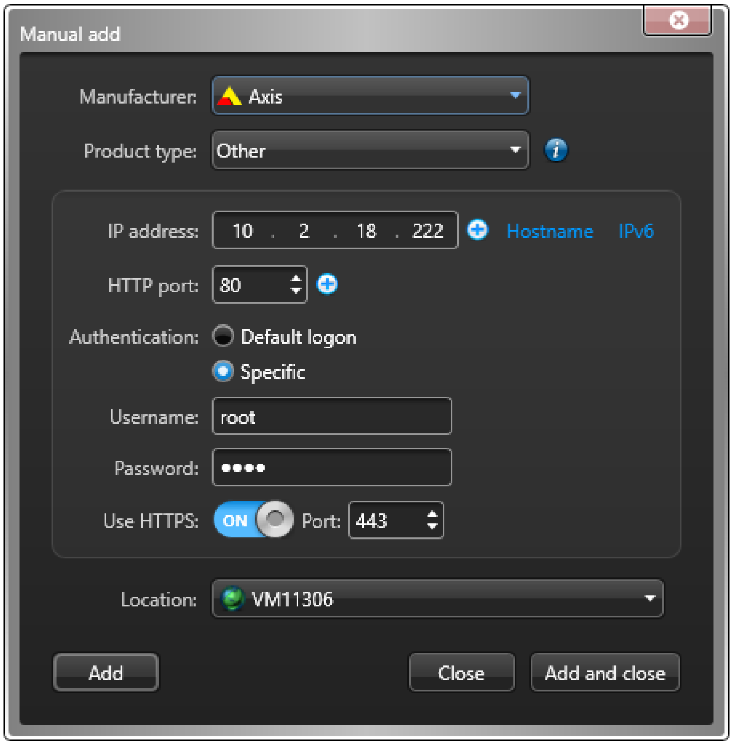
Change the video unit password. For the security of your system, you should never deploy video units with their factory default passwords.

TIP: If you have many video units to add, you can update their passwords at the same time from the *Hardware inventory* task.

To add a video unit:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Click **Video unit** (✚).
The *Manual add* dialog box opens.



Manual add

Manufacturer: Axis

Product type: Other

IP address: 10 . 2 . 18 . 222

HTTP port: 80

Authentication: ○ Default logon ● Specific

Username: root

Password: ●●●●

Use HTTPS: ON Port: 443

Location: VM11306

3 If you have multiple Archiver roles, select one to manage the unit from the **Archiver** list.

4 Select the unit’s manufacturer and product type.

5. Enter the **IP address** of the video unit.
   - Select **IPv4** or **IPv6** and enter the **IP address**.
   - If your network supports DHCP, enter the assigned **IP address**.
     NOTE: If this address is subject to change, click **Hostname** to enter the hostname of the unit.

   To add multiple units in a single operation, enter a range (⊕) of IP addresses.
6. Enter the **HTTP port** for the unit (default = 80).
   NOTE: If the unit uses HTTPS, enter the HTTP port (80) here. You will enter the HTTPS port in the following steps.
7. Select which credentials the Archiver uses to connect to the unit.
   - **Default logon:** Use the default logon credentials defined in the manufacturer’s extension for this Archiver. If the extension has not yet been defined, blank credentials are used.
   - **Specific:** Enter the specific logon credentials used by this unit. This can be changed to **Use default logon** later during video unit configuration.
8. If the video unit is configured to use HTTPS, turn on **Use HTTPS** and enter the HTTPS port of the unit (default = 443).
9. Complete all other settings as needed, and click **Add**.
   If the manufacturer’s extension does not exist, it is created for you.

   If the added unit is an encoder with multiple streams available, each stream is added with the *Camera - n* string appended to the unit name, *n* representing the stream number. For an IP camera with only one stream available, the unit name is not modified.

   NOTE: If the manufacturer supports *automatic enrollment*, all other units on your system with the same *discovery port* are automatically added to the same Archiver, in addition to those added manually.
10. To refresh the **Role view**, press **F5**.
    The new video unit is added under the selected Archiver.

After you finish

If necessary, change the default settings of the video units from their configuration tabs.

Related Topics

Video unit - Identity tab on page 1298
Video unit - Properties tab on page 1299
Video unit - Peripherals tab on page 1301
Updating video unit passwords in batches on page 578

Changing video unit passwords

For the security of your system, you should always change the unit password after enrolling them. For certain models of your video units, you can change their passwords directly from Config Tool.

Before you begin

If you need to change the passwords on a large number of units, you can update them in batches from the *Hardware inventory* task.

CAUTION: Changing a unit password causes a short recording interruption, so choose a time of day that minimizes disruption to your operations.

What you should know

- You need the *Update video unit password* privilege to perform this operation.
- Only certain models of video units support the password update feature from Config Tool. You might have to upgrade the unit firmware for this feature to work. For the list of manufacturers that support this feature, see "Manufacturers that support password update" in the *Security Center Video Unit Configuration Guide*.

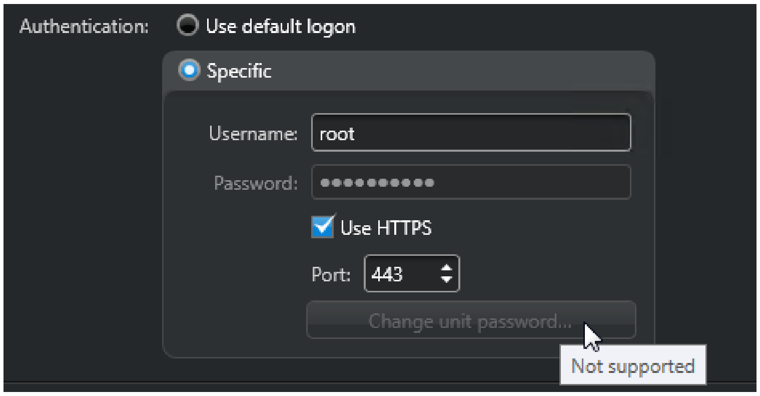
For the video units that are not supported, you must change their password on the unit itself through their web portal, and then update their password in Config Tool to match the new password.

To change a video unit password:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Select the video unit you want and click the **Properties** tab.

3 In the *Authentication* section, if the **Change unit password** button is disabled and its tooltip reads **Not supported**, you must change the password on the unit itself.



Authentication: ○ Use default logon

● Specific

Username: root

Password: ●●●●●●●●●●

☑ Use HTTPS

Port: 443

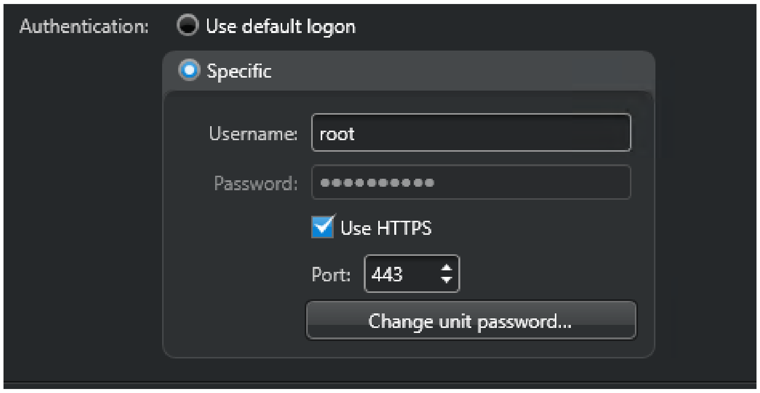
a) At the bottom of the screen, click **Unit** > **Unit's web page**.

b) Log on to the unit's web page and change its password.

c) Return to Config Tool, update the **Password** field, and click **Apply**.

If the tooltip indicates another cause, fix the problem and try again.

4 If the **Change unit password** button is enabled, click it.



Authentication: ○ Use default logon

● Specific

Username: root

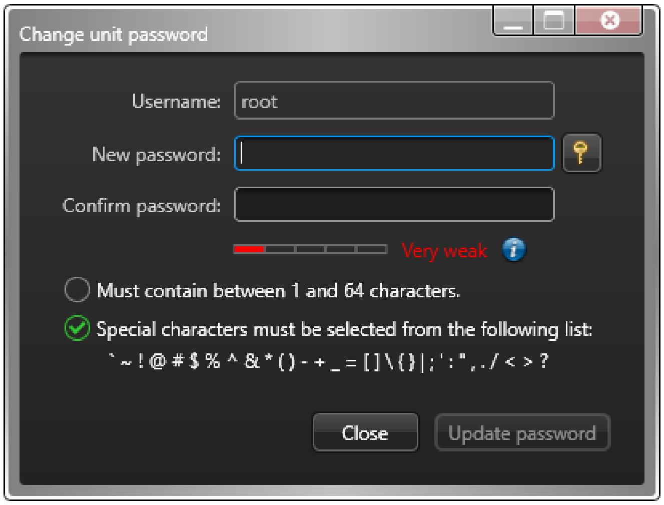
Password: ●●●●●●●●●●

☑ Use HTTPS

Port: 443

5 In the *Change unit password* dialog box, do one of the following:

- (Recommended) Click 🔑 for the system to generate a secure password.
- Enter the password manually, twice. The password must comply with the password policies that are displayed. Ensure that the password strength gauge indicates at least **Strong**.



Change unit password

Username: root

New password:

Confirm password:

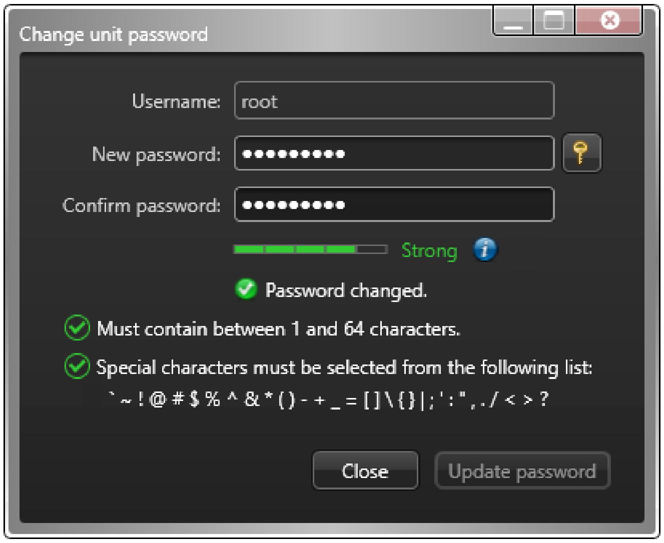
Very weak

○ Must contain between 1 and 64 characters.

✓ Special characters must be selected from the following list:
` ~ ! @ # $ % ^ & * ( ) - + _ = [ ] \ { } | ; ' : " , . / < > ?

6 Click **Update password**.

If the update is successful, you would see **Password changed**.



Change unit password

Username: root

New password: ••••••••••

Confirm password: ••••••••••

Strong

✓ Password changed.

✓ Must contain between 1 and 64 characters.

✓ Special characters must be selected from the following list:

` ~ ! @ # $ % ^ & * ( ) - + _ = [ ] \ { } | ; ' : " , . / < > ?

7 If the password is rejected, log on to the unit's web page to learn about its password policies and try again.

Password policies are defined by manufacturers. Some manufacturers enforce more rules than the ones displayed in the dialog box. For example, some manufacturers do not accept four consecutive ASCII characters, such as "1234" or "abcd", nor a string of four or more identical characters, such as "!!!!" or "aaaa".

After you finish

Change more unit passwords if necessary, then export the new passwords and keep them in a safe place.

IMPORTANT: We strongly recommend that you export your passwords if they are generated by the system. If you ever delete these units from Security Center, you will not be able to connect to these units through their web portal if you do not have a copy of their passwords.

Related Topics

Unit password management on page 251

Viewing video unit password history on page 576

Upgrading video unit firmware on page 739

Viewing video unit password history

You can view the history of unit password changes done through Security Center, using the Unit Assistant role. You can use this information to diagnose problems that might have occurred during a password change.

What you should know

- You need the *View/export unit passwords* privilege to perform this task.
- Password history details include when a unit's password was changed, what the previous password was, and what the password was changed to. You can use this information to resolve connectivity issues by retrying old passwords.

To view video unit password history:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Select the video unit you want and click the **Properties** tab.

3 In the *Authentication* section, select **Unit password history**.

The *Unit password history* dialog box opens showing the details of the previous password change attempts including the date, the previous password, and the new password.

4 Click **Recover password** to recover all previous passwords.

NOTE: The **Recover password** button is only available if there is a connection issue between the unit and Security Center.

If the Unit Assistant role is able to communicate with a password in the history, Security Center uses this password and reconnects the unit.

Related Topics

Changing video unit passwords on page 574

Updating video unit passwords in batches on page 578

Updating video unit passwords in batches

If you have a large number of video units in your system, you can update their passwords in batches from the *Hardware inventory* task.

Before you begin

Back up the Unit Assistant role database. It is used to store the last five password change requests of all units.

CAUTION: Changing a unit password causes a short recording interruption, so choose a time of day that minimizes disruption to your operations.

What you should know

- You need the *Update video unit password* privilege to perform this operation.
- Only certain models of video units support the password update feature from Config Tool. You might have to upgrade the unit firmware for this feature to work. For the list of manufacturers that support this feature, see "Manufacturers that support password update" in the *Security Center Video Unit Configuration Guide*.
- Always test this feature on a few units before applying it to a large batch of units of the same brand and model.

To update video unit passwords in batch:

1. From the Config Tool home page, open the *Hardware inventory* task.
2. Set up the query filters for your report.

   Choose one or more of the following filters:

   - **Units:** Select individual units or roles to investigate. Selecting a role is equivalent to selecting all units managed by that role.
   - **Custom fields:** Restrict the search to a predefined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
3. Click **Generate report**.

   The selected units are listed in the report pane.
4. Ensure that the units whose password you want to update are online.
5. Select the units you want to update and click **Update password** (🔑).

   The system automatically generates a strong password for each selected unit and sends a password change request to each.
6. Confirm that the passwords have been updated by waiting a minute and then regenerating the report.

   In the **Last password change result** column, the message *Password changed successfully* is displayed.

   NOTE: You can verify the password by clicking **Show password** (👁) in the **Password** column.
7. Export the new unit passwords and keep them in a safe place.

Related Topics

Unit password management on page 251

Viewing video unit password history on page 576

Upgrading video unit firmware on page 739

Configuring default camera settings

You can use the **Camera default settings** tab to configure the default video quality and recording settings for all cameras controlled by an Archiver.

What you should know

- Any recording settings configured in the Security Center Installer assistant are carried over to the **Camera default settings** tab.
- Recording settings affect your disk space.
- Recording settings defined in the **Recording** tab of an individual camera supersede the settings defined on the **Camera default settings** tab.

To configure default camera recording settings:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the Archiver to configure, and click the **Camera default settings** tab.
3. Under **Video quality**, select a **Resolution**.
   - **High:** 1270x720 and greater.
   - **Standard:** Between 320x240 - 1280x720.
   - **Low:** 320x240 and less.
   - **Default:** Manufacturer default settings.
   - **Frame rate:** You can select a value from 1 - 30 fps. Does not apply to default settings.
4. Click the **Recording modes** list and select a recording mode:
   - **Continuous:** Records continuously. Recording cannot be stopped by the user (🔴🔒).
   - **On motion/Manual:** Recording begins when triggered by the following:
     - A specific action, such as *Start recording*, *Add bookmark*, or *Trigger alarm*
     - Motion detection
     - User requests

     In this mode, the **Record** button in Security Desk indicates the recording status:

     - Grey (⚫) when the system is not recording. Clicking the button starts the recording.
     - Red (🔴) when the system is recording. Clicking the button stops the recording.
     - Red with a lock (🔴🔒) when the system is recording and cannot be stopped by the user, such as on motion or on alarm.
   - **Manual:** Records only when a user or a system action, such as *Start recording*, *Add bookmark*, or *Trigger alarm*, requests it.
   - **Custom:** Recording is specified by custom schedules.
     CAUTION: Two recording schedules of the same priority level, for example two daily schedules, cannot overlap, regardless of the recording mode configured for each. When a scheduling conflict occurs, the Archiver role and the video units are displayed in yellow in the entity browser and they issue entity warning messages. For more information, see Schedule conflicts on page 585.
   - **Off:** Recording is not permitted (⚫🔒), even when alarms are triggered.
5. Enable **Automatic cleanup** and specify a retention period for recorded video (in days).
   Video archives older than this period are deleted.
6. (Optional) Click **Show advanced settings** and configure the advanced options.
   - **Record audio:** Switch **ON** to record audio with your video. A microphone entity must be attached to your cameras.

NOTE: It is not necessary for the attached devices to belong to the same unit as the video encoder. However, for audio recording to work, ensure that the microphone belongs to a unit managed by the same Archiver, with the same Archiver extension, as the video encoder.

- **Record metadata:** Switch **ON** to record metadata with your video. Recording metadata is useful for analytics and for filtering recorded video.
- **Redundant archiving:** Switch **ON** to allow primary, secondary, and tertiary servers to archive video, and audio, at the same time. This setting is effective only if failover is configured.
- **Time to record before an event:** Use the slider to set the duration (in seconds) recorded before an event. This buffer is saved whenever the recording starts, ensuring that whatever prompted the recording is also captured on video.
- **Time to record after a motion:** Use the slider to set the duration (in seconds) recorded after a motion event. During this time, the user cannot stop the recording.
- **Default manual recording length:** Use the slider to select the duration (in minutes) the recording lasts when it is started manually by a user, or when the *Start recording* action is triggered.

7 (Optional) Select your **Encryption** option.

- **None:** The video is not encrypted.
- **In transit from Archiver:** (Default) The video is encrypted only when it is streamed from the Archiver. The video archive is not encrypted. All users who have the right to access the camera can view the encrypted video. There is no need to install any *encryption certificates*. Use this option if your archive storage is secured behind firewalls.

  You must enable **Secure communication** on the Media Router for this option to work.

  This option has the following limitations:

  - Multicast from the unit is not supported
  - Audio streamed from Security Desk only supports TCP connection type
  - Video streamed to analog monitors is not encrypted in transit
  - Privacy protected streams are not encrypted in transit
  - Backward compatibility (Security Center 5.7 and earlier) is not supported:
    - Clients in compatibility mode cannot view video encrypted in transit
    - Auxiliary Archiver roles in backward compatibility mode cannot archive video encrypted in transit
    - Redirectors in backward compatibility mode cannot redirect video encrypted in transit
- **In transit and at rest:** The video is encrypted after it reaches the Archiver, using *fusion stream encryption*. The video archive on disk is also encrypted. If the video unit supports encryption and is connected through HTTPS, then the video is encrypted end-to-end.

  To enable this option, you must install at least one encryption certificate on the server hosting the Archiver role.

  The video can only be viewed in one of the following ways:

  - Using a workstation with a certificate that matches one of the listed certificates on the Archiver. Access is restricted to the workstation.
  - Using a smart card with a certificate that matches one of the listed certificates on the Archiver. Access is restricted to the holder of the smart card.

  We recommend this option when your data center is managed by a third party.

This option has the following limitations:

- Video thumbnail and motion detection by the Archiver are not supported.
- Multicast from the unit is supported only if the unit supports encryption.
- Video encrypted in version 5.8 and later cannot be decrypted in version 5.7 and earlier.

TIP: Video encryption and privacy protection can be combined.

- If the privacy of the individuals captured on video is your only concern, use privacy protection instead.
- If the privacy of your data is your only concern, select one of the video encryption options.
- If you need to protect the privacy of both the individuals and your data, you can combine privacy protection and encryption.

8 (Optional) Configure different recording retention periods for the secondary and tertiary servers.

9 Click **Apply**.

Related Topics

Creating schedules on page 204

Configuring camera settings on page 614

Setting up Archiver failover on page 193

Configuring the Media Router role on page 597

What is fusion stream encryption? on page 543

Configuring recording settings for cameras

To set the recording mode (continuous, on motion, and so on) or enable encryption for your cameras, you can do so through the **Recording** tab of each individual camera.

Before you begin

If you use multiple disk groups for archive storage, temporarily turn off recording mode and then re-enable it at the end of the process to avoid creating video files on the wrong disk group.

What you should know

- The recording settings of cameras affect your disk space.
- Recording settings defined for an individual camera supersede the settings defined for the Archiver.
- If you disable archiving for a server in the **Camera default settings** tab of the Archiver, recording stops for all the cameras when the role is running on that server. Any recording schedule configurations or custom recording settings are ignored, and the cameras are used only for live viewing.

To configure the recording settings for cameras:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the camera to configure, and then click the **Recording** tab.
3. In the **Recording settings** option, select one of the following:
   - **Inherit from Archiver:** The camera inherits the recording settings configured for the Archiver role in the **Camera default settings** tab.
   - **Custom settings:** The camera uses its own settings.
4. Click the **Recording modes** list and select a recording mode:
   - **Continuous:** Records continuously. Recording cannot be stopped by the user (🔴🔒).
   - **On motion/Manual:** Recording begins when triggered by the following:
     - A specific action, such as *Start recording*, *Add bookmark*, or *Trigger alarm*
     - Motion detection
     - User requests

     In this mode, the **Record** button in Security Desk indicates the recording status:

     - Grey (⚫) when the system is not recording. Clicking the button starts the recording.
     - Red (🔴) when the system is recording. Clicking the button stops the recording.
     - Red with a lock (🔴🔒) when the system is recording and cannot be stopped by the user, such as on motion or on alarm.
   - **Manual:** Records only when a user or a system action, such as *Start recording*, *Add bookmark*, or *Trigger alarm*, requests it.
   - **Custom:** Recording is specified by custom schedules.
     CAUTION: Two recording schedules of the same priority level, for example two daily schedules, cannot overlap, regardless of the recording mode configured for each. When a scheduling conflict occurs, the Archiver role and the video units are displayed in yellow in the entity browser and they issue entity warning messages. For more information, see Schedule conflicts on page 585.
   - **Off:** Recording is not permitted (⚫🔒), even when alarms are triggered.
5. Enable **Automatic cleanup** and specify a retention period for recorded video (in days).

   Video archives older than this period are deleted.

6 (Optional) Click **Show advanced settings** and configure the advanced options.

- **Record audio:** Switch **ON** to record audio with your video. A microphone entity must be attached to your cameras.

  NOTE: It is not necessary for the attached devices to belong to the same unit as the video encoder. However, for audio recording to work, ensure that the microphone belongs to a unit managed by the same Archiver, with the same Archiver extension, as the video encoder.
- **Record metadata:** Switch **ON** to record metadata with your video. Recording metadata is useful for analytics and for filtering recorded video.
- **Redundant archiving:** Switch **ON** to allow primary, secondary, and tertiary servers to archive video, and audio, at the same time. This setting is effective only if failover is configured.
- **Time to record before an event:** Use the slider to set the duration (in seconds) recorded before an event. This buffer is saved whenever the recording starts, ensuring that whatever prompted the recording is also captured on video.
- **Time to record after a motion:** Use the slider to set the duration (in seconds) recorded after a motion event. During this time, the user cannot stop the recording.
- **Default manual recording length:** Use the slider to select the duration (in minutes) the recording lasts when it is started manually by a user, or when the *Start recording* action is triggered.

7 (Optional) Select your **Encryption** option.

- **None:** The video is not encrypted.
- **In transit from Archiver:** (Default) The video is encrypted only when it is streamed from the Archiver. The video archive is not encrypted. All users who have the right to access the camera can view the encrypted video. There is no need to install any *encryption certificates*. Use this option if your archive storage is secured behind firewalls.

  You must enable **Secure communication** on the Media Router for this option to work.

  This option has the following limitations:

  - Multicast from the unit is not supported
  - Audio streamed from Security Desk only supports TCP connection type
  - Video streamed to analog monitors is not encrypted in transit
  - Privacy protected streams are not encrypted in transit
  - Backward compatibility (Security Center 5.7 and earlier) is not supported:
    - Clients in compatibility mode cannot view video encrypted in transit
    - Auxiliary Archiver roles in backward compatibility mode cannot archive video encrypted in transit
    - Redirectors in backward compatibility mode cannot redirect video encrypted in transit
- **In transit and at rest:** The video is encrypted after it reaches the Archiver, using *fusion stream encryption*. The video archive on disk is also encrypted. If the video unit supports encryption and is connected through HTTPS, then the video is encrypted end-to-end.

  To enable this option, you must install at least one encryption certificate on the server hosting the Archiver role.

  The video can only be viewed in one of the following ways:

  - Using a workstation with a certificate that matches one of the listed certificates on the Archiver. Access is restricted to the workstation.
  - Using a smart card with a certificate that matches one of the listed certificates on the Archiver. Access is restricted to the holder of the smart card.

  We recommend this option when your data center is managed by a third party.

This option has the following limitations:

- Video thumbnail and motion detection by the Archiver are not supported.
- Multicast from the unit is supported only if the unit supports encryption.
- Video encrypted in version 5.8 and later cannot be decrypted in version 5.7 and earlier.

TIP: Video encryption and privacy protection can be combined.

- If the privacy of the individuals captured on video is your only concern, use privacy protection instead.
- If the privacy of your data is your only concern, select one of the video encryption options.
- If you need to protect the privacy of both the individuals and your data, you can combine privacy protection and encryption.

8 Click **Apply**.

Related Topics

Creating schedules on page 204
Configuring camera settings on page 614
Setting up Archiver failover on page 193
Configuring the Media Router role on page 597
What is fusion stream encryption? on page 543

Schedule conflicts

A schedule is an entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).

Schedule conflicts

You might have a scheduling conflict when two overlapping schedules apply to the same function. For example, if two schedules apply to the recording of the same camera.

Security Center can resolve some of these conflicts by giving priority to the most specific (or restrictive) schedule, which is determined by its date coverage option in the following order of decreasing priority:

1. Specific (runs only once, highest priority)
2. Ordinal (repeats on a monthly or yearly basis)
3. Weekly (repeats every week)
4. Daily (repeats every day)
5. Always (default schedule, lowest priority)

IMPORTANT: When two overlapping schedules with the same priority level apply to the same function, an unresolved conflict occurs. If the two schedules are applied to an entity, an *Entity warning* occurs, and the entity with the conflicting configuration is displayed in yellow in the entity browser.

Configuring audio codecs

To ensure that audio is properly captured in Security Center, video units must use a compatible audio codec.

What you should know

- Security Center supports the following audio codecs: G.711, G.721, G.723, AAC (8 kHz or 16 kHz).
- Security Center supports mono and stereo audio signals. These signals must be from a single source and encoded with one of our supported codecs.
- Security Center does not support two independent mono signals and cannot mix them to create a stereo signal. Mixing two microphone signals to get left and right channel for stereo must be performed by an audio mixer. The mixed audio then becomes a single source that outputs a stereo signal. This signal must be encoded with a support codec before being imported into Security Center.
- A single soundtrack can be associated to multiple cameras, but multiple soundtracks cannot be associated to one single camera.

To configure a video unit's audio codec:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the video unit to configure, then click the **Peripherals** tab.
3. Double-click the video unit's **Microphone** and select an audio codec from the **Data format** dropdown list.

   NOTE: The **Data format** dropdown only displays codecs that are supported by the selected video unit.
4. Click **Apply**.

Viewing recording states of cameras

You can view the recording state and statistics of each individual camera controlled by an Archiver or Auxiliary Archiver to verify whether each encoder is streaming video and audio, and whether the role is recording the data.

To view the recording state of a camera:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the archiving role in charge, click its **Resources** tab, and then click **Statistics** (◕).

   The **Active cameras** and **Archiving cameras** fields show you how many cameras are active, and how many have archiving enabled.
3. Click **See details**.

   In the *Archiving cameras* dialog box, the recording states of the cameras are listed. The possible recording states are:

   - **Recording off:** Recording is enabled but the Archiver is not recording. If you suspect a problem, click the **Description** column. The possible causes are:
     - Database lost.
     - Disks full.
     - Cannot write to any drive.
   - **Recording on:** Recording was started by a user.
   - **Recording on (locked by system):** Recording is currently controlled by the Archiver, following an On motion or Continuous schedule.
   - **Recording off (locked by system):** Recording is currently disabled on this camera by a schedule.
   - **Recording about to stop:** Recording was started by a user and is within the last 30 seconds of recording.

About the Auxiliary Archiver roles

The Auxiliary Archiver role supplements the video archive produced by the Archiver role. Unlike the Archiver role, the Auxiliary Archiver role is not bound to any particular *discovery port*, therefore, it can archive any camera in the system, including cameras federated from other Security Center systems. The Auxiliary Archiver role cannot operate independently; it requires the Archiver role to communicate with video units.

You can create multiple instances of this role on the system.

Auxiliary Archiver scenarios

The following are some sample scenarios where you need Auxiliary Archivers:

- You need to create a high-resolution off-site (outside your corporate LAN) copy of your video archive for selected cameras. In this scenario, you run the Auxiliary Archiver from a secure location, probably on a server in a separate building with large storage capabilities. The Auxiliary Archiver records high-quality video streams from specific cameras using different recording settings (mode, schedules, and so on) than the Archiver.
- You need to create a lower-quality copy of your video archive to keep for a longer period. In this scenario, you record the low quality video stream with the Auxiliary Archiver and set a longer retention period.
- You need to record more cameras during off-hours when there are no guards on duty. In this scenario, you configure an Auxiliary Archiver to continuously archive cameras during off-hours that are also archived by the regular Archiver.

Limitations of Auxiliary Archiver roles

Auxiliary Archivers cannot record cameras that are federated from an Omnicast™ 4.x system (through *Omnicast™ Federation™*, or through a remote Security Center system that federates an Omnicast 4.x system).

Differences between the Archiver and Auxiliary Archiver

The Archiver role and Auxiliary Archiver role differ in several characteristics.

The following table shows the differences between the Archiver and the Auxiliary Archiver.

Characteristics	Archiver role	Auxiliary Archiver role
Automatic unit discovery	Yes, on units that support it.	No.
Command and control of cameras and video units	Yes.	No. It relies on the Archiver role.
Command encryption using secure protocols (such as HTTPS and *SSL*)	Yes, on units that support it.	Not applicable.
Recorded cameras	A camera can only be associated to one Archiver role.	A camera can be associated to multiple Auxiliary Archiver roles.
	Can only record cameras with which it has a direct connection, usually on the same LAN.	Can record any camera on the system, including federated cameras, but only from Security Center systems.

Characteristics	Archiver role	Auxiliary Archiver role
Recording settings	Each camera has the option to follow the default role settings or its own custom settings.	Each camera has the option to follow the default role settings or its own custom settings.
Recorded video stream	Can only record the stream designated for *Recording*.	Can record any video stream.
Event logging in database	Yes. The events can be searched and viewed with the *Archiver events* video maintenance task.	Yes. The events can be searched and viewed with the *Archiver events* video maintenance task.
Event logging to a flat file	Yes. Found in *ArchiverLogs* folder.	No.
Failover support	Yes. One *secondary server* can be added to the Archiver role.	Not applicable.
Multiple copies of the video archive	Yes, through *redundant archiving*, but the master and redundant copies are identical because they use the same recording settings.	Yes. Each Auxiliary Archiver produces a different set of video archives that follow recording settings.

Creating Auxiliary Archiver roles

To create a set of video archives apart from those managed by the Archiver role, you must create an Auxiliary Archiver.

What you should know

The Auxiliary Archiver role is not created by default; it must be created manually.

NOTE: After you create the Auxiliary Archiver, you should not move the role to a different server unless both the database and the video storage are configured on a separate machine.

To create an Auxiliary Archiver role:

1 Open the *System* task and click the **Roles** view.

2 Click **Add an entity** (➕) > **Auxiliary Archiver**.

3 On the *Specific info* page, do the following:

   a) If you have multiple servers in your system, click the **Server** list and select the server where this role is hosted.

   b) Select the **Database server** used to manage the role database.

   During software installation, a default database server, **(local)\SQLEXPRESS**, might have been installed on your server. You can use it or use another database server on your network.

   c) In the **Database** field, enter the name of the video archive database.

   CAUTION: The default name is *AuxiliaryArchiver*. If the selected server is already hosting another instance of Auxiliary Archiver, you must choose a different name. Otherwise, the new role will corrupt the existing database.

   TIP: You should use a different database name for every instance of Auxiliary Archiver regardless of whether there is a conflict or not, to avoid confusion.

   d) From the **Authentication** list, select which SQL Server authentication is to be used:

   - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
   - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.

   e) Click **Next**.

4 On the *Basic information* page, enter a name and description for the role.

5 If there is a **Partition** field, select the partition this role is a member of.

   Partitions determine which Security Center users have access to this entity. Only users who have been granted access to the partition can see this role.

6 Click **Next** > **Create** > **Close**.

   A new Auxiliary Archiver role () is created. Wait a few seconds for the role to create the database on the selected database server.

7 Select the **Resources** tab, and configure the server and database for this Auxiliary Archiver.

   NOTE: Every newly created Auxiliary Archiver is assigned the default value of 558 for its RTSP port. This port value must be unique for all archiving roles hosted on the same machine.

8 Configure the archive storage settings.

9 Click the **Camera recording** tab, and configure the default recording settings for all cameras recorded by this Auxiliary Archiver.

10 Click the **Cameras** tab, and select the cameras you want to archive.

Related Topics

Auxiliary Archiver - Resources tab on page 1353

Adding cameras to Auxiliary Archiver roles

For the Auxiliary Archiver to create video archives, you must add cameras to be controlled by the role.

What you should know

You cannot add federated cameras from Omnicast™ 4.x systems to the Auxiliary Archiver.

To add a camera to the Auxiliary Archiver:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Select the Auxiliary Archiver, click the **Cameras** tab, and click **Add an item** (✚).

3 In the dialog box that opens, select the cameras you want and click **OK**.

   NOTE: It takes a few seconds for the selected cameras to be added. If the role is unable to add a camera in the given time, a failed status is indicated, and the camera is removed.

4 Click **Apply**.

5 To override the default recording settings on a camera:

   a) Select the camera from the list and click **Jump to** (➔).

      The camera configuration page is selected.

   b) From the **Recording** tab of the camera, select the tab that corresponds to the current Auxiliary Archiver.

   c) Under **Recording settings**, click **Custom settings**, and make the necessary changes.

   d) Click **Apply**.

Removing cameras from Auxiliary Archiver roles

You can remove a camera from the Auxiliary Archiver, so it is no longer recorded by the Auxiliary Archiver.

To remove a camera from an Auxiliary Archiver:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Select the Auxiliary Archiver, click the **Cameras** tab, select the camera from the list, then click **Remove the item** (✖).

3 In the confirmation dialog box that appears, click **Remove**.

4 In the second confirmation dialog box, do one of the following:

   - Click **No** if you want to keep the video archives associated with the camera.

     This allows you to play the video files with the Video file player in Security Desk, but you are no longer able to query the video archives with the *Archives* task.

   - Click **Yes** if you do not want to keep the video archives.

Configuring camera recording settings for an Auxiliary Archiver

You can use the **Camera recording** tab to configure the recording settings for all cameras controlled by an Auxiliary Archiver.

Before you begin

If you use multiple disk groups for archive storage, temporarily turn off recording mode and then re-enable it at the end of the process to avoid creating video files on the wrong disk group.

What you should know

- The recording settings of cameras affect your disk space.
- Recording settings defined in the **Recording** tab of an individual camera supersede the settings defined on the **Camera recording** tab of the Auxiliary Archiver.

To configure recording settings for cameras managed by an Auxiliary Archiver:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the Auxiliary Archiver to configure, and click the **Camera recording** tab.
3. From the **Video stream** list, select the default video stream that the Auxiliary Archiver should record for each camera. The video streams are configured for each camera.
4. From the **Recording modes** list, select one of the following recording modes:
   - **Continuous:** Records continuously. Recording cannot be stopped by the user (●).
   - **Manual:** Records only when a user or a system action, such as *Start recording*, *Add bookmark*, or *Trigger alarm*, requests it. In this mode, the **Record** button in Security Desk indicates the recording status:
     - Grey (●) when the system is not recording. Clicking the button starts the recording.
     - Red (●) when the system is recording. Clicking the button stops the recording.
     - Red with a lock (●) when the system is recording and cannot be stopped by the user, such as on alarm.
   - **Custom:** Recording is specified by custom schedules.

     CAUTION: Two recording schedules of the same priority level, for example two daily schedules, cannot overlap, regardless of the recording mode configured for each. When a scheduling conflict occurs, the Archiver role and the video units are displayed in yellow in the entity browser and they issue entity warning messages. For more information, see Schedule conflicts on page 585.
   - **Off:** Recording is not permitted (●), even when alarms are triggered.
5. Enable **Automatic cleanup** and specify a retention period for recorded video (in days).

   Video archives older than this period are deleted.
6. (Optional) Click **Show advanced settings** and configure the advanced options.
   - **Record audio:** Switch **ON** to record audio with your video. A microphone entity must be attached to your cameras.

NOTE: It is not necessary for the attached devices to belong to the same unit as the video encoder. However, for audio recording to work, ensure that the microphone belongs to a unit managed by the same Archiver, with the same Archiver extension, as the video encoder.

- **Record metadata:** Switch **ON** to record metadata with your video. Recording metadata is useful for analytics and for filtering recorded video.
- **Time to record before an event:** Use the slider to set the duration (in seconds) recorded before an event. This buffer is saved whenever the recording starts, ensuring that whatever prompted the recording is also captured on video.
- **Time to record after a motion:** Use the slider to set the duration (in seconds) recorded after a motion event. During this time, the user cannot stop the recording.
- **Default manual recording length:** Use the slider to select the duration (in minutes) the recording lasts when it is started manually by a user, or when the *Start recording* action is triggered.

7 Click **Apply**.

Related Topics

Creating schedules on page 204

Configuring camera settings on page 614

Configuring HTTPS for video unit extensions

Additional configuration is required on the unit's web page for video units that support HTTPS connections.

To configure an HTTPS connection for a video unit:

1 Add a server certificate to the unit and enable HTTPS on the unit’s web page. For more information, see the manufacturer’s documentation.

2 If you are using a self-signed certificate, do the following:

a) In Config Tool, select the Archiver managing the camera and click the **Extensions** tab.

b) Select the camera extension.

c) In **Advanced security settings**, do the following if required:

- For the Archiver to accept self-signed certificates, turn on the **Allow unknown certificate authority** option.
- For the Archiver to accept non-server certificates, turn on the **Allow non-server certificates** option.

  This tells the system to skip the validation of the X.509 extended key usage (EKU).
- For the Archiver to accept certificates that do not have the IP address or hostname of the unit entered as the **Subject name** and **Alternative name**, set the **Allow certificates with invalid subject name** option to ON.
- For the Archiver to accept expired certificates, turn on the **Allow certificates with invalid date** option.

d) Click **Apply**.

3 If the camera was previously added to Security Center, do the following:

a) From the *Video* task in Config Tool, select the unit to configure.

b) Make sure the **Use HTTPS** setting is selected in the **Properties** tab.

c) Configure the HTTPS **Port** (default is 443) and click **Apply**.

4 If the camera was not added to Security Center, do the following:

a) From the *Video* task in Config Tool, click **Video unit** (✚).

b) In the *Manual add* dialog box, complete the necessary settings to add the camera. Make sure the **Use HTTPS** setting is **ON**.

c) Click **Add**.

Related Topics

Unit certificate management on page 234

About the Media Router role

The Media Router role is the central role that handles all stream requests (audio and video) in Security Center. It establishes streaming sessions between the stream source, such as a camera or an Archiver, and its requesters (client applications). Routing decisions are based on the location (IP address) and the transmission capabilities of all parties involved (source, destinations, networks, and servers).

Role of the Media Router

The Media Router ensures all video streams use the best route to get to their destinations, while performing any necessary transport transformation, for example, from unicast to multicast, or from IPv4 to IPv6.

Only a single instance of the Media Router role is permitted per system.

Network security

The Media Router role has a default RTSP port of 554, and its redirectors have a default RTSP port of 560 and a default RTP port of 960. Archiver roles have two default RTSP ports: 555 and 605. If the Media Router, redirector, and Archiver are hosted on the same server, each of these ports must be unique. For all ports requirements, see Ports used by Omnicast applications in Security Center on page 1460.

If multiple Archiver roles are created on the same server, they must each have different RTSP ports. Otherwise, the role entity turns yellow and an *Entity warning* event is generated.

Multicast optimization

Client applications can only request multicast streams by IP address from the router, not by port number. Therefore, although a client application listens only on a specific port, all stream sources sharing the same IP address are sent by the router. If your system uses Federation™, there is a good chance that a federated camera would be assigned the same IP address, with a different port, as a local camera. When a client requests a multicast stream from a local camera while a federated camera assigned to the same IP address is in use, both streams are sent to the client, although only one is needed. The likelyhood of this conflict is greatly increased if, for example, you record the federated stream continuously.

To avoid wasting network bandwidth, the Media Router uses two separate ranges of IP addresses, one for local streams and another for federated streams. Each range of multicast IP addresses is defined by a **Start address** and a specific port number.

Overcoming Windows multicast performance issue

There is a known Windows limitation that puts a cap on the bandwidth of a single port at around 100 Mbps. For systems with a lot of multicast traffic, a second optimization is available, and that is to increment the port number for each new multicast address. For each new multicast address, the port number is incremented by 2. Even port numbers are used for data transmission, while odd port numbers are used for RTCP control messages. This option is available on the *Properties* page of the Media Router.

For more information, see "Best practices for configuring Multicast in your network for Security Center" in *Security Center Best Practices - Enterprise*.

Related Topics

Media Router configuration tabs on page 1369

Configuring the Media Router role

You can configure the Media Router role settings to optimize the throughput and increase the security of your private network.

Before you begin

Read about the various optimizations offered by the Media Router.

What you should know

When Omnicast™ is enabled by your license, the Media Router role is created by default and hosted on the main server. The default setup is usually sufficient, unless you have a complex system involving multiple private networks.

To configure the Media Router role:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the **Media Router** role.
3. (Optional) Click the **Resources** tab, and configure the following:
   a) Change the role's primary server.
   b) To configure failover for the Media Router, add a standby server.
4. Click the **Properties** tab.
5. To secure and authenticate RTSP video requests in Security Center, enable **Secure communication**.

   When secure communication is enabled, all video communications use RTSP over TLS, but only the RTSP control channel is encrypted for live video streaming. To encrypt the video data channel, set the camera encryption to *In transit from Archiver* or *In transit and at rest*. Video playback and video export always use RTSP over TCP, therefore the RTSP control channel and the video data channel are both encrypted.

   IMPORTANT: Secure communication is enabled by default on new installations, but disabled if you upgraded from version 5.5 or earlier. When secure communication is turned on, Security Center systems older than 5.5 cannot federate your Security Center system.
6. In the *Multicast* section, if the default **Start address** and port settings conflict with other applications on your system, select different values for your local and federated streams.

   In multicast, all audio and video sources are streamed to different multicast addresses while using the same port number, because multicast switches and routers use the destination IP address to make their routing decisions. Similarly, in its default configuration, the Media Router assigns that same port number to all streaming devices (microphones and cameras), starting with the specified IP address, and adding 1 for every new device it encounters.
7. If your system has a has a lot of multicast traffic, turn on the **Increment ports** option (off by default).

   When this option is turned on, the Media Router increments the port number by 2 for every multicast address. Even port numbers are used for data transmission, while odd port numbers are used for RTCP control messages. This strategy is used to overcome a known Windows limitation that puts a cap on the bandwidth of a single port at around 100 Mbps. When the maximum value (65535) is reached, the port number restarts from the value that you configured.
8. Add or change the redirector configurations.
9. Click **Apply**.

Related Topics

Adding networks on page 155

Setting up a Security Center Federation™ on page 275

Adding redirectors to the Media Router

To reach clients on remote networks or balance the redirection workload between multiple servers, you can create redirector agents on additional servers.

What you should know

Redirectors are servers assigned to host *redirector agents*. A redirector agent is a software module launched by the Media Router to redirect data streams from one IP endpoint to another. The Media Router automatically creates a redirector agent on every server assigned to an Auxiliary Archiver role.

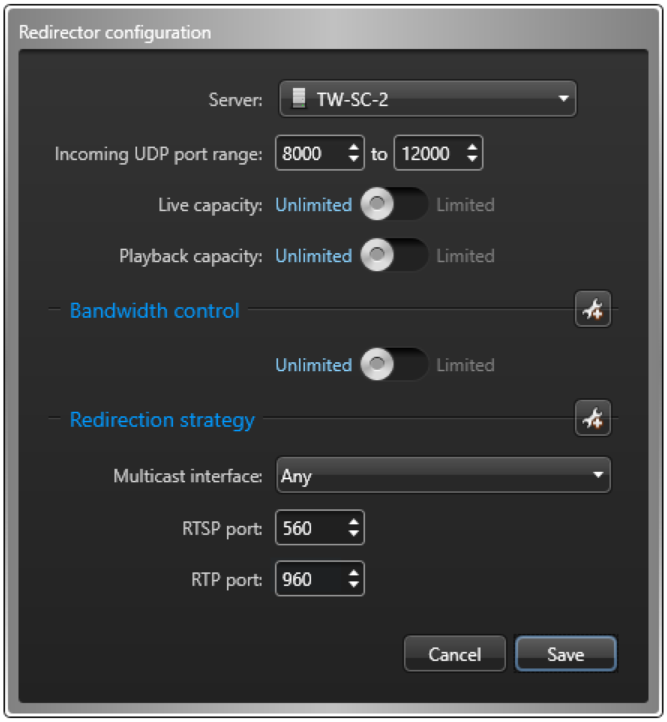
To add a redirector to the Media Router role:

1 Open the *System* task and click the **Roles** view.

2 Select the Media Router, and click the **Properties** tab.

3 Click **Add an item** (➕).

4 In the *Redirector configuration* dialog box, configure the redirector settings as follows:



Redirector configuration

Server: TW-SC-2

Incoming UDP port range: 8000 to 12000

Live capacity: Unlimited Limited

Playback capacity: Unlimited Limited

Bandwidth control

Unlimited Limited

Redirection strategy

Multicast interface: Any

RTSP port: 560

RTP port: 960

- **Server:** Server selected to host the redirector agent.
- **Incoming UDP port range:** Range of ports used by the redirector agent to send video using *UDP*. If the redirector agent is running behind a firewall, ensure that these ports are unlocked for inbound packets for UDP connections.
- **Live capacity:** Limit the maximum number of live streams that can be redirected through this server (redirector). This feature prevents overloading the server with too many users who are simultaneously trying to view video that needs redirection. When the limit is reached, an error message is displayed on the client application when users request live video, stating that the live stream capacity is exceeded.
- **Playback capacity:** Limit the maximum number of playback streams that can be redirected through this server (redirector). This feature prevents overloading the server with too many users who are simultaneously trying to view video that needs redirection. When the limit is reached, an error

message is displayed on the client application when users request playback video, stating that the playback stream capacity is exceeded.

- **Bandwidth control:** Limit the maximum bandwidth for video streams that are redirected through this server (redirector). You can also set a different bandwidth limit for live and playback video. This feature prevents overloading the network with too many video streams coming from a remote site that has limited bandwidth.

  When the limit is reached and users request a new video stream, an error message displays stating that the bandwidth limit is exceeded. If the bandwidth limit is reached and a user with a high *user level* requests a stream, the user with the lowest user level who is viewing video that is being redirected from that redirector loses their stream connection. If multiple users with the same user level are viewing redirected video streams, the user who requested the video stream last loses the stream connection.
- **Redirection strategy:** If you have multiple network cards, you can specify the actions performed by each network card. For example, you might want to specify that video export and video transfer can only be performed by your Wireless network card. For more information, see Configuring network card usage for a redirector on page 599.

  NOTE: By default, all actions are performed on the connected network card with the highest priority.
- **Multicast interface:** Network adaptor to use for streaming data in multicast mode.
- **RTSP port:** Port used by the redirector agent to receive TCP commands.

  NOTE: If you configure the redirector agent on the server hosting the Media Router, the RTSP port cannot be the same as the one used by the Media Router.
- **RTP port:** Port used by the redirector agent to stream live video data using TCP.

5 Click **Save** > **Apply**.

Configuring network card usage for a redirector

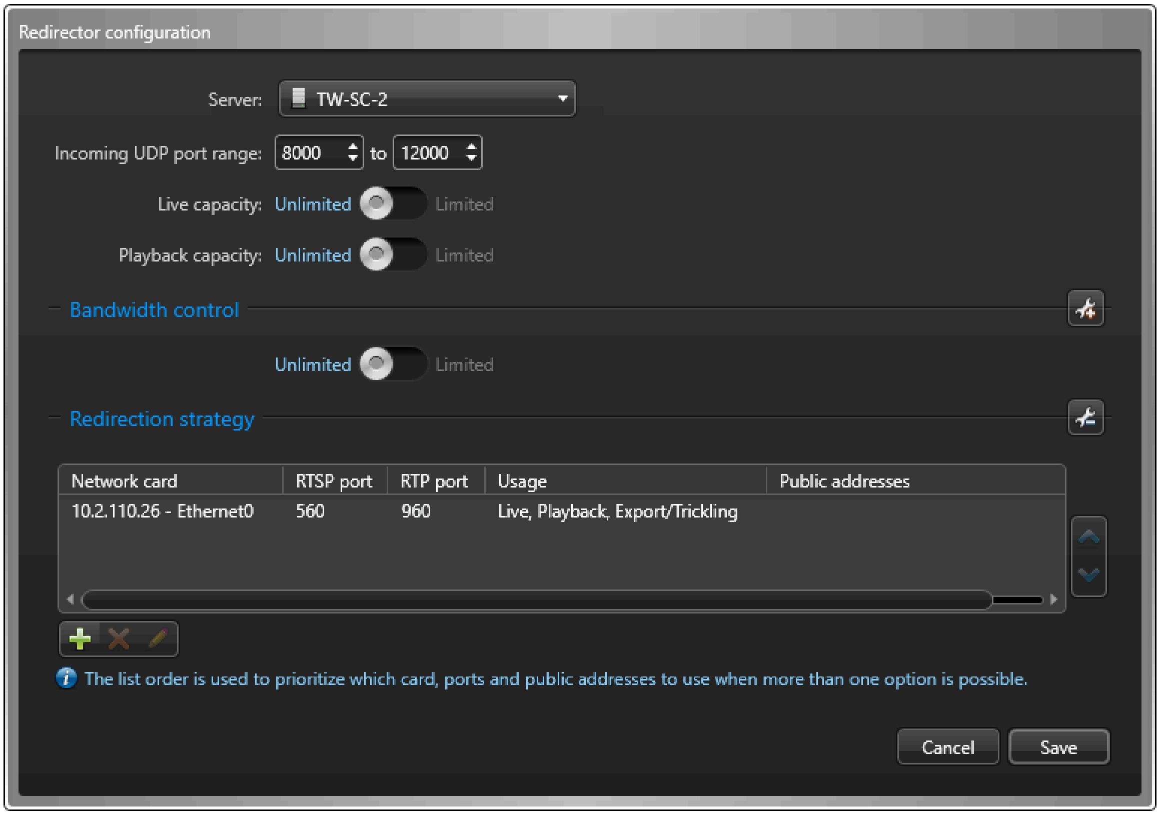
You can configure a redirector to use different network cards for specific actions. For example, you can specify that export and video transfer only be performed by your wireless network card. You can also assign multiple public addresses to the same network card to take advantage of multiple network options.

To configure the network card use for a redirector:

1. Open the *System* task and click the **Roles** view.
2. Select the Media Router, and click the **Properties** tab.
3. From the **Redirectors** list, select the redirector you want to configure and click **Edit the item** (✏).

   The *Redirector configuration* window opens.

4 Beside *Redirection strategy*, click **Advanced** (⚙).



Redirector configuration

Server: TW-SC-2

Incoming UDP port range: 8000 to 12000

Live capacity: Unlimited Limited

Playback capacity: Unlimited Limited

Bandwidth control

Unlimited Limited

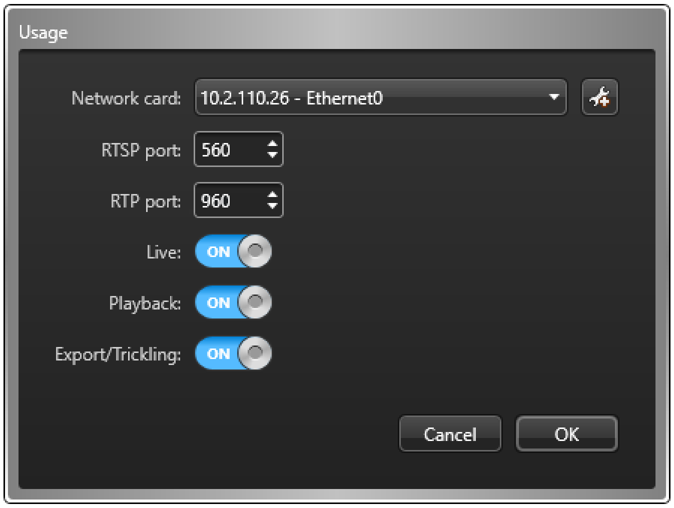
Redirection strategy

Network card	RTSP port	RTP port	Usage	Public addresses
10.2.110.26 - Ethernet0	560	960	Live, Playback, Export/Trickling	

The list order is used to prioritize which card, ports and public addresses to use when more than one option is possible.

5 Click **Add** (✚).

6 In the *Usage* dialog box, select the network card you want to configure.



Usage

Network card: 10.2.110.26 - Ethernet0

RTSP port: 560

RTP port: 960

Live: ON

Playback: ON

Export/Trickling: ON

7 Enter the **RTSP port** (control channel) and the **RTP port** (data channel).

8 Enable the actions you would like to assign to the selected network card. You can choose from the following:

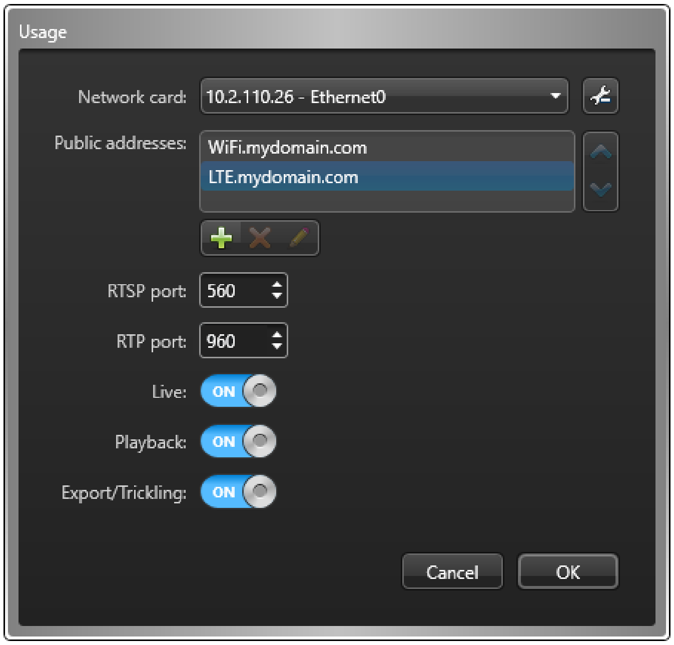
- **Live**
- **Playback**
- **Export/Trickling**

IMPORTANT: You cannot add the same network card and port combination twice; the network card and port number combination must be unique. For the same network card, the two port numbers must be different. You can block a certain type of strream on that redirector by disabling its corresponding action.

9 To configure multiple public addresses for the same network card, click **Add public address override** ().

This configuration might be necessary if a standalone Security Center system is installed on a moving vehicle, such as a train or a bus. The system on the vehicle is federated by a central system at the main terminal. When the vehicle is away from the main terminal, the central system communicates with the remote system through the cellular network. When the vehicle is near the main terminal, the central system switches to the Wi-Fi network because it is cheaper and has a higher bandwidth.

10 Click **Add** (✚) to add public addresses.



Usage

Network card: 10.2.110.26 - Ethernet0

Public addresses: WiFi.mydomain.com, LTE.mydomain.com

RTSP port: 560

RTP port: 960

Live: ON

Playback: ON

Export/Trickling: ON

IMPORTANT: If you decide to override the public address of the redirector configured in Server Admin, ensure the following:

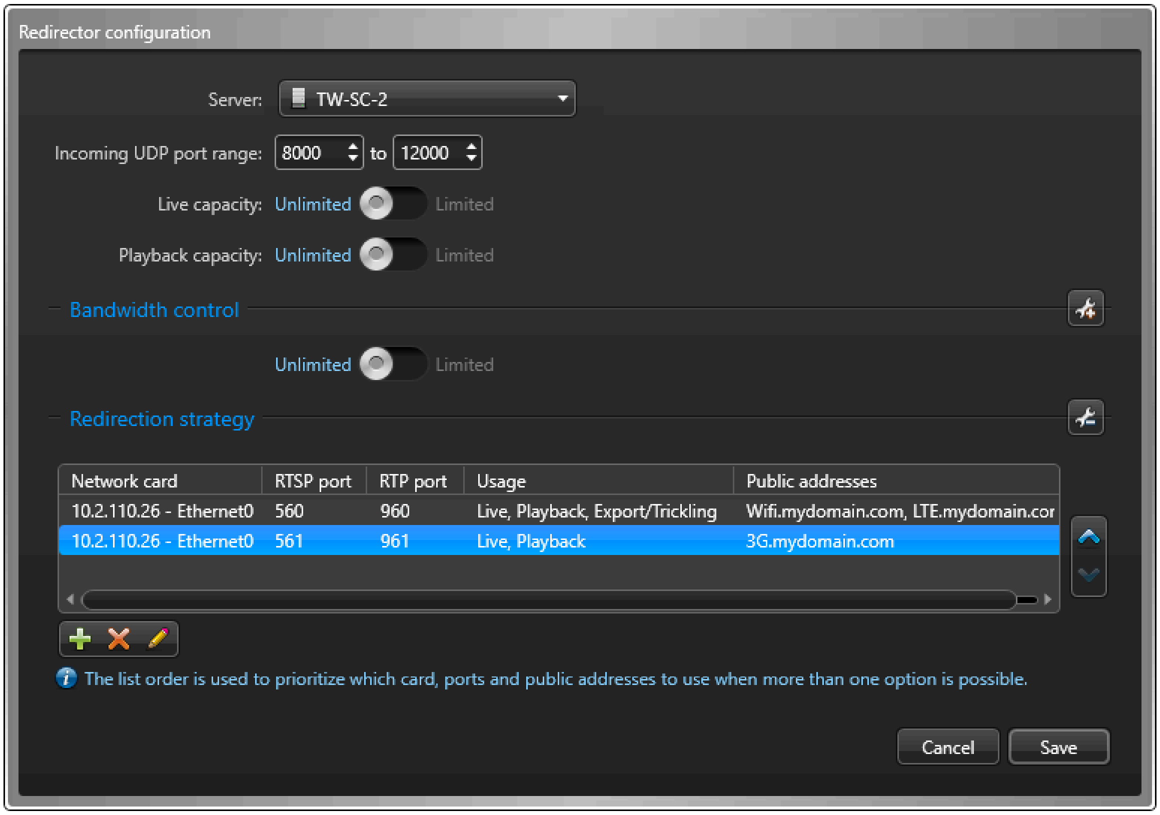
- The network route being used is set to public (**Use of private address** is turned off). See Creating direct connections between networks on page 155.
- The public address on your redirector is configured. See Server Admin - Expansion server page on page 105.

11 Click **OK**.

12 (Optional) Change the network card priority.

a) In the *Redirector configuration* window, select a card from **Network card** list.

b) Click the ⌄ or ⌃ buttons to move it to the top or bottom of the list.



Redirector configuration

Server: TW-SC-2

Incoming UDP port range: 8000 to 12000

Live capacity: Unlimited Limited

Playback capacity: Unlimited Limited

Bandwidth control

Unlimited Limited

Redirection strategy

Network card	RTSP port	RTP port	Usage	Public addresses
10.2.110.26 - Ethernet0	560	960	Live, Playback, Export/Trickling	Wifi.mydomain.com, LTE.mydomain.cor
10.2.110.26 - Ethernet0	561	961	Live, Playback	3G.mydomain.com

The list order is used to prioritize which card, ports and public addresses to use when more than one option is possible.

In the example illustrated in the screen capture, the redirector is only equipped with one network card. If live or playback video is requested from that system, the Media Router will always try the Wi-Fi network first, followed by the LTE network, followed by the 3G network. For video export and trickling, only the Wi-Fi and LTE networks can be used.

13 Click **Save** > **Apply**.

- To edit the settings for a network card, select it from the network card list and click **Edit the item** (✎).
- To delete a network card, select it from the network card list and click **Delete** (✗).

Viewing Archiver statistics

You can view the operation statistics of all archiving roles (Archiver and Auxiliary Archiver) in your system using the *Archiver statistics* report.

What you should know

You can view more details about each archiving role, such as the average disk usage per day, the protected video file statistics, and the statistics of each individual camera, by going to the *Resources* page of the archiving role in Config Tool and clicking **Statistics** (●).

To view Archiver statistics:

1 From the Config Tool home page, open the *Archiver statistics* task.

2 In the **Archiver** filter, select the archiving roles you want to investigate.

3 Click **Generate report**.
The operation statistics of the selected archiving roles are listed in the report pane.

Related Topics

Viewing recording states of cameras on page 587
Monitoring disk space available for video files on page 665
Overview of the System status task on page 382

Report pane columns for the Archiver statistics task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Archiver statistics task.

- **Entity:** Entity name.
- **Server:** Name of the server hosting this role.
- **Active cameras:** Number of cameras detected by the Archiver.
- **Archiving cameras:** Number of cameras that have archiving enabled (Continuous, On event, or Manual) and that are not suffering from any issue that prevents archiving.

  See details: View the *recording state* and statistics of each individual camera in the *Archiving cameras* dialog box. The statistics are taken from the last refresh of the *Statistics* dialog box. This report allows you to verify whether each encoder is currently streaming video (and audio), whether the Archiver is currently recording the data, and the rate at which the events were received from the cameras over the last minute.
- **Total number of cameras:** Total number of cameras assigned to this role.
- **Used space:** Amount of space used by video archives.
- **Free space:** Free space on disk.
- **Available space:** Available free space for video archives (equals *Free space on disk* minus *Min. free space*).
- **Load percentage:** Percentage of space used over the allotted space.
- **Archiver receiving rate:** Rate at which the Archiver is receiving data.
- **Archiver writing rate:** Rate at which the Archiver is writing to disk.
- **Estimated remaining recording time:** Number of days, hours, and minutes of recording time remaining based on the average disk usage and the current load.
- **Network traffic in:** Incoming network traffic bit rate on this computer.
- **Network traffic out:** Outgoing network traffic bit rate on this computer.
- **Archiving span:** Time bracket in which video archives can be found.

Investigating Archiver events

You can search for events related to archiving roles (Archiver and Auxiliary Archiver) using the *Archiver events* report.

What you should know

You can check the status of an Archiver by selecting it, setting the time range to one week, and making sure there are no critical events in the report. You can also troubleshoot an Archiver by searching for important events, such as *Disk load threshold exceeded* or *Cannot write to any drive*, and see when those events occurred.

TIP: You can monitor incoming camera events on the Archiver and be notified if an unusually high event rate is occurring. This allows you to investigate, take action, and prevent performance issues.

To investigate Archiver events:

1. From the Config Tool home page, open the *Archiver events* task.
2. Set up the query filters for the report. Choose from one or more of the following filters:
   - **Archiver:** Select the archiving roles (Archiver and Auxiliary Archiver) you want to investigate.
   - **Event timestamp:** Define the time range for the query. You can define the time range for a specific period or a relative period, such as the previous week or the previous month.
   - **Events:** Select the events of interest. The available event types depend on the task you are using.
   - **Custom fields:** Restrict the search to a predefined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
3. Click **Generate report**.

   The Archiver events are listed in the report pane.

Report pane columns for the Archiver events task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Archiver events task.

- **Custom fields:** Predefined custom fields for the entity. The columns only appear if custom fields are defined for the entity and were made visible to you when they were created or last configured.
- **Description:** Description of the event, activity, entity, or incident.

  IMPORTANT: To comply with State laws, if the **Report generated** option is used for an Activity trails report that contains ALPR data, the reason for the ALPR search is included in the **Description** field.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **Source (entity):** The name of the system the camera belongs to.

About the Media Gateway role

The Media Gateway role is used by Genetec™ Mobile, Web Client, and the Genetec™ Web App to get transcoded video from Security Center. The Media Gateway role supports the Real Time Streaming Protocol (RTSP), which external applications can use to request raw video streams from Security Center.

When is video transcoding necessary?

Video transcoding is the conversion of a video stream from one video codec to another. Transcoding is used for the following reasons:

- The client application does not support the codec used by the camera.
- To reduce latency. For example, to downscale a high-resolution video when the PTZ camera is being moved.
- To reduce bandwidth. For example, to downscale a high-resolution video when it is viewed on a mobile device.

Transcoding is very CPU intensive and requires high-end servers. Adding a dedicated GPU card is recommended. Depending on your equipment and needs, you can decide to disable transcoding or only allow it under certain conditions.

When do you need raw video streams?

There are many uses for raw (not transcoded) video streams. For example, an external system can use the raw video streams to perform video analytics and trigger events. Another application can display video on a web page using a commonly available viewer that supports the camera's specific encoding.

Media Gateway features

- RTSP and RTSPS (through TLS) are supported following the RFC 2326 standard.
- IPv6 multicast is supported.
- GPU hardware acceleration is supported.
- Live and playback video can be requested.
- Load distribution can be enabled by assigning multiple servers to this role.

Scope and limitations

- Federated Omnicast™ 4.x streams are not supported.
- Non-video streams such as audio, PTZ commands, overlays, and metadata are not supported.
- IPv6 multicast is only used under the following conditions:
  - Both the client and the server have IPv6 enabled. Otherwise, the system falls back to IPv4.
  - The initial setup request was done using IPv6. Otherwise, the system falls back to IPv6 unicast.

Creating Media Gateway roles

Before you can request live and playback video and receive raw video streams using the RTSP protocol, you must first create at least one Media Gateway role in your system with Config Tool.

Before you begin

Ensure that the *Number of Media Gateway RTSP streams* option in your Security Center license supports at least one stream.

What you should know

A Media Gateway role is created by default if your Security Center license supports mobile devices or web connections (*Number of mobile and web connections* > 0).

To create a Media Gateway role:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 At the bottom of the page, click ▾ beside **Video unit**, and then click **Media Gateway**.

3 On the *Specific info* page, select the **Server** to host the role on, and then click **Next**.

This step is skipped if you have only one server in your system.

4 On the *Basic information* page, enter a name and description for the role.

5 If there is a **Partition** field, select the partition this role is a member of.

Partitions determine which Security Center users have access to this entity. Only users who have been granted access to the partition can see this role.

6 Click **Next** > **Create** > **Close**.

A new Media Gateway role ( ) is created.

After you finish

Configure the Media Gateway role.

Related Topics

License options in Security Center on page 1447

Configuring Media Gateway roles

You can enable the RTSP protocol on your system or improve the streaming performance of the Web Server role by changing the settings of the Media Gateway role it is assigned to.

Before you begin

If you want to enable the RTSP protocol, the *Number of Media Gateway RTSP streams* option in your Security Center license must be greater than zero.

What you should know

The RTSP protocol is disabled by default for security reasons. If you enable it, we recommend that you also enable **User authentication**.

To configure the Media Gateway role:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Click the Media Gateway role you want to configure and click the **Resources** tab.
3. (Optional) Change the role's primary server.
4. To configure load distribution for the Media Gateway, add servers to the role.
    a) Click the **Resources** tab.
    b) Under the **Servers** list, click **Add an item** (✚).
       A dialog box opens, listing all remaining servers on your system not assigned to the role.
    c) Select the server you want to add, and then click **Add**.

    All video streaming requests are distributed among the listed servers.
5. Click the **Properties** tab.
6. (Optional) Enable the RTSP protocol.
    a) Under the *RTSP* section, turn on the **Enable** option.
    b) Ensure that the default **Start multicast address** and port settings for IPv4 and IPv6 do not conflict with other roles, such as the Archiver roles, the Media Router role, the redirectors, and other applications on your system.

       In multicast, all video sources are streamed to different multicast addresses using the same port number, because multicast switches and routers use the destination IP address to make their routing decisions. Similarly, the Media Gateway assigns that same port number to all streaming cameras, starting with the specified IP address and incrementing the IP address by 1 for each new camera it encounters.
    c) If the default **Listening port** (654) conflicts with other roles or applications on your server, select a different port number.
    d) Turn on the **Require TLS (RTSPS)** option to force RTSP client applications to use secure transport (TLS) to communicate with this Media Gateway role.
    e) Turn on the **User authentication** option to limit the user accounts that RTSP client applications, such as third-party video analytics software, can use to communicate with this Media Gateway role.

       If you disable this option, anyone can connect to the Media Gateway. We recommend that you enable this option to heighten the security of your system; however, you can disable it if you know that your network is secure.

       NOTE: The cameras that an RTSP client application can view in the system depend on the user account the client uses to log on to Security Center. If RTSPS is disabled, you must specifically add the users you allow to access this Media Gateway role to the **Accessible to** list. Assign to each user a different password than the one used for connecting to Security Center to minimize the risks of exposing their Security Center passwords. If RTSPS is enabled, the Media Gateway uses regular Security Center credentials to validate access. Moreover, the Security Center users must have the *Log on using the SDK* privilege.

7 If necessary, change the default HTTP ports and URL used to connect to this Media Gateway role.

Turn off the **Use the default web ports of the server** option if you need to make changes. The format of the URL is *https://host:port/web address*, where *host* is the IP address or host name of the server that hosts the Media Gateway role, *port* is the HTTP port or the HTTPS port, and *web address* is media by default.

8 If necessary, change the default settings for streaming video to the Web Client or Genetec™ Web App.

Decide between one of the five standard streams: *Live*, *Recording*, *Remote*, *Low resolution*, *High resolution*, or *Automatic*.

With the *Automatic* option, the Media Gateway decides between the *Low resolution*, the *Live*, or the *High resolution* stream, based on the resolution of the viewing tile in the browser. The following thresholds help the Media Gateway make that decision.

- **Low resolution to Live:** Resolution at which the Media Gateway decides to use the *Live* stream. Below this resolution, the Media Gateway uses the *Low resolution* stream.
- **Live to High resolution:** Resolution at which the Media Gateway decides to use the *High resolution* stream.

9 Decide whether the Media Gateway should be allowed to transcode and in what situation.

Transcoding is very CPU intensive and requires high-end servers. You have the following options:

- **Never:** The Media Gateway never transcodes. If the client device cannot decode the stream, the error "Unsupported codec" is displayed.
- **Only for PTZ control and Mobile Server:** The Mobile Server role can request transcoded streams at any time. Other applications can only use transcoding to reduce video latency while the user is controlling a PTZ, otherwise an error message is displayed.
- **Always (for unsupported devices and codecs):** The Media Gateway transcodes when:
  - The client application requests it.
  - PTZ camera is being moved (to reduce latency).
  - The codec used by the camera is not supported by the client application.

10 If you allow the Media Gateway to transcode, configure the following settings:

- **Maximum resolution for MJPEG transcoding:** When transcoding, downscale the resulting transcoded stream to this resolution. Stream that are not transcoded are untouched.
- **Frame rate:** Maximum frame rate of the resulting transcoded stream.

11 Click **Apply**.

Related Topics

Configuring video streams of cameras on page 616

Media Gateway configuration tabs on page 1367

License options in Security Center on page 1447

Limiting Media Gateway connections

You can limit the number of simultaneous live and playback connections that the Media Gateway role will accept by generating a configuration file (gconfig).

What you should know

- If you save the gconfig file on the machine hosting the Media Gateway role, the configuration is forwarded to all Agent machines. If you require a unique configuration on a specific Agent machine, you can save a modified gconfig file on the Agent machine.
- Both RTSP and web interface connections are included in the total number of connections.

To limit Media Gateway connections:

1. Create the following *mediagateway.gconfig* file where *n1* is the maximum simultaneous number of live connections and *n2* is the maximum simultaneous number of playback connections that the Media Gateway role accepts.

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <configuration>
     <MediaGateway MaximumLiveSessionCount="n1" MaximumPlaybackSessionCount="n2"></
   MediaGateway>
   </configuration>
   ```

   NOTE:

   - The default value is *0* and allows an unlimited number of connections.
   - A negative value prevents any connections.

2. Save the *mediagateway.gconfig* file to the Security Center installation folder.

   On a 64-bit machine, the default location is *C:\Program Files (x86)\Genetec Security Center 5.11\ConfigurationFiles*.

   NOTE:

   - Saving the file to the machine hosting the Media Gateway role configures that machine and all Agent machines.
   - Saving the file to an Agent machine configures only that machine.

3. Restart the role.

   NOTE:

   - If you saved the gconfig file to the machine hosting the Media Gateway role, restart the role.
   - If you saved the gconfig file to an Agent machine, restart the machine.

About the Genetec™ Web Player Library

The Genetec™ Web Player is a web library used to display Security Center camera audio and video in any web page.

This library is intended for web developers and is designed to be used with Javascript or Typescript code. It is lightweight and easy to integrate in existing web pages because it doesn't depend on any other library or framework.

The Genetec™ Web Player library can be used to show live streams, control PTZ cameras, and play back recorded sequences. It also provides a list of time ranges that can be used to create timeline controls. The integrated player supports various play speeds along with pause and resume commands.

The website displaying the library must be hosted on an independent web server. After loading the webpage in your browser, the Genetec™ Web Player must be connected to an accessible Security Center Media Gateway. WebSocket protocol is used for this connection.

By default, transcoding is disabled on the Media Gateway role because of its intensive CPU requirement. As a result, video codecs incompatible with your browser are not playable and an Unsupported codec error is displayed in the player. If full compatibility with all cameras is required, you can enable transcoding in Media Gateway role configurations.

NOTE: Transcoding is required for the Mobile Server, to optimize PTZ camera latency, and for codecs other than MJPEG and H.264.

For more information on Genetec™ Web Player integration, see the *Security Center SDK Help* guide provided through GTAP.

Configuring the Media Gateway role for the Genetec Web Player

To display cameras from the Genetec™ Web Player library in your independent web page, it must be connected to properly configured Media Gateway role.

Before you begin

Ensure the following conditions:

- The Media Gateway role is created in your system.
- You have your own web server to host the independent web page.
- You have a valid SDK certificate.
- The Genetec™ Server is using a valid certificate, not self-signed, containing the server's public address.

To configure the Media Gateway role for use with the Genetec™ Web Player:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. In the entity tree, select the Media Gateway role, and click the **Properties** tab.
3. In the **HTTP** section, enable the **Use the default web ports of the server** setting to ensure port 80 and 443 are available to the Genetec™ Web Player.
4. Note the **Web address** entry.

   It is required for integrating the player in your web page.
5. In the **Video streaming** section, select the desired **Default live stream** setting.
6. Allow transcoding as needed.

   NOTE: Transcoding is required for the use of the Mobile Server, the optimization of PTZ camera latency, and for certain codecs.
7. Click **Apply**.
8. Click the **Resources** tab.
9. (Optional) Change the role's primary server.
10. (Optional) Add servers to the role to configure load distribution for the Media Gateway.
11. Click **Apply.**

28

Cameras

This section includes the following topics:

About cameras (video encoders)

A camera entity represents a single video source in the system. The video source can either be an IP camera, or an analog camera that connects to the video encoder of a video unit. Multiple video streams can be generated from the same video source.

A video encoder is a device that converts an analog video source to a digital format using a standard compression algorithm (H.264, MPEG- 4, or M-JPEG). The video encoder is one of many devices found on a video unit.

Each video encoder can generate one or multiple video streams using different compression schemes and formats for different usages. In an IP camera, the camera and the video encoder are an inseparable unit, and the two terms are often used interchangeably.

Cameras (or video encoders) are automatically created when you add the video units they are part of to Security Center.

About video streams

Most video encoders and IP cameras supported by Security Center can generate multiple video streams from the same video source.

When a camera has multiple video streams, you can define different video quality settings for the live monitoring stream and the recording stream. Additional streams can also be configured for other needs, such as low bandwidth for remote access or low resolution versus high resolution streams.

Each video stream is defined by the following settings:

- **Video quality:** The quality of the video stream, made up of parameters such as image resolution, *bit rate*, frame rate, and so on, that varies by manufacturer. The video quality can have multiple configurations for different *schedules*. Video quality directly affects your bandwidth and archiving disk space.
- **Stream usage:** The purpose of the video stream, and when it is used: for live video, recordings, and so on.
- **Network settings:** The specific connection type and *multicast* address that is configured for the stream, based on the stream's usage and your network configuration.

Automatic stream selection

Displaying high-resolution video requires a lot of CPU power. To display the maximum number of live video streams simultaneously in Security Desk, you should optimize CPU use.

You can configure Security Desk to use *Automatic* video stream mode. When this mode is selected, Security Desk displays the *Low resolution* or *High resolution* stream, depending on the size of the selected canvas tile. The video stream that has an image resolution equal to, or lower than, the display area of the tile is selected.

The video stream also changes dynamically when the user resizes the Security Desk window, or changes the *tile pattern*.

NOTE: When *Automatic* mode is selected as the default viewing stream in Security Desk, the *High resolution* stream is always used when a tile is maximized, or when the digital zoom is in use.

For more information about changing the default live stream in Security Desk, see the *Security Center User Guide*.

Configuring camera settings

For optimal performance, configure your camera settings after the video units have been added in Security Center.

What you should know

Security Center provides default settings; however, we recommend that you go through the configuration of each entity to get the best results.

NOTE: For federated cameras, only the settings in the **Identity** and **Video analytics >Visual tracking** tabs are configurable.

To configure a camera:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the camera to configure.
3. Configure the video streams for the encoder to generate.
4. Configure specific recording settings for the camera.

   If you do not configure specific settings for the camera, it follows the recording settings for the archiving roles (Archiver and Auxiliary Archivers) that control it.

   NOTE: If a camera has been configured for archive transfer, recording can only be configured using its web page.
5. Configure the motion detection settings for the camera.
6. (Optional) Configure the privacy protection settings for the camera.

   NOTE: The **Privacy protection** tab is only displayed if you have a privacy protection license. For more information, see "Configuring privacy protection on cameras" in the *KiwiVision™ User Guide for Security Center*.
7. Adjust the camera’s video attributes (brightness, contrast, hue, saturation) to account for different times of the day.
8. Configure Visual tracking so users can switch to adjacent cameras by clicking a camera in a Security Desk tile.
9. Click the **Hardware** tab, and associate hardware devices to the camera if they are not built-in.
   - **PTZ motors:** Configure the PTZ motor.
   - **Microphones:** Select a microphone from the **Microphone** drop-down list.
   - **Speakers:** Select a speaker from the **Speaker** list.
   - **Image rotation:** Use this setting to correct the orientation of the image when the camera is mounted upside down or at a 90 degree angle. This method uses the camera's capability to perform image rotation.
     - This feature is only available if it is supported by the camera hardware.
     - The rotation options vary depending on the model of the camera.
     - Using the *Image rotation* feature is preferable to using the *Video rotation* feature, if it does not adversely affect video frame rate.
   - **Video rotation:** Use this setting to correct the orientation of the image when the camera is mounted upside down or at a 90 degree angle. This method uses Security Center to rotate the video.
     - Using *Video rotation* adds extra load on client workstations, so *Image rotation* is preferable if it is available for the camera.
     - This feature is not available for PTZ cameras or cameras that use panomorph (fisheye) lenses.
10. If the camera includes interchangeable lenses, select the correct **Lens type**.
11. Click **Apply**.

12 Test the video settings you have configured.

After you finish

You can copy the settings you configured for this camera to other cameras of the same model.

Configuring video streams of cameras

Before you start monitoring video in Security Desk, you should decide how you want to use each video stream, and configure the appropriate settings for it.

What you should know

Every video stream setting affects your bandwidth and archive storage. You must find a balance between quality, CPU usage, and disk space.

Security Desk only switches to a higher resolution when it makes a visual difference to the users. Therefore, make sure the *Live* stream has a better resolution than the *Low resolution* stream, and that the *High resolution* stream has a better resolution than the *Live* stream.

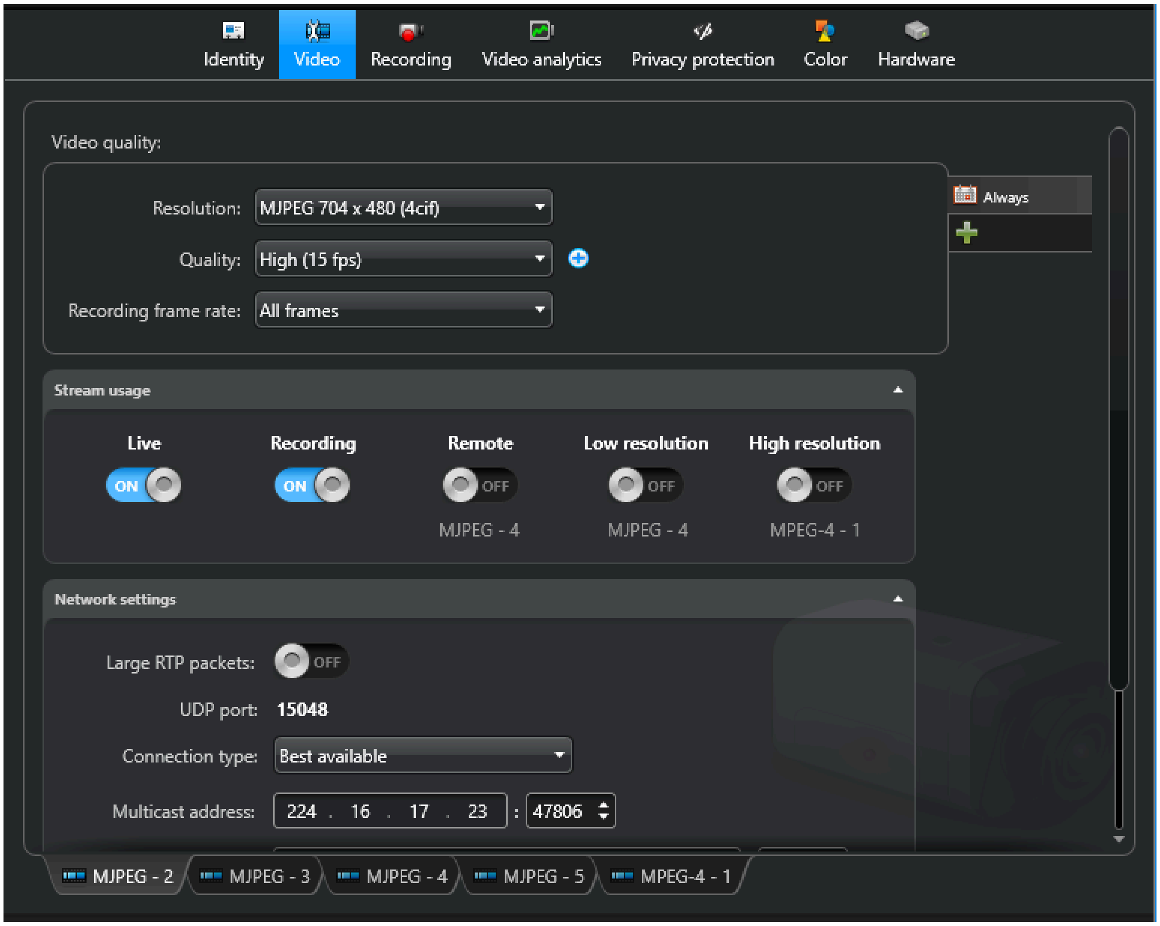
To configure a camera's video streams:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Select the camera to configure, and then click the **Video** tab.

3 If the camera supports multiple video streams, select a video stream tab at the bottom of the **Video** tab.

4 In the *Video quality* section, set the video quality settings (resolution, frame rate, and so on) for the selected video stream.



Video quality:

Resolution: MJPEG 704 x 480 (4cif)

Quality: High (15 fps)

Recording frame rate: All frames

Always

Stream usage

Live	Recording	Remote	Low resolution	High resolution
ON	ON	OFF	OFF	OFF
		MJPEG - 4	MJPEG - 4	MPEG-4 - 1

Network settings

Large RTP packets: OFF

UDP port: 15048

Connection type: Best available

Multicast address: 224 . 16 . 17 . 23 : 47806

5 In the **Stream usage** section, specify the purpose for the selected video stream.

   NOTE: A stream can be assigned all, some, or none of the usage options. A stream that has no usage assigned is not generated by the video encoder, which conserves CPU on the unit.

   - **Live:** Default stream used for viewing live video in Security Desk.
   - **Recording:** Stream recorded by the Archiver for future investigation.

     TIP: The quality of the recording stream can be temporarily boosted when the recording is triggered by certain types of events.
   - **Remote:** Stream used for viewing live video when the bandwidth is limited.
   - **Low resolution:** Stream used instead of the *Live* stream when *Automatic* is selected for **Live stream** in Security Desk and the tile used to view the stream is small.
   - **High resolution:** Stream used instead of the *Live* stream when *Automatic* is selected for **Live stream** in Security Desk and the tile used to view the stream is large.

6 In the *Network settings* section, click **Connection type** and select how communication between the Archiver and the camera is established for sending or receiving video streams:

   - **Best available:** Lets the Archiver select the best available connection type for the stream. The best available types rank in this order, according to availability:
     - Multicast (not available for the recording stream).
     - UDP
     - TCP
     - RTSP over HTTP
     - RTSP over TCP
   - **Unicast UDP:** Forces the stream to be sent in UDP to the Archiver. The stream must be formatted using the RTP protocol.
   - **Unicast TCP:** Forces the stream to be sent in TCP to the Archiver. Here, TCP is taken in the broad sense. For some types of cameras, the Archiver establishes a TCP connection to the unit and receives the stream in a proprietary protocol. For others, the stream is sent over HTTP. Typically, the stream is not formatted according to the RTP protocol by the unit. The Archiver has to convert the stream to the RTP protocol to be archived or retransmitted to the system.
   - **RTSP stream over HTTP:** This is a special case of TCP connection. The Archiver uses the RTSP protocol to request the stream through an HTTP tunnel. The stream is sent back through this tunnel using the RTP protocol. This connection type is used to minimize the number of ports needed to communicate with a unit. It is usually the best way to request the stream when the unit is behind a NAT or firewall, because requests sent to HTTP ports are easily redirected through them.
   - **RTSP stream over TCP:** This is another special case of TCP connection. The Archiver uses the RTSP protocol to request the stream in TCP. The request is sent to the RTSP port of the unit.

7 Click **Apply**.

8 Configure the other video streams available on the camera.

Related Topics

Camera - Video tab on page 1252

Boosting video recording quality on important events on page 618

Boosting video recording quality on important events

To provide adequate support for future investigation of video footage, you can increase the video quality of the recording stream when important events occur.

What you should know

To save storage space, the video stream used for recording is typically of a lower quality (lower frame rate or lower image resolution) than the stream used for live viewing.

Boost quality on event recording settings have priority over the *Boost quality on manual recording* settings. The length of the video quality boost depends on the event type, and the camera’s recording settings.

To boost video recording quality on important events:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Select the camera to configure, and then click the **Video** tab.

3 Turn **ON** one or both of the automatic boost quality settings:

- **Boost quality on manual recording:** Temporarily boosts video quality when a Security Desk user manually starts the recording by clicking the *Record* (●) button or the *Add bookmark* () button.
- **Boost quality on event recording:** Temporarily boosts video quality when a system event triggers the recording: the *Start recording* action was executed, an *alarm* was triggered, or because of a motion event.

4 In the *Video quality* section, configure the boost quality settings.

5 Click **Apply**.

Boosting video recording quality manually

You can boost the video quality of the recording stream using a manual action.

Before you begin

The video quality settings for the recording stream during *Boost quality on manual recording* and *Boost quality on event recording* must be configured in the camera's **Video** tab.

What you should know

When the video quality is boosted through an action, the custom boost quality settings override the general settings for event recording until you trigger another action, or until the Archiver restarts.

To boost video recording quality manually:

1 In the Security Desk notification tray, click **Hot actions** ().

2 In the *Hot actions* dialog box, click **Manual action**.

3 In the *Configure an action* window, select one of the following action types, and select a camera:

- **Override with manual recording quality:** Turn the **Boost quality on manual recording** option to **ON**.
- **Override with event recording quality:** Turn the **Boost quality on event recording** option to **ON**.

4 Click **OK**.

The custom boost quality settings for video recording are applied to the selected camera.

5 To return to the normal recording video quality settings:

   a) In the notification tray, click **Hot actions** (📢).

   b) In the *Hot actions* dialog box, click **Manual action**.

   c) Select the **Recording quality as standard configuration** action, and select a camera.

   d) Click **OK**.

Changing multicast addresses of cameras

If you are short of multicast addresses, you can use the same multicast address for multiple cameras, and assign a different port number to each.

What you should know

Since a multicast address and port number are automatically assigned to a video unit when it is discovered, you only need to edit the multicast addresses when you do not have enough of them (certain switches are limited to 128).

NOTE: Using the same multicast address on multiple encoders is less efficient than using a different address for each encoder, because it causes more network traffic.

To change the multicast address of a video encoder:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the camera to configure, and click the **Video** tab.
3. In the **Network settings** section, type the **Multicast address** and port number you want to use.

   NOTE: All multicast addresses must be between the range 224.0.1.0 and 239.255.255.255.
4. Click **Apply**.
5. To restart the video unit, select the unit in the roles and units view, and click **Reboot** (↩) in the toolbar at the bottom of the workspace.

Related Topics

Changing multicast ports of cameras on page 621

Changing multicast ports of cameras

If you have a large number of cameras streaming in multicast, you can improve your system performance by assigning a different multicast port number to each camera on your system.

What you should know

There is a known issue that causes Windows to use a lot of CPU to process multicast packets when they are on the same port. This issue effectively limits the maximum throughput on a single port at around 100 Mbps. By default, the system only increments the multicast address assigned to every video encoder it discovers, not the port numbers. If you frequently use multicast, you should also change the port number. For example, if you use Auxiliary Archiver roles or if everything is recorded in multicast.

To change the multicast port on all video encoders:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the Media Router and click the **Properties** tab.
3. In the *Multicast* section, turn on the **Increment ports** option.
4. Click **Apply**.

To change the multicast port on a specific video encoder:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the camera to configure, and click the **Video** tab.
3. In the *Network settings* section, beside **Multicast address**, set the port number you want to use.
4. Click **Apply**.
5. To restart the video unit, select the unit in the roles and units view, and click **Reboot** (↩) in the toolbar.

   NOTE: If the new port is being used by another stream, your change is automatically reverted.

Related Topics

Changing multicast addresses of cameras on page 620

Testing video settings of cameras

After configuring your cameras, test that the video settings and make sure you can view the camera.

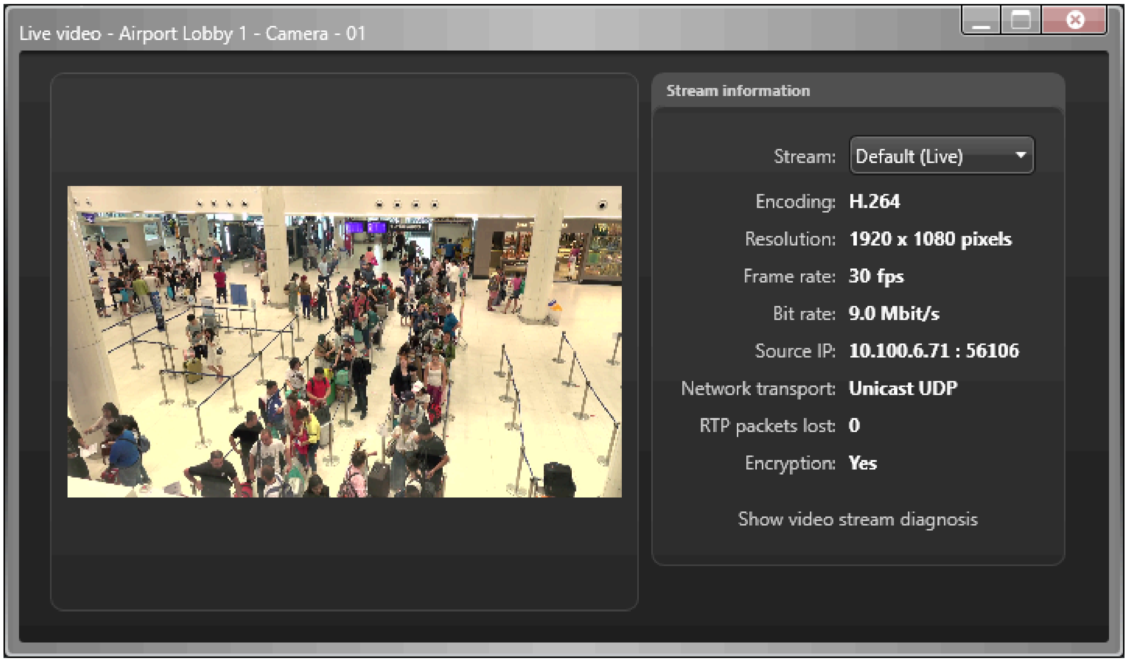
To test camera video settings:

1 In the *Video* task, double-click the camera you want to test in the entity tree.

The camera stream opens in a pop-up window.

2 Click **Expand** (☑).

The *Live video* dialog box opens and shows you live statistics about the video stream coming from the video encoder.



Live video - Airport Lobby 1 - Camera - 01
Stream information

Stream: Default (Live)

Encoding: H.264

Resolution: 1920 x 1080 pixels

Frame rate: 30 fps

Bit rate: 9.0 Mbit/s

Source IP: 10.100.6.71 : 56106

Network transport: Unicast UDP

RTP packets lost: 0

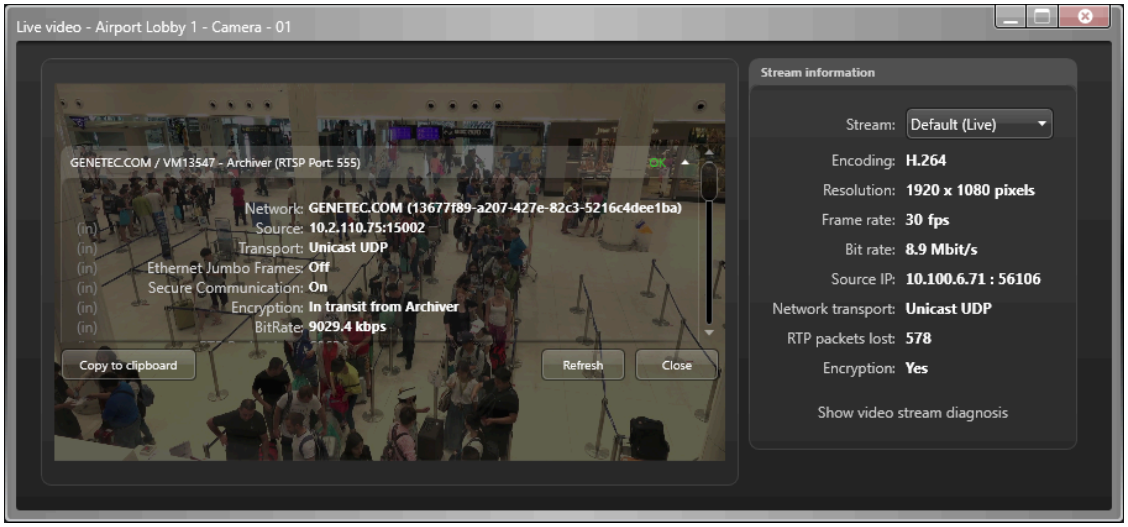
Encryption: Yes

Show video stream diagnosis

3 If you have configured multiple video streams, click the **Stream** list to select a different stream to view: live, recording, and so on.

4 If you have configured separate **High resolution** and **Low resolution** streams, select **Automatic** from the **Stream** drop-down list, and resize the *Live video* dialog box to test if the stream selection automatically changes.

5 If you are experiencing streaming problems, click **Show video stream diagnosis** > **Show video stream status** to display diagnostic information as a transparent overlay on the video.



Live video - Airport Lobby 1 - Camera - 01

GENETEC.COM / VM13547 - Archiver (RTSP Port: 555) OK

Network: GENETEC.COM (13677f89-a207-427e-82c3-5216c4dee1ba)
(in) Source: 10.2.110.75:15002
(in) Transport: Unicast UDP
(in) Ethernet Jumbo Frames: Off
(in) Secure Communication: On
(in) Encryption: In transit from Archiver
(in) BitRate: 9029.4 kbps

Stream information

Stream: Default (Live)
Encoding: H.264
Resolution: 1920 x 1080 pixels
Frame rate: 30 fps
Bit rate: 8.9 Mbit/s
Source IP: 10.100.6.71 : 56106
Network transport: Unicast UDP
RTP packets lost: 578
Encryption: Yes

6 To capture information, click **Copy to clipboard**.

7 To hide the status overlay, click **Close.**

About motion detection

Motion detection is the feature that watches for changes in a series of video images. The definition of what constitutes motion in a video can be based on highly sophisticated criteria.

For pre-configuration instructions or any additional configuration steps required to enable motion detection in Security Center for specific video units, see the *Security Center Video Unit Configuration Guide*.

There are two types of motion detection:

- **Software motion detection:** Motion detection is executed by the *Archiver* on the video stream set for recording, and motion events are generated by Security Center.
- **Hardware motion detection:** Motion detection is executed by the *video unit*, and motion events are generated by the unit and sent to Security Center.

Supported capabilities differ between the two types as shown in the following table:

Capability	Software	Hardware
Configuring motion detection settings	Config Tool	Unit's proprietary configuration tool[1]
Motion search task in Security Desk[2]	Yes	Limited support[3]
Shows motion indicators (green bars) in the timeline	Yes	See our Supported Device List[4]
Multiple motion detection zones	Yes	Camera-specific[5]
Requires additional server resources	Yes	No
Auto calibration of sensitivity[6]	Yes	No

IMPORTANT:

1. To ease configuration of hardware motion detection, motion blocks derived from software motion detection are shown in Config Tool.
2. The *Motion search* task does not support cameras using H.265 (HEVC) streams.
3. Only Axis cameras with legacy motion detection are supported.
4. For cameras with hardware motion detection, the green bars only indicate the presence of motion in the timeline (0% or 100%). For Axis cameras with legacy motion detection, the green bars also indicate the amount of motion as a percentage.
5. Not all units support multiple motion detection zones. If you switch motion detection from **Archiver** to **Unit**, existing zone configurations not supported by the unit are lost.
6. The unit and Archiver might interpret sensitivity differently, so testing your motion zones in Config Tool might not accurately reflect the unit's behavior.

To configure motion detection, you must specify areas of the video image, motion sensitivity, and a schedule for when to apply motion detection settings. Every camera has a default motion detection configuration based on the **Always** schedule. The default motion detection configuration can be modified but not deleted.

When an H.264 stream is selected as the recording stream, the **Advanced settings** button becomes available. Clicking this button opens the *H.264 advanced motion detection settings* dialog box which you can use to refine the motion detection settings.

Motion block

A *motion block* is when motion is detected inside one of the blocks you configure on the video image. There is positive motion in a video image when the area covered by the block detects motion in two consecutive video frames. The number of motion blocks detected represents the amount of motion. A motion block is represented by a semi-transparent green square overlay on the video image.

Positive motion detection

Seeing motion blocks on the video does not necessarily mean that the system will generate a motion related event. It might be noise. To determine when motion started (*Motion on* event) and stopped (*Motion off* event), adjust the *Sensitivity*, *Consecutive frame hits*, *Motion on threshold*, and the *Motion off threshold* parameters to achieve the best results in the specific environment.

Best practices for configuring motion detection

The main purpose for using motion detection is to minimize storage requirements, search times, and retrieval times by reducing the amount of video recordings that must be saved. However, configuration of motion detection must be done carefully and on an individual camera basis. When configuring motion detection, consider the following:

- It is preferable to have sensitive settings that might trigger false motion events, than missing expected recordings when settings are not sensitive enough.
- All motion settings are stored in the Directory database, so make sure to back up your database when changes are made.
- Motion detection is the most basic video analytic capability. Due to possible false motion events, it should not be used to trigger alarms in critical situations, for example in replacement to a specialized intrusion detection system.
- If you set the **Time to record before an event** parameter to a high value, it increases the memory (RAM) resources required by the Archiver. This reduces the camera count allowed on the Archiver. Cameras with a higher resolution have the same effect on the memory resources.

When configuring software motion detection:

- It is always possible to use MJPEG streams.
- It is possible to use MPEG-4 streams.
- It is also possible to use H.264 streams, but because of the notion of *profiles*, some cameras must be configured through the additional *H.264 advanced motion detection settings* dialog box.

Configuring motion detection

To monitor motion in a camera image, you must configure motion detection for the video unit.

Before you begin

Make sure the unit supports motion detection.

What you should know

Motion detection can be performed by the Archiver or by the unit, on the entire video image (default) or only on certain areas (motion zones).

BEST PRACTICE: For H.264 and MPEG-4 streams, software motion detection is performed by analyzing P-frames. Ensure that your video stream is not made up of only key frames when configuring the **Key frame interval** and **Frame rate** settings of the camera.

When you define motion detection zones in Security Center, the image keeps the orientation sent from the camera, and therefore might be viewed upside down or at a 90 degree angle.

To learn more about configuring advanced motion detection, watch our GTAP Webinar. For pre-configuration instructions or any additional configuration steps required to enable motion detection in Security Center for specific video units, see the *Security Center Video Unit Configuration Guide*.

To configure motion detection:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the camera to configure, and click **Video analytics** > **Motion detection**.
3. Turn on **Motion detection**.
4. For **Detection is done on**, select whether motion detection is performed by the Archiver or the video unit.

   NOTE: Motion detection on the Archiver is always available. To perform motion detection on the video unit, it must support this feature.
5. For **Sensitivity**, select how much of a difference must be detected in a block between two consecutive frames before it is highlighted as a motion block.

   A plain image, such as viewing an empty wall, is more prone to generate noise than an image containing a lot of detail.

   TIP: First set a high value, and then slowly lower it until you are only receiving a few false motion reads in the image.

   You can also calibrate the sensitivity automatically.
6. For **Consecutive frame hits**, select how many frames in a row the *Motion on* **Threshold** must be reached to generate positive motion detection.
7. For *H.264* streams, configure the **Advanced settings**, if required.

   For more information, refer to Camera - Video analytics > Motion detection tab on page 1257.
8. Define the motion detection zones.
9. Set the motion detection criteria for each motion zone as follows:

   If these values are too low, motion will be detected too often. If these values are too close together, you might receive many consecutive events.
   - **Motion on:** If the number of detected motion blocks reaches the **Threshold** over the required number of **Consecutive frame hits**, the selected event is raised.
   - **Motion off:** If the number of detected motion blocks falls below the **Threshold** for at least five seconds, the selected event is raised.
10. Select the event types you want to generate when motion is detected for each motion zone.

Related Topics

Camera - Video analytics > Motion detection tab on page 1257
Motion detection is not working in Security Center on page 715

Automatically calibrating motion detection sensitivity

You can determine what constitutes positive motion detection by automatically calibrating the sensitivity value.

Before you begin

Make sure there is no motion in the camera’s field of view (0 motion blocks).

What you should know

If your camera is located outdoors, the accuracy of this test might be affected due to wind, moving trees, and so on.

To automatically set the motion detection sensitivity:

1. Open the *Video* task.
2. Select the camera to configure, and click **Video analytics** > **Motion detection**.
3. Select one of the following options from the **Auto calibrate** drop-down list:
   - **Current zone:** Calibrate the sensitivity for motion detected in the currently selected motion zone on the video image.
   - **All zones:** Calibrate the sensitivity for motion detected in all the motion zones on the video image.
   - **All motion:** Calibrate the sensitivity for motion detected on the whole video image.

   Different sensitivity values are tested to find the highest value without detecting motion in the image. This test accounts for any unwanted background noise that your camera may pick up and consider as motion.

Defining motion detection zones

To define the areas of the video image where motion is meaningful, you can draw motion detection zones, or *blocks* on the image.

To define a motion detection zone:

1. Open the *Video* task.
2. Select the camera to configure, and click **Video analytics** > **Motion detection**.
3. Under **Motion zone 1**, use the following tools to define the motion detection zone:

   TIP: For cameras positioned near a window or door, make sure that the motion detection zone covers that important area.

   - To cover the entire image with motion detection blocks, use the **Fill** () tool.
   - To draw a group of motion detection blocks, use the **Rectangle** () tool.
   - To draw single motion detection blocks, use the **Pen** () tool.
   - To invert the area with motion detection blocks and the area without any selected blocks, use the **Invert** () tool.
   - To erase all the motion detection blocks in the image, use the **Clear all** () tool.
   - To erase the motion detection blocks that are not needed, use the **Eraser** () tool.

4. To remove the blocks where motion typically occurs so they do not generate false motion reads, click **Learning mode** (💡).

   You should only use this option if the video image is displaying what it normally does. If there is usually a lot of motion in the image, but you use the *Learning mode* in the middle of the night, it is not helpful.

   The affected areas where motion typically occurs are turned off.
5. If necessary, add additional motion detection zones to the image.
6. Click **Apply**.

Selecting which events are triggered on motion

When motion is detected on a motion zone, you can select which event is triggered when the motion period starts, and which one is triggered when it stops.

What you should know

The default events that are triggered when motion detection is generated are the following:

- **Motion on:** Default event triggered at the beginning of the motion period.
- **Motion off:** Default event triggered at the end of the motion period.

Using custom events is useful when you have multiple motion zones. Each zone can be configured to detect motion in a different area of the camera’s field of view and generate different events. Having different events allows you to program different actions to respond to different situations.

To select which events are triggered on motion:

1. Open the *Video* task.
2. Select the camera to configure, and cclick **Video analytics** > **Motion detection**.
3. Under **Motion zone 1**, click **Events**.
4. In the *Motion events* dialog box, select which events will be triggered for the **Motion on event** and the **Motion off event**.
5. Click **OK**, and then click **Apply**.
6. If you have more than one motion zone configured, repeat the steps for each zone.

Testing motion detection settings

After modifying the motion detection settings for a camera, test your new settings to make sure that you get the expected results.

What you should know

There are limitations with hardware motion detection. If motion detection is performed on the unit, then the test might not be completely accurate.

CAUTION: Light reflections on windows, switching lights on or off, and light level changes caused by cloud movement can cause undesired motion detection responses, and generate false alarms. Therefore, you should perform a number of tests for different day and night conditions. For surveillance of indoor areas, ensure that there is consistent lighting of the areas during the day and at night. Uniform surfaces without contrast can trigger false alarms even with uniform lighting.

To test your motion detection settings:

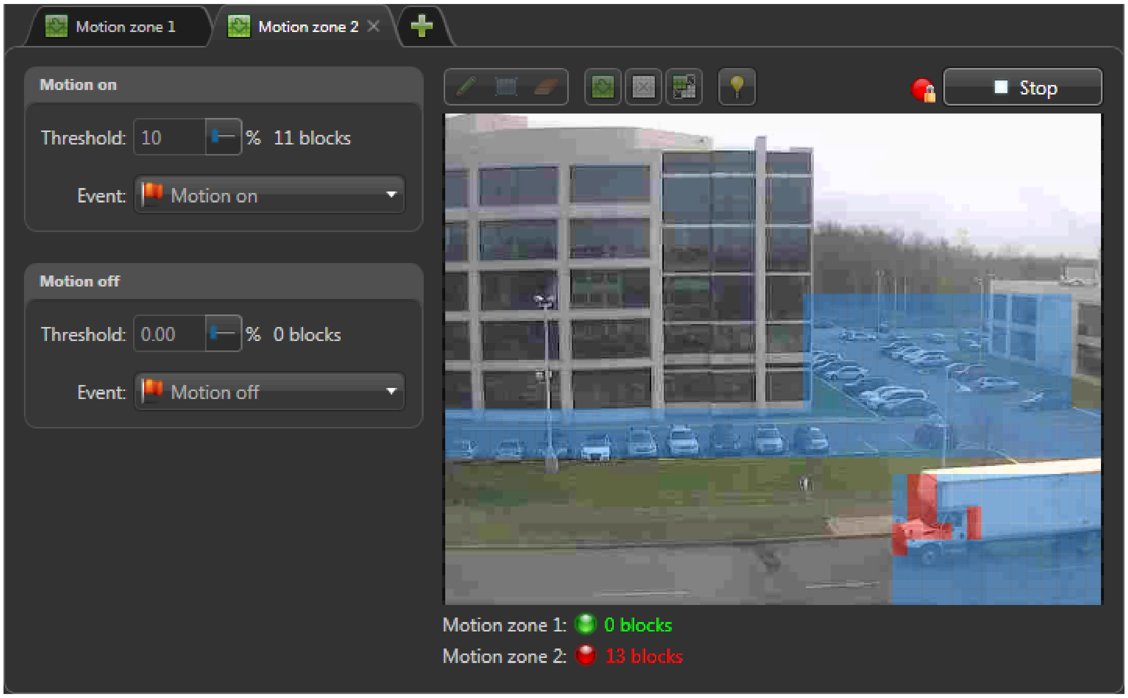
1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Select the camera to configure, and click **Video analytics** > **Motion detection**.

3 Under **Motion zone**, select one of the following test modes from the **Test zone** list:

- **Test zone:** The motion zone is displayed as blue overlays. The *motion blocks* are displayed as green overlays. The number of motion blocks is updated in real time. When the number of motion blocks reaches the *Motion threshold*, they are displayed as red.

  NOTE: If the camera is configured to record on motion, the recording state (●) will turn red when the **Motion threshold** is reached.
- **Test all zones:** In this mode, all *motion zones* are displayed at the same time, with the number of motion blocks in each displayed separately.



Motion on

Threshold: 10 % 11 blocks

Event: Motion on

Motion off

Threshold: 0.00 % 0 blocks

Event: Motion off

Motion zone 1: ● 0 blocks

Motion zone 2: ● 13 blocks

- **View all motion:** In this mode, the entire video image is tested for motion. All motion in the image is displayed as motion blocks (green overlays). The total number of motion blocks is updated in real time. Use this mode to test the sensitivity setting for this camera.

Related Topics

About motion detection on page 624

Adjusting camera color settings

You can adjust the video attributes such as brightness, contrast, hue and saturation for a camera based on schedules, to account for different times of the day.

Before you begin

Schedules must be created before you set the video attributes for that schedule.

What you should know

These settings are helpful for twilight schedules since the ambient lighting is different at dawn and dusk.

To adjust the color settings of a camera:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Select a camera, and then click the **Color** tab.

3 Adjust the **Brightness**, **Contrast**, **Hue**, and **Saturation** for the video image.

4 To add a new color configuration, click **Add schedule**.

5 Select a previously created schedule, and click **Add**.

6 Adjust the **Brightness**, **Contrast**, **Hue**, and **Saturation** for the video image during that schedule.

7 To reset all parameters to their default values, click **Load default**.

8 Click **Apply**.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

Related Topics

About twilight schedules on page 202

About visual tracking

With visual tracking you can follow an individual in live or playback mode from camera to camera through your facility.

Benefits

Visual tracking saves you time and simplifies monitoring and investigation tasks. You can follow someone quickly without losing time looking for the right camera to switch to. You do not have to remember all the camera names in your system because the cameras are linked together.

Some other advantages of linking cameras are:

- Training new operators quickly.
- Reducing operator stress during high-alert situations.

Common use cases

Some common use cases for visual tracking are:

- **Following suspects:** Following a suspect in real time or in playback mode after an incident has occurred.
- **Guard tours:** Conducting manual guard tours at your own pace.
- **Exit routes:** Monitoring individuals as they exit a building.
- **Visitor escorts:** Tracking visitors and their escorts through your facility.
- **Business processes:** Monitoring individuals during a money collection and distribution route in a casino.
- **Loading docks:** Following goods as they are received and unloaded.

How it works

When you turn on visual tracking using the feet icon (👣) in Security Desk, colored shapes are displayed on the video image, according to how they are configured. Each shape corresponds to another camera field of view that you can switch to by clicking it. If more than one camera is associated with a shape, a list of camera names is shown when you click the shape.

When you hover your mouse pointer over a shape, you can see a preview of the next camera image.

TIP: You can press `Ctrl+Shift+F` to turn on visual tracking for all cameras that are displayed in the canvas.

Example

Watch this video to learn more.

▶

Configuring visual tracking

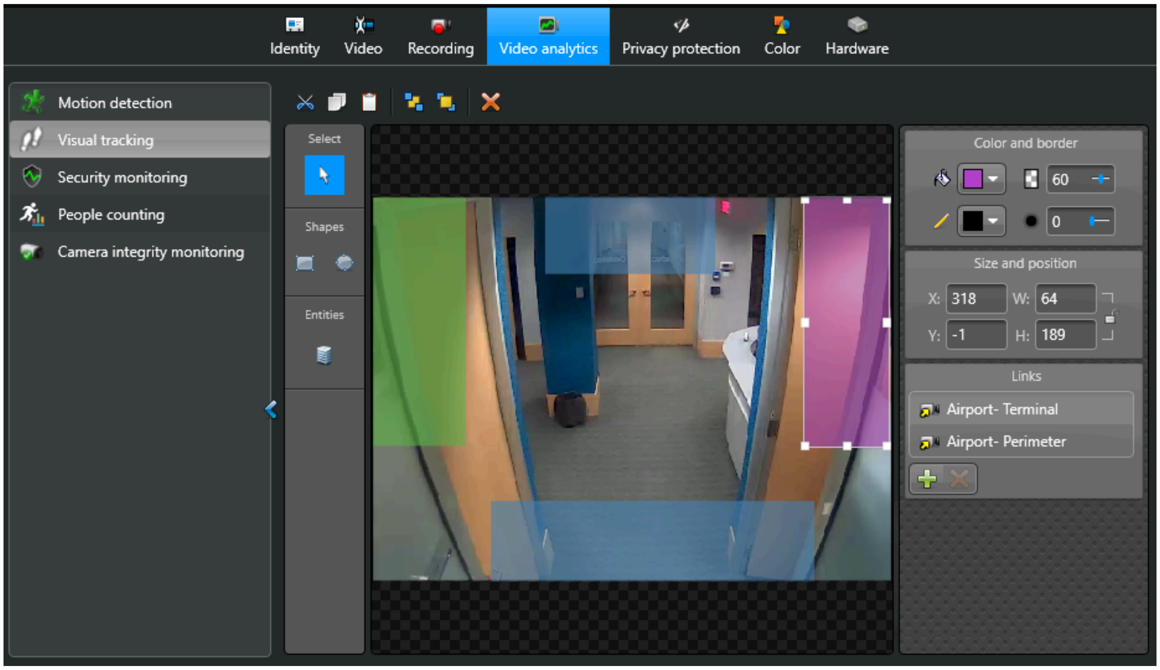
Before you to can follow an individual through a facility, you must create links between your cameras so you can easily switch to those video streams.

To configure visual tracking:

1. Open the *Video* or *Area view* task.
2. Select a camera and click **Video analytics** > **Visual tracking**.
3. Create shapes on the video image:
   a) Select the **Rectangle** (▭) or **Ellipse** (○) drawing tool and draw a shape.
   b) Resize, reposition, and rotate the shape using your mouse or using the **Size and position** fields.
   c) Set a color, opacity, border color, and border thickness for the shape.

   We suggest color-coding your shapes for different objects on your system, such as exit cameras in red, PTZ cameras in green, and so on.

   TIP: If you like the dimensions of your shape, you can copy and paste the shape to use it again. You can also copy the shape and use it for another camera.



4. Link cameras to each shape:
   a) Select a shape and click **Entities** (▤) in the toolbar.
   b) Drag a camera from the area view onto the shape.

      The camera name is listed in the *Links* section. If you link multiple cameras to a shape, Security Desk users must select which camera to jump to.
5. Click **Apply**.

Example

Watch this video to learn more.

▶

Viewing camera settings

You can view a list of all the local and federated Security Center cameras and their settings that are part of your system, using the *Camera configuration* report.

What you should know

The *Camera configuration* report is helpful for comparing camera settings, and making sure that your cameras are configured properly according to your requirements. If the camera has multiple video streams or multiple streaming schedules set, each stream and schedule is displayed as a separate result item.

NOTE: This report is not supported with Omnicast™ federated cameras.

To view the settings of cameras in your system:

1 Open the *Camera configuration* task.

2 Set up the query filters for the report. Choose one or more of the following filters:

- **Cameras:** Select the camera to investigate.
- **Custom fields:** Restrict the search to a predefined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.

3. Click **Generate report**.

   The following camera settings are listed in the report pane:

   - **Camera:** Camera name.
   - **Owner:** Archiver that manages the camera.
   - **Resolution:** Resolution of the camera’s video stream.
   - **Image quality:** Image quality setting for the camera.
   - **Frame rate:** Frame rate setting for the camera.
   - **Stream usage:** Purpose of the video stream, such as for live video, recordings, and so on.
   - **Network setting:** Connection type used by the camera.
   - **Bit rate:** Bit rate setting for the camera.
   - **Stream:** The video stream of the camera.
   - **Key frame interval:** Key frame interval setting for the camera.
   - **Primary recording mode:** Recording mode for the camera when the Archiver is recording on the primary server.
   - **Primary retention period:** Retention period of the camera when the Archiver is recording on the primary server.
   - **Type:** Type of camera, such as fixed camera or PTZ camera.
   - **Streaming schedule:** Schedule when the camera streams video.
   - **Manufacturer:** Manufacturer of the unit.
   - **Product type:** Model or series of the video unit.
   - **Area path:** List of all parent areas, starting from the system entity. If the camera has multiple parent areas, “*\” is shown as the path.
   - **Description:** Entity description.
   - **Edge transfer:** Whether the camera is configured for edge transfer or not.
   - **Firmware version:** Firmware version of the camera.
   - **IP address:** IP address of the camera.
   - **Logical ID:** Logical ID of the camera.
   - **Multicast address:** Multicast address of the camera.
   - **Multicast port:** Connection port of the video unit.
   - **Secondary recording mode:** Recording mode for the camera when the Archiver is recording on the secondary server.
   - **Secondary retention period:** Retention period of the camera when the Archiver is recording on the secondary server.
   - **Tertiary recording mode:** Recording mode for the camera when the Archiver is recording on the tertiary server.
   - **Tertiary retention period:** Retention period of the camera when the Archiver is recording on the tertiary server.

4. To modify the settings of a camera, right-click an item in the report pane, and then click **Configure** ().

   The configuration page for the entity opens in Config Tool.

   NOTE: You need the user privilege to modify entities to use this command.

Configuring PTZ motors

If the PTZ motor is not integrated with your camera on the video unit, you need to configure the PTZ motor separately before you can control it in Security Desk.

What you should know

Some PTZ motors support the following additional commands:

- **Zoom-box:** Zoom in on an area by drawing a box on the video image using your mouse. This works like the digital zoom for fixed cameras.
- **Center-on-click:** Center the camera on a point of the video image with a single click.
- **Enhanced zoom:** Zoom in or out to a specific zoom factor (absolute value) using the slider available in the tile. For example, you can move the slider to 10x and it will keep its position when released. When **Enhanced PTZ** is disabled, the zoom factor is not available and the slider returns to its center position when released, similar to a joystick used to pan and tilt a camera.

When these commands are enabled, they replace the normal pan, tilt, and zoom commands when controlling the PTZ in Security Desk.

To configure PTZ motors:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select the camera to configure, and click the **Hardware** tab.
3. Turn on the **PTZ** option.
4. From the **Protocol** drop-down list, select the protocol used by the PTZ motor.
5. Beside the **Protocol** field, click ✎ to set the **Idle delay**, **Idle command**, and **Lock delay** options.
6. From the **Serial port** list, select the serial port used to control the PTZ motor.
7. In the **PTZ address** box, select the number that identifies the PTZ motor on the serial port.

   This number is important because it is possible to connect more than one PTZ motor on the same serial port. This number must correspond to the dip switch settings on the PTZ hardware.
8. To enable the enhanced PTZ commands (zoom-box, center-on-click and enhanced zoom), turn on the **Enhanced PTZ** option and calibrate the PTZ coordinates.
9. Click **Apply.**

After you finish

- Test the PTZ motor.
- Define which users have priority to control the PTZ motor.

Related Topics

Camera - Hardware tab on page 1261

Calibrating PTZ coordinates

For most cameras, you need to calibrate the limits of the PTZ movement to use the zoom-box, center-on-click, and enhanced zoom commands properly in Security Desk.

What you should know

Not all cameras require PTZ calibration. For example, Axis cameras do not require calibration.

To calibrate the PTZ coordinates:

1. Open the *Video* task.
2. Select the camera, and click the **Hardware** tab.
3. Next to the **Enhanced PTZ** option, click **Calibrate**.
4. To set the PTZ coordinates automatically, click **Calibration assistant**, and follow the on-screen instructions.
5. To set the PTZ coordinates manually, move the PTZ motor around in the live video image, and enter the corresponding values on the right:
   - **Max zoom factor:** Zoom in to the maximum level you want Security Desk users to reach, and enter the **Zoom** value from the **Coordinates** section.
   - **Horizontal field of view:** Enter the horizontal field of view specified by the camera manufacturer. If you do not have this information, zoom out until the **Zoom** value indicates 1x, and estimate the angle of the horizontal field of view from the image you see on screen.
   - **Vertical field of view:** Enter the vertical field of view specified by the camera manufacturer. If you do not have this information, zoom out until the **Zoom** value indicates 1x, and estimate the angle of the vertical field of view from the image you see on screen.
   - **Minimum pan angle:** Turn the camera to the left-most position of the area under surveillance, and enter the **Pan** value from the **Coordinates** section.
   - **Maximum pan angle:** Turn the camera to the right-most position of the area under surveillance, and enter the **Pan** value read from the **Coordinates** section.
   - **Minimum tilt angle:** Turn the camera to the bottommost position of the area under surveillance, and enter the **Tilt** value read from the **Coordinates** section.
   - **Maximum tilt angle:** Turn the camera to the topmost position of the area under surveillance, and enter the **Tilt** value read from the **Coordinates** section.
6. If you want to flip the camera image at any point, select one of the following from the **Flip camera** list:
   - **Minimum tilt:** Flips the camera image when the PTZ motor reaches the minimum tilt coordinate.
   - **Maximum tilt:** Flips the camera image when the PTZ motor reaches the maximum tilt coordinate.
7. If you see that the **Minimum pan angle** value is higher than the **Maximum pan angle** value, select the **Invert pan axis** option.
8. If you see that the **Minimum tilt angle** value is higher than the **Maximum tilt angle** value, select the **Invert tilt axis** option.

After you finish

Test the zoom-box, center-on-click, and enhanced zoom commands from a Security Desk tile. If needed, adjust the calibration, and test the PTZ camera again.

Testing PTZ controls

After you set up your PTZ motor, you should test if the controls are working properly.

What you should know

Every time you change a PTZ parameter, you must remove the camera from the tile and drag it back to the tile for your changes to take effect.

To test PTZ controls:

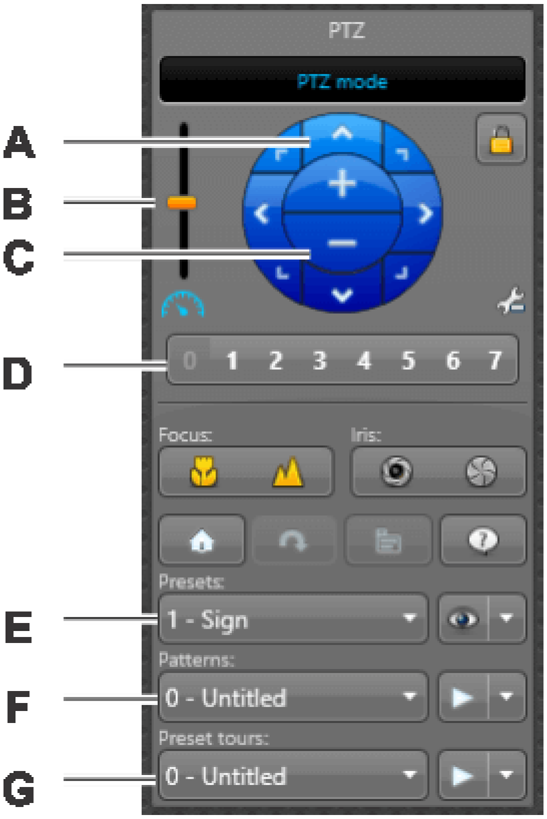
1 Open the *Video* task and double-click the camera you want to test.

2 In the *Live video* dialog box, test the PTZ controls in the video image using the PTZ widget.

PTZ widget

The *PTZ* widget controls the pan, tilt, and zoom operations on the displayed camera. It appears in the *Controls* pane when the selected tile displays a PTZ-enabled camera.

IMPORTANT: If one or more of the PTZ buttons are grayed out, the PTZ camera ( ) you are working with does not support that command.



Button/Letter	Command	Description
A	**Direction arrows**	Pan the PTZ motor using the eight direction arrows.
B	**Speed slider**	Adjust the speed of the PTZ motor.
C	**Zoom in/out**	Zoom in and out using the plus (+) and minus (-) commands.

Button/Letter	Command	Description
D	**Quick access buttons**	Move the PTZ motor to one of the eight quick access PTZ presets.
E	**Presets**	Select a preset from the drop-down list to move the PTZ motor to that preset, save a new preset position, or rename the preset.
F	**Patterns**	Select a PTZ pattern from the drop-down list to do one of the following: • Start a PTZ pattern (series of presets or recorded PTZ movements. • Record a new pattern. • Rename the pattern.
G	**Preset tours**	Select an auxiliary from the drop-down list to start or stop an auxiliary command, or rename the command.
🔒	**Lock PTZ**	Lock the PTZ motor so only you have control of the PTZ.
⚙	**Toggle to advanced mode**	Open the PTZ Advanced mode menu.
🌷	**Focus near**	Focus the PTZ near.
⛰	**Focus far**	Focus the PTZ far.
◉	**Open iris**	Manually control the iris (open iris).
◎	**Close iris**	Manually control the iris (close iris).
⌂	**PTZ home**	Go to the PTZ home (default) position.
↻	**Flip**	Flip the PTZ motor 180 degrees.
☰	**Menu on/off**	Open the PTZ menu. This option is only for analog PTZ cameras.
?	**Specific commands**	Use commands that are specific to that camera model.
👁	**Go to preset**	Jump to the preset position selected in the drop-down list. • **Save:** Save the preset selected in the drop-down list, using the current PTZ position. • **Clear preset:** Clear the PTZ position from the preset.
▶	**Start pattern**	Start the PTZ pattern selected in the drop-down list. You can click any preset of PTZ button to stop the pattern. • **Rename:** Rename the selected preset, pattern, or auxiliary. • **Record pattern:** Record a new PTZ pattern. • **Clear pattern:** Clear the pattern.
▮	**Start auxiliary command**	Start a PTZ auxiliary command (for example, a wiper blade).

Button/Letter	Command	Description
⏹	**Stop auxiliary command**	Stop the PTZ auxiliary command.
ABC	**Rename**	Rename the selected preset, pattern, or auxiliary.

Overriding user levels for specific areas and cameras

To set a seperate user level for specific areas or cameras, you can create overrides for a user, or user group.

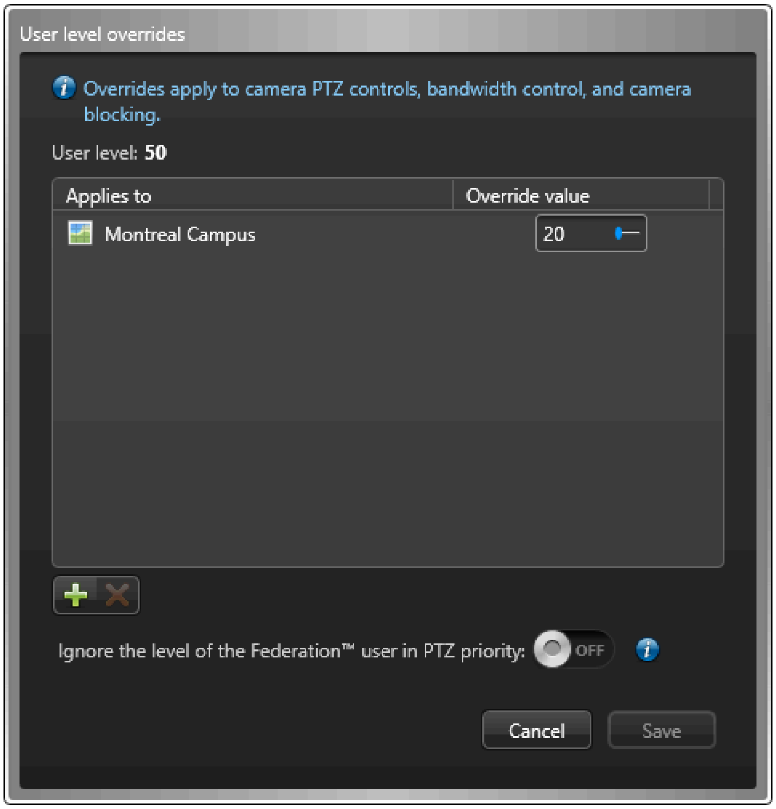
What you should know

By default, the general *user level* applies to PTZ control, bandwidth control, and *camera blocking*. This level is set individually or inherited from the parent user group. If the general user level does not apply to specific areas or cameras, you can create user-level overrides. These overrides take precedence over the general user level for the cameras you specify. If you override a user level for an area, it applies to all cameras in that area.

To define a user-level override:

1. From the Config Tool home page, open the *User management* task.
2. Select the user or user group to configure, and click the **Properties** tab.
3. Set the **User level** option to **Override**, and then click **Configure user-level overrides**.
4. In the *User level overrides* dialog box, click **Add an item** (+).
5. Select the area or camera to override, and click **OK**.
6. In the **Override value** column, select a user level that applies to the area or camera.

   Example: Paul is a member of the Operators user group in his company, and he is in charge of monitoring the Montreal Campus. As part of the Operators user group, he has a default user level of 50. Because he is in charge of monitoring the Montreal Campus, he needs a higher priority to control the PTZ cameras in that area. Therefore, a user level override with the value of 20 is created for him for the Montreal Campus.



User level overrides

Overrides apply to camera PTZ controls, bandwidth control, and camera blocking.

User level: 50

Applies to	Override value
Montreal Campus	20

Ignore the level of the Federation™ user in PTZ priority: OFF

7. (Optional) For *Federation™ users* only. Enable **Ignore the level of the Federation™ user in PTZ priority** to prioritize control of federated PTZ cameras only by the user level of the remote user who issued the PTZ commands. The user level of this user is ignored.

8 Click **Save** > **Apply**.

Related Topics

About users on page 431

About camera sequences

A camera sequence is an entity that defines a list of cameras that are displayed one after another in a rotating fashion within a single tile in Security Desk.

When displayed in a Security Desk, the camera sequence can be paused (stop cycling) and unpacked (showing all cameras).

The cameras composing the sequence can be fixed, PTZ enabled, or federated. Each camera is given a preset amount of display time. PTZ cameras can be configured to point to a preset position, to run a pattern, or to turn on/off an auxiliary switch.

Creating camera sequences

You can group fixed, PTZ-enabled, and federated cameras into a camera sequence, so they are displayed one after another in Security Desk tiles.

What you should know

The cameras in the camera sequence list are displayed in the same order in Security Desk.

To create a camera sequence:

1. Open the **Area view** task.
2. Click **Add an entity** (➕) > **Camera sequence**.

   A new camera sequence entity (📹) appears in the area view.
3. Type a name for the camera sequence, and press Enter.
4. Click the **Cameras** tab, and click **Add an item** (➕).
5. From the **Camera** list, select a camera to be part of the sequence.
6. In the **Dwell time** box, set the amount of time the camera is displayed when cycling through the sequence.
7. From the **PTZ command** list, choose what action the PTZ camera will perform when it is displayed in the sequence.

   This option is only for PTZ-enabled cameras.

   - **Preset:** Move the PTZ camera to a preset position.
   - **Position:** Start a PTZ pattern.
8. From the **PTZ auxiliary** list, configure the switch number and the state to set it to.

   This option is only for PTZ-enabled cameras that support auxiliary switches.
9. Click **Save** > **Apply**.
10. If necessary, add additional cameras to the sequence.
11. To change the order of the cameras in the sequence, use the ▲ and ▼ buttons.
12. To remove a camera from the sequence, select the camera, and click **Remove the item** (✖).
13. Click **Apply**.

Related Topics

About camera sequences on page 643

About analog monitors

An analog monitor entity represents a monitor that displays video from an analog source, such as a video decoder or an analog camera. This term is used in Security Center to refer to monitors that are not controlled by a computer.

A video decoder is a device that converts a digital video stream into analog signals (NTSC or PAL) for display on an analog monitor. It is one of the many devices found on a video decoding unit. A video decoding unit can have multiple video decoders, each connected to an analog monitor. Each video decoder found on a video decoding unit is represented by an analog monitor entity in Security Center.

The *monitor group* entity is used to configure the properties of a group of analog monitors.

Configuring analog monitors

To achieve optimal performance with your analog monitor, configure its settings.

What you should know

Analog monitor entities are automatically created when the video decoding units they are connected to are added to your system. Although Security Center provides workable default settings when analog monitor entities are added, we recommend that you configure each analog monitor.

To configure analog monitors:

1. Add a video decoding unit to your system.
2. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
3. Select an analog monitor to configure, and then click the **Properties** tab.
4. Configure the video settings, network settings, and the hardware connected to the analog monitor.
5. Click **Apply**.
6. Configure each analog monitor connected to the decoder.

Related Topics

Analog monitor - Properties tab on page 1246

Adding analog monitors as alarm recipients

To receive alarms on your physical analog monitors, you must create a monitor group, and then add that group as recipient of the alarm.

What you should know

When you receive alarms on an analog monitor, high priority alarms do not replace lower priority alarms that are displayed on the monitor. For more information about viewing video or receiving alarms in analog monitors in Security Desk, see the *Security Center User Guide*.

IMPORTANT: If you add more than one analog monitor to a monitor group, the first analog monitor in the list will receive the highest priority alarm, the second analog monitor will receive the second highest priority alarm, and so on. The last analog monitor in the monitor group list will receive all the other alarms.

To add analog monitors as alarm recipients:

1. Open the *Alarms* task, and click the **Monitor groups** view.
2. Click **Monitor group** (+), and type a name for your monitor group.
3. Select the monitor group, and click the **Monitors** tab.
4. At the bottom of the page, click +, select the analog monitors to be part of the monitor group, and then click **OK**.

   You can select multiple analog monitors by holding the Shift or Ctrl keys.
5. Click **Apply**.
6. In the *Alarms* task, click the **Alarms** view, select an alarm, and then click the **Properties** tab.
7. In the **Recipients** section, click +, select the monitor groups to be recipients of the alarm, and then click **OK**.

8 Click **Apply**.

When the alarm is triggered, the video associated with the alarm is shown on the physical analog monitor.

Testing analog monitor settings

After configuring your analog monitors, you should always test to make sure you can view video on the analog monitors.

Before you begin

Make sure the cameras you want to test viewing video with are supported (same manufacturer as the decoder, and use the same video format).

What you should know

For more information about viewing video in an analog monitor in Security Desk, see the *Security Center User Guide*.

To test analog monitor settings:

1 Open Security Desk.

2 In the Monitoring task, display an analog monitor in a canvas tile, and then add a supported camera to the tile.

About body-worn cameras

A body-worn camera (BWC), also known as a wearable camera, is a video recording system that is typically used by law enforcement to record their interactions with the public or gather video evidence at crime scenes.

Wearable Camera Manager role

The Wearable Camera Manager role is used to configure and manage body-worn camera (BWC) devices in Security Center, including configuring camera stations, adding officers (wearable camera users), uploading content to an Archiver, and setting the retention period for uploaded evidence.

You can use this role when you do not or cannot upload your evidence data to the cloud (Genetec Clearance™), or when you want to access Security Center Archiver functions such as retention period.

You can then search body-worn camera archives using the *Archives* task in Security Desk.

The storage requirements for body-worn cameras takes into account the following factors:

- Number of cameras.
- Retention period: amount of time to keep the archives online.
- Average recording size.

NOTE: The data is duplicated for body-worn cameras. For example, the original recording mp4 (in the G64) is kept as well as the archive G64 (audio and video).

When using the Wearable Camera Manager role, the Genetec™ Server should use an NTP server. The servers for all Associated Archiver roles should also be synched with this NTP server and the docking station's NTP time server must be configured.

Body-worn camera station

A body-worn camera station is a physical device or software used to automatically upload media from a body-worn camera to Genetec Clearance™ or the Wearable Camera Manager role in Security Center, depending on which *.json* file is used.

Related Topics

Configuring body-worn cameras on page 649
Backing up the Wearable Camera Manager server configuration on page 654
Adding cameras and officers to the Wearable Camera Manager role on page 651

Configuring body-worn cameras

To upload evidence from a body-worn camera (BWC) to a Security Center archive, you must configure the Wearable Camera Manager role.

Before you begin

- Ensure that you have a valid *body-worn camera* license (Part Number: GSC-Om-X-1BWC).
- Ensure that you configured the firewall ports before creating the Wearable Camera Manager role.

  NOTE: Firewall ports must also be updated after a major upgrade.

What you should know

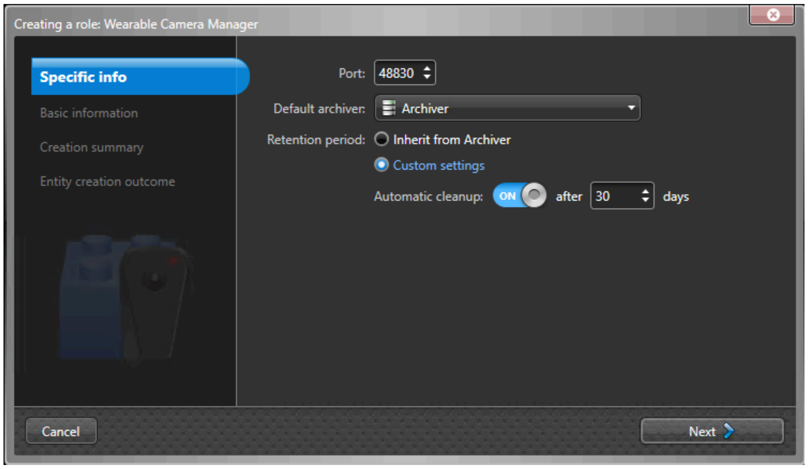
- Redundant archiving or failover is not supported when using body-worn cameras.
- For a list of *body-worn camera* devices that are supported by Security Center, see our Supported Device List.
- The *.json* config file is used to connect the role and to secure the communication with the body-worn camera docking station.

To configure body-worn cameras:

1 Create a Wearable Camera Manager role:

a) Open the *System* task and click **Roles** > **Add an entity** > **Wearable Camera Manager**.

b) (Optional) In the *Specific info* section, click **Custom settings**, select a retention period, and click **Next**.



Port: 48830

Default archiver: Archiver

Retention period: ○ Inherit from Archiver ● Custom settings

Automatic cleanup: ON after 30 days

Selecting a retention period automatically ensures that older videos are deleted after the specified period.

IMPORTANT: Imported files must not be older than the current retention period.

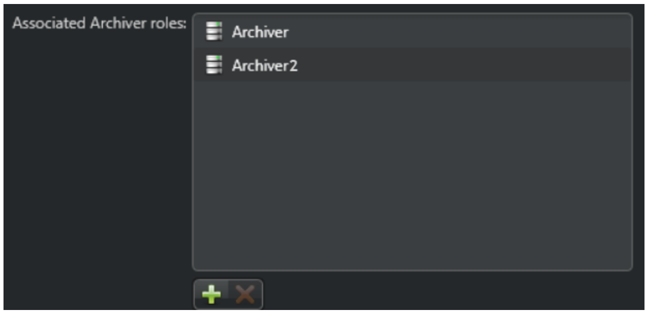
c) In the *Basic info* section, enter an entity name and click **Next**.

d) In the *Creation summary* section, click **Create**.

2 (Optional) Add additional Archivers to share the load on systems with a large number of body-worn cameras:

a) In the *Associated Archiver roles* section of the *Properties* page, click ✚.

b) Select the additional Archivers you want to use.



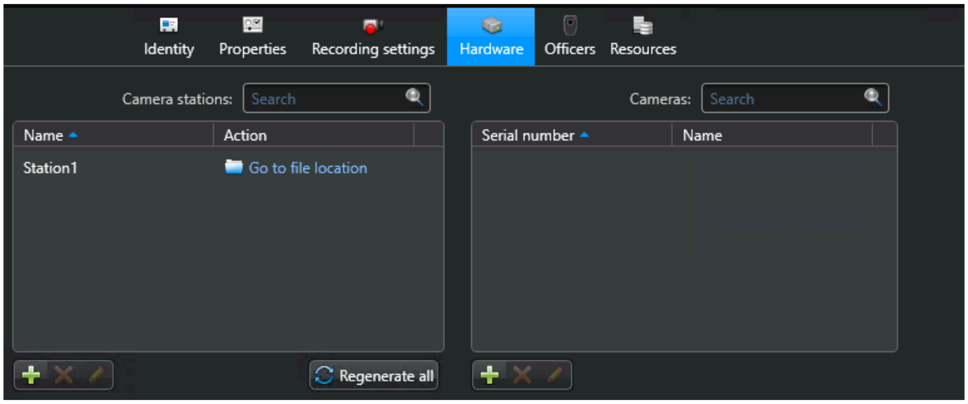
c) Click **Apply**.

IMPORTANT: If your body-worn camera station is already configured, you must re-upload the *.json* file to the station.

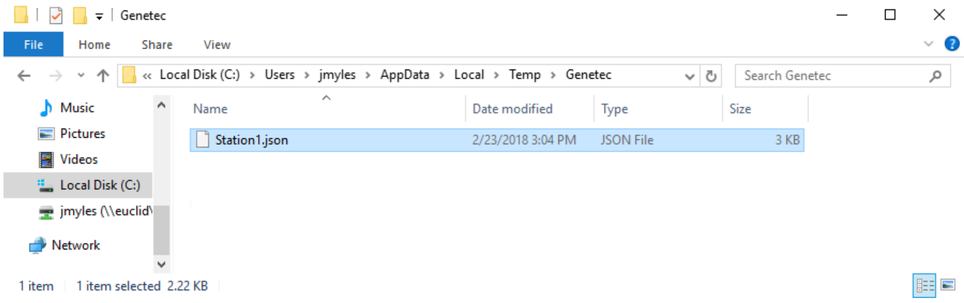
3 Configure the Camera station:

a) In the *Camera stations* section of the *Hardware* page, click ✚.

b) Enter a station name and click **Apply**.



c) In the *Camera stations* section, click **Go to file location** and copy or transfer the *.json* file to the camera station. For more information, refer to your body-worn camera docking station's documentation.



d) (Optional) To delete a camera station, select it from the list and click ✖.

4 (Optional) Add a camera or an *officer*.

After you finish

You can now dock your body-worn camera to connect and sync.

- The upload begins when a camera is connected to the body-worn camera station. Your evidence is uploaded automatically, no further intervention is required.
- After the upload completes, you can find and view the uploaded evidence in Security Desk by using the Archives report in the *Archives* task.

  NOTE: Depending on the size and number of evidence files that you upload, the videos might not appear in the Security Desk archives report immediately. Configure an event-to-action for *Evidence ready* to be notified when an officer's recording is ready for viewing.

Related Topics

About body-worn cameras on page 648

Archives report for body-worn camera is empty on page 699

Adding cameras and officers to the Wearable Camera Manager role

You can create a new officer, assign a new camera to an existing officer, or modify officer-camera relationships from the Wearable Camera Manager role. When there is video to upload from body-worn cameras that have no assigned officer, officers are added automatically.

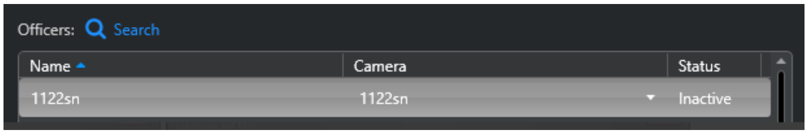
Before you begin

Ensure that you have a valid *body-worn camera* license for part number GSC-Om-X-1BWC.

What you should know

- Redundant archiving or failover is not supported when using body-worn cameras.
- For a list of *body-worn camera* devices that are supported by Security Center, see our Supported Device List.
- When using the Axis body-worn camera solution, you must create officers and associate cameras on the Axis W800 SCU web page. The Axis body-worn camera solution automatically updates the Wearable Camera Manager role with the latest information.

  CAUTION: Removing Axis body-worn cameras or officers from Config Tool can cause data loss. Always use Axis Body Worn Manager to remove officers and cameras.
- The upload process begins automatically when a camera is connected to the body-worn camera docking station.
- If the body-worn camera has not been configured, the camera is created automatically with the serial number of the camera device. In this situation, the *officer* (wearable camera user) is created at the same time.
- If the officer is automatically created, the officer's name is the same as the camera serial number.



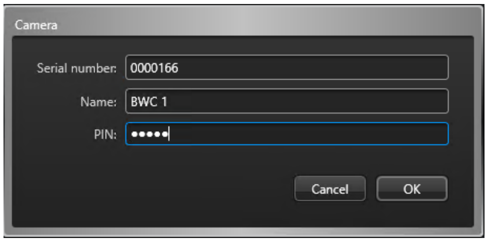
Name	Camera	Status
1122sn	1122sn	Inactive

NOTE: You can modify the **Camera** device and assigned officer. Choose names that can help you track and find your imported video.

To add cameras manually:

1 In the *Cameras* section of the *Hardware* page, click ➕.

2 In the *Camera* dialog box, enter the serial number and name and click **OK**.



Serial number: 0000166

Name: BWC 1

PIN: •••••

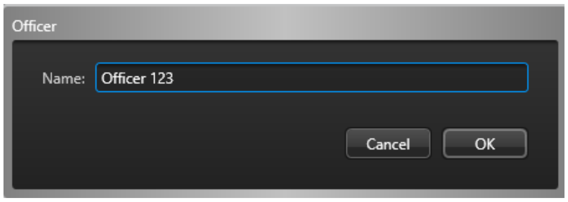
IMPORTANT: Enter the correct serial number to match the upload request device to the serial number in the Wearable Camera Manager role's **Hardware** tab.

3 Click **Apply**.

To add officers manually:

1 In the *Cameras* section of the *Officers* page, click ➕.

2 In the *Officer* dialog box, enter a name and click **OK**.



Name: Officer 123

3 Click **Apply**.

After you finish

- To modify a previously saved officer, select the **Officer**, click ➜ to jump to the configuration page, and make the required changes.
- To delete an officer, select the **Officer**, click ➜ to jump to the configuration page, and click ✖.

Related Topics

About body-worn cameras on page 648

Deactivating officers

To reassign a body-worn camera license while retaining the officer's video archive, you can deactivate officers in the Wearable Camera Manager role.

Before you begin

- Ensure that you have a valid *body-worn camera* license (Part Number: GSC-Om-X-1BWC).
- Ensure that the BWC is online before deactivating officers.

What you should know

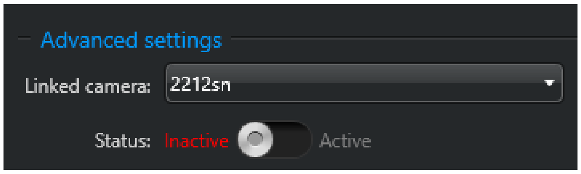
- Redundant archiving or failover is not supported when using body-worn cameras.
- For a list of *body-worn camera* devices that are supported by Security Center, see our Supported Device List.

To deactivate an officer:

1 In the *Officers* section, select the officer you want to deactivate.

2 Click ⧉ to jump to the selected entity's configuration page.

3 In the *Advanced settings* section of the *Properties* page, click the **Status** toggle.



Advanced settings

Linked camera: 2212sn

Status: Inactive ○ Active

4 Click **Apply**.

Backing up the Wearable Camera Manager server configuration

The Wearable Camera Manager role requires a direct link to your body-worn camera stations. To reestablish this link if your server fails, you can back up the original configuration so it can be restored on different server.

Before you begin

Create and configure the Wearable Camera Manager role.

What you should know

This procedure makes the following assumptions about your Security Center servers:

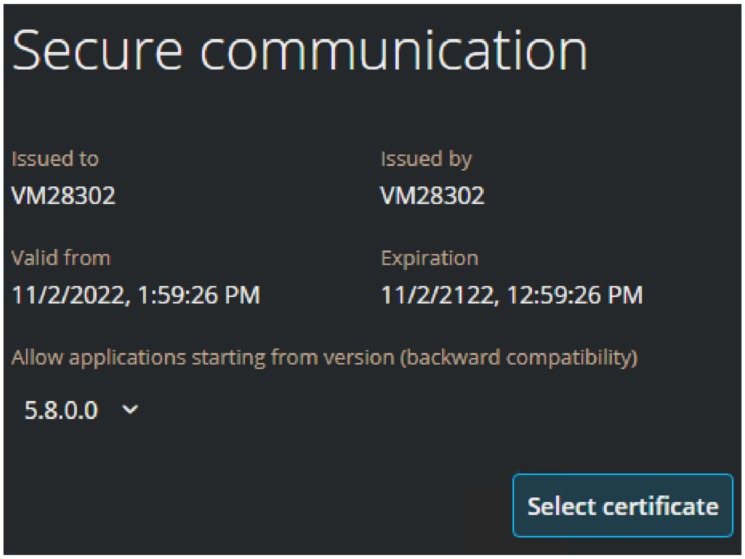
- The Wearable Camera Manager role is hosted on a dedicated expansion server with no other roles.
- The servers use static IP addresses, not the Dynamic Host Configuration Protocol (DHCP).
- The replacement expansion server must have the same certificate, serverIdentification ID, and IP address to reestablish a link to the body-worn camera station.

To back up the Wearable Camera Manager server configuration:

1 Back up the Security Center server certificate:

a) Open Server Admin on the expansion server hosting the Wearable Camera Manager role and click **Stay on this expansion server**.

b) Click the server and note the **Secure communication** information.



Secure communication

Issued to
VM28302

Issued by
VM28302

Valid from
11/2/2022, 1:59:26 PM

Expiration
11/2/2122, 12:59:26 PM

Allow applications starting from version (backward compatibility)
5.8.0.0

c) From the Windows Start menu, enter `Manage computer certificates` to open Certificate Manager on the local machine.

d) In **Personal** > **Certificates**, locate the certificate used by Security Center.

e) Right-click the certificate and select **All Tasks** > **Export**.

f) In the *Certificate Export Wizard*, click **Yes, export the private key**.

g) Choose the .PFX file format and click **Next**.

h) Select **Password** and enter a password.

Take note of the password. It is required for the recovery process.

i) Name the file and save it in a secure location.

2 Back up the Server ID:

a) Navigate to the Security Center installation folder *C:\Program Files (x86)\Genetec Security Center 5.x \ConfigurationFiles* on the server that runs the Wearable Camera Manager role.

b) Open *GenetecServer.gconfig* and note the serverIdentification id.

c) Retain the serverIdentification id in a secure location.

3 Back up the server IP address:

a) On the server running the Wearable Camera Manager role, start a Windows Command Prompt.

b) Enter `ipconfig`.

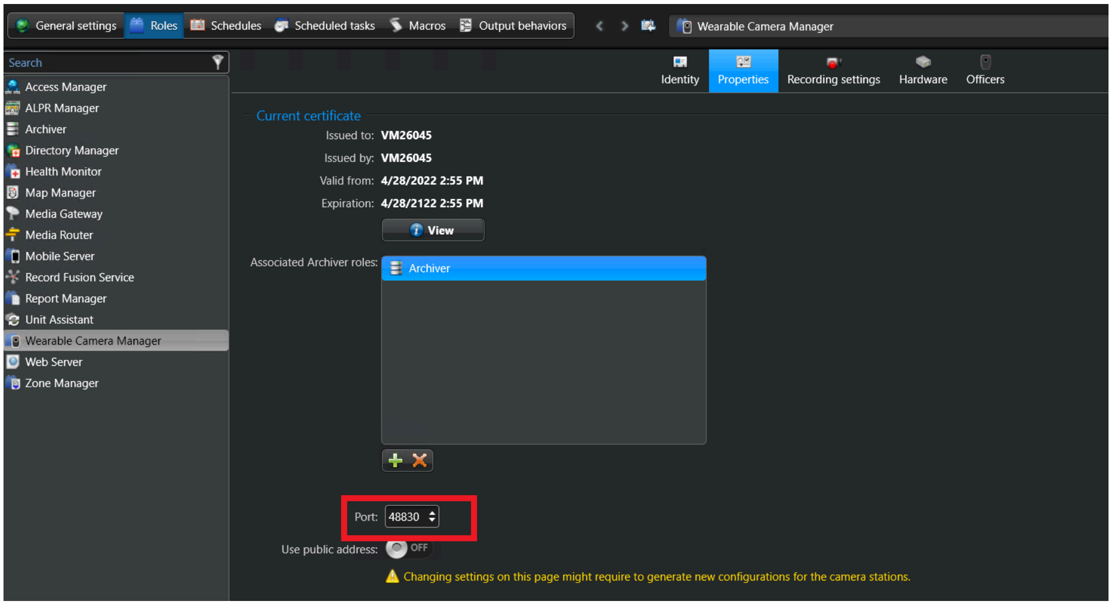
c) Retain the IP address of the server in a secure location.

4 Back up the port:

The correct port is required when recreating the firewall rules if there is a recovery.

a) Open Config Tool and navigate to **System** > **Roles** and select the Wearable Camera Manager role.

b) Click the **Properties** tab and retaif there is the port in a secure location.



Current certificate

Issued to: VM26045

Issued by: VM26045

Valid from: 4/28/2022 2:55 PM

Expiration: 4/28/2122 2:55 PM

Associated Archiver roles: Archiver

Port: 48830

Use public address: OFF

Changing settings on this page might require to generate new configurations for the camera stations.

After you finish

The Wearable Camera Manager server configuration is successfully backed up.

Related Topics

About body-worn cameras on page 648

Recovering the Wearable Camera Manager role on another server on page 657

Recovering the Wearable Camera Manager role on another server

If the server running the Wearable Camera Manager role fails, and you followed the recommended backup procedure, you can transfer the configuration to a new server.

Before you begin

- Back up the Wearable Camera Manager server configuration.
- Generate a current directory database backup.
- Install the new expansion server. See Installing Security Center expansion servers in the *Security Center Installation and Upgrade Guide*.

  CAUTION: On the *Server Configuration* page, do not connect to the main server during the installation process. Leave the **Main Server** section blank.
- Have the information for connecting the new expansion server available. You typically need IP addresses, certificates, and passwords.

What you should know

When the new server is configured, set the Internet Protocol of the server to match the exact IP of the previous server. You cannot have both machines running at the same time with the same IP.

To recover the Wearable Camera Manager role on another server:

1 In the Windows Firewall, open the port used by the Wearable Camera Manager role on the previous server:

   a) From the Windows Start menu, go to **Windows Defender Firewall** and select **Advanced** settings.

   b) Click **Inbound Rules** > **New rule**.

      The *New Inbound Rule Wizard* opens.

   c) On the *Rule Type* page, select **Port** and click **Next**.

   d) On the *Protocol and Ports* page, select **TCP** and enter the Wearable Camera Manager port number in **Specific local ports**, and click **Next**.

   e) On the *Action* page, select **Allow the connection** and click **Next**.

   f) On the *Profile* page, ensure that all options are selected and click **Next**.

   g) On the *Name* page, enter BWC and click **Finish**.

2 Ensure that the new server time matches the time on the other Security Center servers (Directory and Archiver).

   This setting is configured in Windows. It is recommended that an NTP server configured on each server running Security Center.

3 Restore the certificate from the original expansion server:

   a) Copy the backed-up certificate file to the new server.

   b) Right-click the certificate and click **Install PFX**.

   c) In the *Certificate Import Wizard*, select **Local machine** and click **Next**.

   d) Ensure that the file name is correct and click **Next**.

   e) Enter the password that was set when creating the certificate backup.

   f) In the *Certificate store* section, select **Place all certificates in the following store**.

   g) Click **Browse** and select **Personal** from the list.

   h) Click **Next** and click **Finish**.

4 Reset the serverIdentification id:

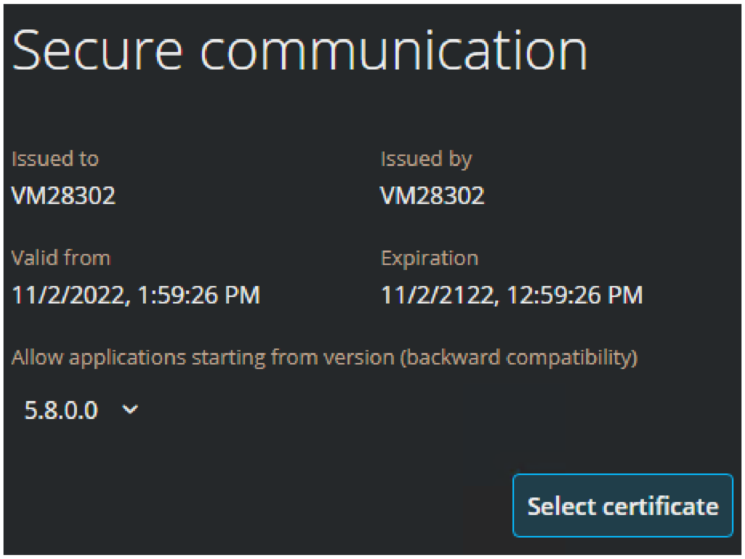
a) Stop the Genetec™ Server service.

b) Navigate to the Security Center configuration files folder: *C:\Program Files (x86)\Genetec Security Center 5.x\ConfigurationFiles*.

c) Open the *GenetecServer.gconfig* file and replace the serverIdentification id value with the serverIdentification id from the old server, and click **Save**.

d) Start the Genetec™ Server service.

e) Open Server Admin and click **Select certificate**.



Secure communication

Issued to
VM28302

Issued by
VM28302

Valid from
11/2/2022, 1:59:26 PM

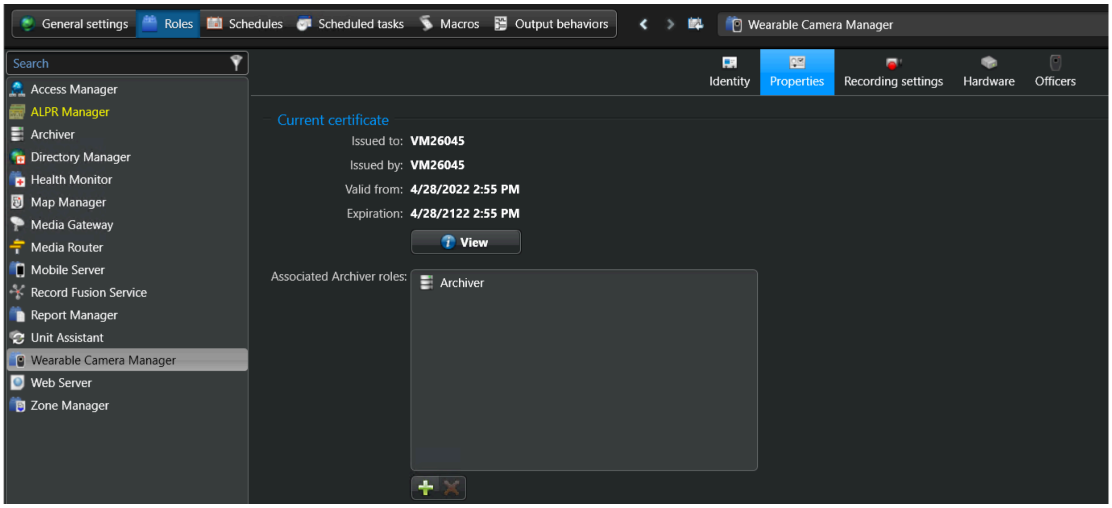
Expiration
11/2/2122, 12:59:26 PM

Allow applications starting from version (backward compatibility)
5.8.0.0

f) Select the certificate that was backed up from the old server.

g) Input the main Directory information: IP or hostname and Password, and click **Save**.

h) Open Config Tool and validate that the Wearable Camera Manager role has the correct information in the **Current Certificate** section and is not in a warning state.



Current certificate

Issued to: VM26045

Issued by: VM26045

Valid from: 4/28/2022 2:55 PM

Expiration: 4/28/2122 2:55 PM

Associated Archiver roles: Archiver

NOTE: If you have a warning on the Wearable Camera Manager role, see the *Troubleshooting* section.

5 Connect the new expansion server to the main server.

For more information, see Connecting expansion servers to the main server in the *Security Center Installation and Upgrade Guide*.

After you finish

The Wearable Camera Manager role is successfully restored on the new server.

Related Topics

Backing up the Wearable Camera Manager server configuration on page 654

29

Video archives

This section includes the following topics:

About video archives

A video archive is a collection of video, audio, and metadata streams managed by an Archiver or Auxilliary Archiver role. These collections are catalogued in the archive database that includes camera events linked to the recordings.

Each Archiver and Auxilliary Archiver is responsible for the video archives of the *cameras* it controls. The video archives are divided into the archive database, and the archive storage.

Archive database

The archive database in your Security Center system stores a video catalog and events. Each Archiver role and Auxiliary Archiver role in your system maintains an archive database.

The archive database stores the following types of information:

- A catalog of recorded video footage.
- Events describing the recording activities, such as when recording started and stopped, and what triggered the event.
- Events associated with the recorded video footage, such as motion detected, *bookmarks*, and occasional metadata.
- Events related to the archiving process, such as *Disk load is over 80%* and *Cannot write to any drive*.

For Archiver roles, the default name of the database is *Archiver*. For Auxiliary Archiver roles, the default name of the database is *AuxiliaryArchiver* .

IMPORTANT: A separate archive database must be configured for each server assigned to the Archiver role or Auxiliary Archiver role. Because of this requirement, it is a best practice to host the archive database locally on each server. When two or more archiving roles are hosted on the same server, you must assign a different database to each role instead of using the default one.

Related Topics

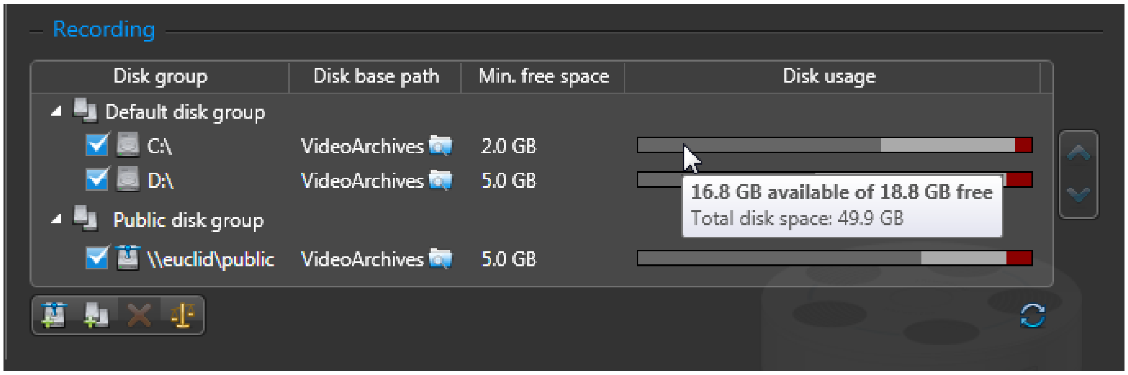
Databases on page 134

Archive storage

In Security Center, video recordings are stored on disk, in small G64 files that each contain one or more short video sequences.

Like the archive database, the archive file storage is specific to each server. The location of the video files and the description of the *video sequences* they contain (source camera, beginning and end of sequence) are stored in the database catalog managed by the *Archiver* or *Auxiliary Archiver*.

Both local drives and network drives can be used to store video. In the **Resources** tab for the archiving role, all local drives on the host server are listed by default and grouped under *Default Disk Group*, as shown in the following image:



Recording

Disk group	Disk base path	Min. free space	Disk usage
Default disk group			
☑ C:\	VideoArchives	2.0 GB	
☑ D:\	VideoArchives	5.0 GB	
Public disk group			
☑ \\euclid\public	VideoArchives	5.0 GB	

16.8 GB available of 18.8 GB free
Total disk space: 49.9 GB

Disk space cannot be allocated to video archives in advance. Instead, archiving roles can only use a limited amount of the available disk space. This limit is set by the **Min. free space** attribute for each disk. The recommended minimum free space is at least 2% of the total disk space, or 2 GB per TB.

IMPORTANT: You must ensure that the service user running the Archiver or Auxiliary Archiver role has write access to all the archive root folders assigned to the role.

Archive storage requirements

Because the Archiver role and Auxiliary Archiver roles can control a different number of cameras, you must evaluate the storage requirements for each of these roles separately.

The storage requirements are affected by the following factors:

- Number of cameras to archive.
- Archive retention period: amount of time to keep the archives online.
- Percentage of video files protected from automatic deletion.
- Percentage of recording time, which depends on the selected archiving mode: continuous, on motion, manual, scheduled, or off. Continuous recording consumes disk space faster than the other archiving modes.
- Frame rate: higher frame rate recordings need more storage space.
- Image resolution, which depends on the video data format: higher resolution recordings need more storage space.
- Percentage of movement: most video encoding schemes compress data by storing only the changes between consecutive frames. Scenes with a lot of movement require more storage than scenes with little movement.
- Audio: including audio increases the required storage space.
- Metadata from features such as *video analytics*, *privacy protection*, and *fusion stream encryption*. Included metadata can increase the required storage space.

TIP: Regularly checking the disk usage statistics is the best way to estimate future storage requirements, and to make quick adjustments.

Related Topics

Camera - Video tab on page 1252
Freeing up storage space for video files on page 666
Configuring recording settings for cameras on page 582
Monitoring disk space available for video files on page 665

Managing video archives

You must work with your video archives to ensure that the recordings are always available to assist an investigation.

Security Center stores surveillance video as *video archives*. You control where the archives are stored and how long they are retained. To ensure your video is properly archived and available when you need it, you must perform the following tasks:

- Check the archive storage requirements to ensure you have enough room for your video recordings.
- If storage performance is an issue, consider distributing the archive storage over multiple disks.
- Regularly monitor how much disk space you have left to ensure there is always sufficient space for new recordings.
- When required, free up disk space by deleting older video files, shortening retention periods for cameras, and so on.
- Ensure the recordings are properly archived, easily accessible, and secure. You can:
  - Transfer video recordings from cameras or other edge devices to your video archives.
  - Copy video archives from one Archiver role to another.
  - Back up video archives to protect them from loss.
  - Restore video archives from a backup to an Archiver.
- Protect important video files from being automatically deleted.
- Protect important video files from tampering by adding digital signatures.
- Audit the archive storage by reviewing the video file properties.
- If required, manage the effects of Daylight Savings Time on your video archives.
- Import external video files to Security Center.

Related Topics

About video archives on page 661

Distributing archive storage over multiple disks

To avoid a bottleneck on the Archiver or Auxiliary Archiver due to disk throughput, you can enable the role to write simultaneously to multiple disks.

What you should know

The Archiver and Auxiliary Archiver roles can write to multiple disks by spreading the video archive over several *disk groups*. Each disk group must correspond to a separate disk controller. By splitting the video archive from different cameras over different disk groups, you can maximize throughput in terms of disk access.

CAUTION: Nothing prevents other applications from using the disk space set aside for the Archiver or Auxiliary Archiver, so it is recommended to assign a disk that is not shared with other applications to these roles. In cases where multiple Archivers share the same server, use a separate disk for each.

To distribute the archiving cameras over multiple disk groups:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Select the Archiver or Auxiliary Archiver role, and click the **Resources** tab.

3 To create a disk group, click **Add group** (🖴).

4 In the **Disk group** column, click **New disk group** and type a name for the group.

5 Click **Camera distribution** (⚖).

6 In the *Camera distribution* dialog box, divide the cameras between the disk groups by selecting them one at a time and moving them with the arrow buttons.

7 Click **Close** > **Apply**.

Monitoring disk space available for video files

To prevent a sudden stop of video archiving, you should regularly monitor how much disk space you have left.

What you should know

Too many protected video files on a disk can deplete the storage space available for new video files. When regularly checking your disk space, you should also check the percentage of protected video files on each disk.

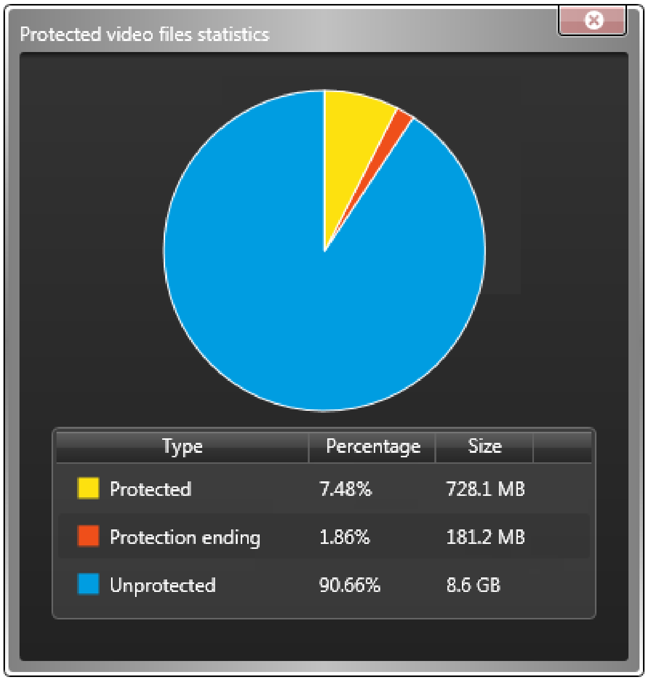
TIP: You can create an *event-to-action* to alert you when an Archiver or Auxiliary Archiver is running out of disk space, or has stopped archiving. You can also monitor incoming camera events on the Archiver and be notified if an unusually high event rate is occurring. This allows you to investigate, take action, and prevent performance issues.

To monitor the disk space available for video files:

1. Open the *Video* task, and select the Archiver or Auxiliary Archiver role.
2. Click the **Resources** tab, and then click **Statistics** ().
3. In the *Statistics* dialog box, click **Refresh** () to see the latest information.

   NOTE: Information in the *Statistics* dialog box does not refresh automatically. If information is displayed, the **Last update** timestamp shows when that information was last updated.
4. In the *Statistics* dialog box, check the following statistics:
   - **Available Space:** Disk space available for video archives.
   - **Average disk usage:** Average space used per day (first line) and average space used per camera per day (second line).
   - **Estimated remaining recording time:** Number of days, hours, and minutes of recording time left based on the average disk usage and the current load.
   - **Active cameras:** Number of cameras that are currently active.
   - **Archiving cameras:** Number of cameras for which archiving is enabled.

5 To view statistics for protected video files, select a disk group and click the (●) icon.



Protected video files statistics

Type	Percentage	Size
🟨 Protected	7.48%	728.1 MB
🟥 Protection ending	1.86%	181.2 MB
🟦 Unprotected	90.66%	8.6 GB

The pie chart indicates the status of video files on the disk, as follows:

- **Protected:** Percentage of video files on the disk that are currently protected.
- **Protection ending:** Percentage of video files on the disk that a user has decided to unprotect. When a user selects to remove protection from a video file, the Archiver waits 24 hours before removing protection from the file. During this time, the status indicates *Protection ending*.
- **Unprotected:** Percentage of video files on the disk that are not protected.

After you finish

If the disk is getting full, consider checking the video archives for videos that you can delete. You can also configure the Archiver settings to free up as much disk space as possible.

Freeing up storage space for video files

Within each disk group, you can free up storage space for new video files.

What you should know

There are different ways to free up storage space for video files. Using a combination of the following strategies can help to maximize the available storage:

- Delete the oldest video files when available disk space gets low. This strategy is recommended if most of your video footage is equally important, and you want to keep as much footage as possible. This maximizes disk usage.
- Set archiving retention periods for cameras to specify the amount of time that recorded footage must be kept online. Video is automatically deleted at the end of the retention period. This strategy keeps more important video footage for a longer period.
- Limit the size and length of video files. If you protect many short video sequences from deletion, limiting the size of your video files can help to optimize your storage use.

- Limit the disk storage space allocated to protected video files; they are not automatically deleted during normal cleanup procedures.

IMPORTANT: Archiving stops when disk space runs out. It is highly recommended to align your file retention strategies with the available storage space. Only deleting files when storage is full can impact archiving performance.

To free up storage space for video files:

1. Open the *Video* task, and select the Archiver or Auxiliary Archiver to configure.
2. Click the **Resources** tab, and click **Advanced settings**.
3. In the *Advanced settings* dialog box, set the following options as required:
   - Set **Delete oldest video files when disks are full** to **ON**.
   - Set **Protect video threshold** to the maximum percentage of storage space that protected video files can occupy on disk.

     When this threshold is exceeded, the Archiver generates a *Protected video threshold exceeded* event every 15 minutes, so you can review the video files and delete the ones that are no longer needed. The Archiver does not delete protected files.
   - In the *Video files* section, set the following:
     - The **Maximum length** for video sequences, in minutes.
     - The **Maximum size** of video files. Select **Specific**, and set a maximum size, in megabytes.
4. After configuring the advanced settings, click **OK** > **Apply**.

To set a retention period for video stored by an Archiver or Auxiliary Archiver:

1. In the *Video* task, select an Archiver or Auxiliary Archiver in the role entity tree and do one of the following:
   - For an Archiver role, click the **Camera default settings** tab.

     NOTE: Different retention periods can be configured for each server associated to the role.
   - For an Auxiliary Archiver role, click the **Camera recording** tab.
2. Set **Automatic cleanup** to the required number of days, and click **Apply**.

To set a retention period for a specific camera:

1. In the *Video* task, expand the role entity tree, and select the camera.

   This is helpful for cameras that have more important video footage.

   TIP: Set a shorter retention period for PTZ cameras, because they often use more storage due to the increased movement.
2. Click the **Recording** tab.
3. If **Recording settings** is set to **Inherit from Archiver**, switch it to **Custom settings**.
4. Set **Automatic cleanup** to the required number of days, and click **Apply**.

Transferring video archives

Use Security Center to move your video files from one location to another. Moving video ensures that it is properly archived, easily accessible, and secure.

Security Center lets you dynamically manage where your video files are stored with archive transfer. Using archive transfer you can:

- Transfer video recordings from cameras or other edge devices to your video archives.
- Copy video archives from one Archiver role to another.
- Back up video archives to protect them from loss.
- Restore video archives from a backup to an Archiver.

With archive transfer, you gain full control of where your video recordings are stored. This flexibility reduces storage costs when maintaining long-term archives and helps you optimize video search and investigation performance.

To better manage repeating transfers, you can define *transfer groups*. A transfer group is a persistent archive transfer scenario that lets you run a video transfer without redefining the transfer settings. These transfers can be scheduled or executed on demand. Transfer groups define which cameras or archiving roles are included in the transfer, when the archives are transferred, what data is transferred, and so on.

NOTE: Only system administrators can configure archive transfer settings.

Transfer groups only move new video. For example, if the last frame retrieved from a unit is "7/30/2014 3:44:40" and you try to retrieve video between 3:40:00 and 3:50:00, only video between 3:44:40 and 3:50:00 is retrieved and stored in the target Archiver.

Before a major operation, such as a software upgrade or server replacement, archive transfer lets you act quickly to move important video archives without creating a transfer group.

In addition to video recordings, the following information is sent with an archive transfer, if available:

- Audio and metadata
- Digital signatures
- Camera blocking settings
- Protection settings

When video is transferred to an Archiver, it is kept in accordance with the retention period of that Archiver.

Limitations of archive transfer

- Only original files can be transferred between Archivers. For example, archives can only be duplicated from the Archiver where the video was originally recorded.
- ALPR images and video streams stored in the Archiver database are not transferred or backed up with the Video Archiver transfer feature in Security Center despite the fact that the ALPR unit is displayed in the Area View.

Archive transfer troubleshooting

If your Archiver goes offline during an archive transfer and the process stops, the transfer must be restarted after the Archiver reconnects.

- If you were performing a manual archive transfer, then you must restart the process manually.
- If the archive transfer was set to run on a schedule, then the transfer restarts at the next scheduled time.

NOTE: The archive transfer restarts at the last successfully transferred frame.

Related Topics

Consolidating video archives after Archiver failover on page 197

Retrieving video recordings from units

To store video on your video units, and periodically transfer those recordings to Security Center, you must enable edge recording on the units and configure the cameras to transfer video to their main Archiver.

Before you begin

You must determine whether the video unit supports edge recording and archive transfer. To find out which edge devices are currently supported, contact Genetec™ Technical Assistance.

What you should know

You can configure the archives to be retrieved automatically when the unit connects to the Archiver.

You can continue to record video on the Archiver, even if the camera is configured for archive transfer. Cameras can only be added to one transfer group for retrieving video recordings from units.

Archive transfer from units to Archivers is helpful in the following scenarios:

- For remote sites connected to a central site with limited bandwidth: Typically, a server is deployed at the remote site to host the recording. However, with archive transfer you can retrieve the video directly from the cameras on demand without requiring a server.
- For city-wide surveillance using edge recording cameras: Cameras are always recording. Recordings are only retrieved on demand for investigation purposes, or outside of peak hours.
- If there is a network failure, the portions of video that are missing from the Archiver recordings can be retrieved from the video unit.

To retrieve video archives from units:

1. Enable edge recording on the video unit.
2. Select which cameras will transfer video archives to the Archiver, and define the transfer settings. You can set transfers to occur upon connection, on a schedule, or manually.

Related Topics

Transferring video archives on page 668

Duplicating video archives on page 671

Turning on edge recording

To store recordings on a video unit, you must enable edge recording in the unit's settings. Security Center can retrieve these recordings and transfer them to an Archiver.

What you should know

You can set the video recording to be continuous, or triggered by specific events, such as inputs, motion, analytics, and so on. Edge recording can only be enabled from the unit’s web page.

To turn on edge recording:

1. Open the *Video* task.
2. Select the video unit and click **Unit** > **Unit’s web page** ( ) in the toolbar at the bottom of the workspace.

3. After opening to the unit's web page, follow the instructions from the unit’s manufacturer to enable recording.
4. Close the web browser window when you are done.

Configuring video transfer settings for cameras

To transfer video recordings from video units to Security Center, you must configure the video transfer settings for those cameras, such as the type of video data you want to download, and when.

Before you begin

Enable edge recording on all required cameras.

To configure video transfer settings for cameras:

1. From the Config Tool home page, open the *Video* task and click the **Archive transfer** view.
2. Click **Add an item** > **Retrieve from edge**.
3. In the *Transfer group properties* dialog box, enter a name for this archive transfer scenario.
4. In the *Sources* section, click **Add an item** (✚), select the cameras you want, and then click **Add**.

   TIP: Hold Ctrl or Shift to select multiple cameras.
5. For **Recurrence**, select a schedule for the archive transfer:
   - **Manual:** Transfer archives manually.
   - **Minutes:** Transfer archives every 1-59 minutes.
   - **Hourly:** Transfer archives every 1-23 hours.
   - **Daily:** Transfer archives every day at the specified time. Optionally, set a maximum duration for the transfer to complete.
   - **Weekly:** Transfer archives every week, on specific days at the specified time. Optionally, set a maximum duration for the transfer to complete.

   NOTE: If you set a maximum duration to transfer files on a *Daily* or *Weekly* schedule, ongoing transfers are stopped at the specified time, and will resume from the last successfully transferred video frame at the next scheduled transfer. If you do not set a maximum duration, and the transfer is still in progress at the beginning of the next scheduled transfer, then the new transfer starts when the current transfer is completed.

   Transferring archives on a schedule is recommended for fixed cameras with limited network bandwidth. The transfer can be scheduled for a time when network demand is low.
6. To retrieve archives upon connection to the network, set the **Upon reconnection** to **ON**, and specify how many seconds the Archiver must wait before querying the edge device for archives to transfer. The edge device must have enough time to finish writing the video it is recording to local storage before starting the transfer.

   This option is recommended for cameras connected to mobile units that regularly move into and out of Wi-Fi coverage. It is also helpful if you have an unstable network where your cameras frequently go on and offline.
7. Under *Data*, select **All** to transfer everything since the last successful transfer, or **Specific** to transfer specific sequences based on event filters.

8 If you select **Specific**, select the data types to transfer:

- **All archives when the camera was offline:** Transfer video segments recorded between *Unit lost* and *Unit discovered* events.
- **Alarms:** Transfer video segments related to alarm events. The record of the alarm itself is not transferred.
- **Bookmarks:** Transfer video segments that contain bookmarks.
- **Input triggers:** Transfer video segments that contain input events.
- **Motion events:** Transfer video segments recorded between *Motion on* and *Motion off* events. This option only applies to unit motion detection.
- **Video analytics events:** Transfer video segments that contain video analytics events.
- **Time range:** Transfer video segments recorded during a specific period. You can specify a time range or a relative time range, such as the last *n* days, hours, or minutes.

9 Event-based transfer only: If you selected specific data, specify how many seconds of video should be transferred before and after the event occurs.

Example: If you select the **Motion events** filter, this setting indicates how many seconds of video preceding the *Motion on* event, and how many seconds of video following the *Motion off* event are included in the transfer.

10 Click **Save**.

Duplicating video archives

To copy video archives from one Archiver to another, you can duplicate specific archives on a schedule using archive transfer. Duplicate archives can be queried in Security Desk.

What you should know

When duplicating video from one Archiver role to another, the original archives are kept by the source Archiver until the retention period ends.

Video transfer between Archivers is helpful in the following scenarios:

- For multi-tiered storage solutions: High quality video is recorded in real-time on the first Archiver, which uses a costly, high-performance storage device. Important video files are periodically duplicated on the second Archiver, which uses a slower device that is better for long-term storage.
- If you moved video units to a new Archiver using the Move unit tool and you also want to transfer the video archives from those cameras to the new Archiver.
- Transferring video recordings from a federated site to a central system for long-term storage, local investigations, and to manage bandwidth.

To duplicate archives:

1 From the Config Tool home page, open the *Video* task, click the **Roles and units** view, and select an Archiver to duplicate.

2 Click the **Resources** tab, and then click **Advanced settings**.

3 Set **Max archive transfer throughput** to the maximum bandwidth available to the Archiver for archive transfer, and then click **OK** > **Apply**.

This setting ensures that enough network bandwidth is available for live video and playback requests.

4 In the *Video* task, click the **Archive transfer** view.

5 Click **Add an item** > **Duplicate archives**.

6 In the *Transfer group properties* dialog box, name this archive transfer scenario.

7. In the *Sources* section, click **Add an item** (➕), select the cameras or Archivers you want, and then click **Add**.

   When a camera is selected as a source, the transfer will include associated video from all Archivers.

   TIP: Hold Ctrl or Shift to select multiple cameras or Archivers.

8. From the **Destination** list, select an Archiver to receive the video.
9. For **Recurrence**, select a schedule for the archive transfer:
   - **Manual:** Transfer archives manually.
   - **Minutes:** Transfer archives every 1-59 minutes.
   - **Hourly:** Transfer archives every 1-23 hours.
   - **Daily:** Transfer archives every day at the specified time. Optionally, set a maximum duration for the transfer to complete.
   - **Weekly:** Transfer archives every week, on specific days at the specified time. Optionally, set a maximum duration for the transfer to complete.

   NOTE: If you set a maximum duration to transfer files on a *Daily* or *Weekly* schedule, ongoing transfers are stopped at the specified time, and will resume from the last successfully transferred video frame at the next scheduled transfer. If you do not set a maximum duration, and the transfer is still in progress at the beginning of the next scheduled transfer, then the new transfer starts when the current transfer is completed.

   Transferring archives on a schedule is recommended for fixed cameras with limited network bandwidth. The transfer can be scheduled for a time when network demand is low.

10. In the **Coverage** option, select whether to transfer all the data that has been accumulated since the last transfer, or only for a set range of days.
11. Under *Data*, select **All** to transfer everything since the last successful transfer, or **Specific** to transfer specific sequences based on event filters.
12. If you select **Specific**, select the type of data to transfer:
    - **Alarms:** Transfer video segments related to alarm events. The record of the alarm itself is not transferred.
    - **Bookmarks:** Transfer video segments that contain bookmarks.
    - **Input triggers:** Transfer video segments that contain input events.
    - **Motion events:** Transfer video segments recorded between *Motion on* and *Motion off* events. This option only applies to unit motion detection.
    - **Protected video:** Transfer video segments that are protected.
    - **Video analytics events:** Transfer video segments that contain video analytics events.
    - **Time range:** Transfer video segments recorded during a specific period. You can specify a time range or a relative time range, such as the last *n* days, hours, or minutes.
13. Event-based transfer only: If you selected specific data, specify how many seconds of video should be transferred before and after the event occurs.

    Example: If you select the **Motion events** filter, this setting indicates how many seconds of video preceding the *Motion on* event, and how many seconds of video following the *Motion off* event are included in the transfer.

14. Click **Save**.

Related Topics

Transferring video archives on page 668

Retrieving video recordings from units on page 669

Backing up video archives on a schedule

To save important video on a regular basis, you can back up specific archives to a file server or a network drive on a schedule using archive transfer.

What you should know

The video is saved to G64x video files, which can be restored at a later time. Backed up video files are not searchable in Security Desk unless they are restored, but the original files are still searchable.

You can also back up video archives manually if you need to bypass the backup schedule.

Backing up your video archives is helpful in the following scenarios:

- If you are performing maintenance on the server and need to temporarily store the archives in a secure location.
- If your Archiver fails and you need to restore the video to another Archiver.

To back up video archives on a schedule:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Select an Archiver and click the **Resources** tab.

3 In the *Backup configuration* section, set the following options:
   - **Backup folder:** Location where backed up archives are saved as G64x files.
   - **Delete oldest files when disks are full:** Turn this option on to delete the oldest video archives when the disk is full.
   - **Automatic cleanup:** Turn this option on to specify a retention period for the backed up video archives (in days). If you do not enable this option, backed up video archives are not automatically deleted by the system, and must be manually removed.

4 Click **Advanced settings**.

5 Set **Max archive transfer throughput** to the maximum bandwidth available to the Archiver for archive transfer, and then click **OK** > **Apply**.

6 In the *Video* task, click the **Archive transfer** view.

7 Click **Add an item** > **Backup**.

8 In the *Transfer group properties* dialog box, name this archive transfer scenario.

9 In the *Sources* section, click **Add an item** (➕), select the cameras or Archivers you want, and then click **Add**.

   When a camera is selected as a source, the transfer will include associated video from all Archivers.

   TIP: Hold Ctrl or Shift to select multiple cameras or Archivers.

10 For **Recurrence**, select a schedule for the archive transfer:
   - **Manual:** Transfer archives manually.
   - **Minutes:** Transfer archives every 1-59 minutes.
   - **Hourly:** Transfer archives every 1-23 hours.
   - **Daily:** Transfer archives every day at the specified time. Optionally, set a maximum duration for the transfer to complete.
   - **Weekly:** Transfer archives every week, on specific days at the specified time. Optionally, set a maximum duration for the transfer to complete.

   NOTE: If you set a maximum duration to transfer files on a *Daily* or *Weekly* schedule, ongoing transfers are stopped at the specified time, and will resume from the last successfully transferred video frame at the next scheduled transfer. If you do not set a maximum duration, and the transfer is still in progress at the beginning of the next scheduled transfer, then the new transfer starts when the current transfer is completed.

Transferring archives on a schedule is recommended for fixed cameras with limited network bandwidth. The transfer can be scheduled for a time when network demand is low.

11 In the **Coverage** option, select whether to transfer all the data that has been accumulated since the last transfer, or only for a set range of days.

12 Under *Data*, select **All** to transfer everything since the last successful transfer, or **Specific** to transfer specific sequences based on event filters.

13 If you select **Specific**, select the type of data to transfer:

- **Alarms:** Transfer video segments related to alarm events. The record of the alarm itself is not transferred.
- **Bookmarks:** Transfer video segments that contain bookmarks.
- **Input triggers:** Transfer video segments that contain input events.
- **Motion events:** Transfer video segments recorded between *Motion on* and *Motion off* events. This option only applies to unit motion detection.
- **Protected video:** Transfer video segments that are protected.
- **Video analytics events:** Transfer video segments that contain video analytics events.
- **Time range:** Transfer video segments recorded during a specific period. You can specify a time range or a relative time range, such as the last *n* days, hours, or minutes.

14 Event-based transfer only: If you selected specific data, specify how many seconds of video should be transferred before and after the event occurs.

Example: If you select the **Motion events** filter, this setting indicates how many seconds of video preceding the *Motion on* event, and how many seconds of video following the *Motion off* event are included in the transfer.

15 Click **Save**.

The video archives are backed up at the scheduled time.

Related Topics

Transferring video archives on page 668

Restoring video archives on page 676

Transferring video archives on demand on page 675

Bypassing archive transfer schedules

If you need to retrieve video recordings from a video unit, copy archives to another Archiver, or back up your video archives before the next scheduled transfer, you can execute a scheduled transfer on demand.

Before you begin

The archive transfer settings for the transfer group must be configured.

To bypass an archive transfer schedule:

1 From the Config Tool home page, open the *Video* task and click the **Archive transfer** view.

2 Select one or more of the transfer groups in the list.

TIP: Hold Ctrl or Shift to select multiple cameras or Archivers.

3 Click **Start transfer for selected transfer groups** (▶).

Transferring video archives on demand

To quickly safeguard your video archives before a major operation such as a software upgrade or server replacement, you can move video archives on demand without creating a transfer group.

To transfer video archives on demand:

1. From the Config Tool home page, open the *Video* task and click the **Archive transfer** view.
2. At the bottom of the window, click **Transfer now**.
3. In the *Transfer group properties* dialog box, select the type of transfer you want to perform:
   - **Backup:** Backup video archives from an Archiver to a G64x file.
   - **Duplicate archives:** Copy video archives from one Archiver to another.
4. In the *Sources* section, click **Add an item** (➕), select the cameras or Archivers you want, and then click **Add**.

   When a camera is selected as a source, the transfer will include associated video from all Archivers.

   TIP: Hold Ctrl or Shift to select multiple cameras or Archivers.
5. For **Duplicate archives**, select an Archiver to receive the video from the **Destination** list.
6. For **Time range**, set the start and end time of the video archives to transfer.
7. Under *Data*, select **All** to transfer everything since the last successful transfer, or **Specific** to transfer specific sequences based on event filters.
8. If you select **Specific**, select the type of data to transfer:
   - **Alarms:** Transfer video segments related to alarm events. The record of the alarm itself is not transferred.
   - **Bookmarks:** Transfer video segments that contain bookmarks.
   - **Input triggers:** Transfer video segments that contain input events.
   - **Motion events:** Transfer video segments recorded between *Motion on* and *Motion off* events. This option only applies to unit motion detection.
   - **Protected video:** Transfer video segments that are protected.
   - **Video analytics events:** Transfer video segments that contain video analytics events.
   - **Time range:** Transfer video segments recorded during a specific period. You can specify a time range or a relative time range, such as the last *n* days, hours, or minutes.
9. Event-based transfer only: If you selected specific data, specify how many seconds of video should be transferred before and after the event occurs.

   Example: If you select the **Motion events** filter, this setting indicates how many seconds of video preceding the *Motion on* event, and how many seconds of video following the *Motion off* event are included in the transfer.
10. Click **Start**.

    The archive transfer begins immediately.

Related Topics

Transferring video archives on page 668

Backing up video archives on a schedule on page 673

Restoring video archives

After backing up your video archives, you can restore the backup to an Archiver.

What you should know

By default, backup files are retrieved from the **Backup folder**, which is specified in the *Backup configuration* section of the *Resources* page when you back up video archives on a schedule. If required, G64x backup files can also be selected from a different folder.

Backup files can only be restored to an Archiver in your Security Center system.

Only the types of video data that were backed up are restored. After restoring the archives, the video is searchable using Security Desk reports.

To restore video archives:

1. From the Config Tool home page, open the *Video* task and click the **Archive transfer** view.
2. At the bottom of the window, click **Restore archives**.
3. In the *Restore archives* dialog box, select a **Restore type**. The following options are available:
   - **Camera:** Restore video from enrolled cameras that was backed up to the default backup folder. If you select **Camera**, you must specify one or more enrolled cameras to restore.

     NOTE: Video archives for a deleted camera can only be restored in this way if video from that camera is still managed by the Archiver. If a camera and all associated archives are deleted, you must use **Custom** to restore the archives.
   - **Archiver:** Restore video from specific Archivers that was backed up to the default backup folder. If you select **Archiver**, you must select one or more Archivers to restore.
   - **Custom:** Restore video from a specific backup file or location, such as a folder, or a USB storage device. If you select **Custom**, you must select an Archiver to receive the video, and a backup file or location to load.
4. In the *When* section, select **From**, **To**, or both to filter for archives within the specified period.
5. Click **Find archives**.
6. Select the archives you want to restore.

   TIP: Hold Ctrl or Shift to select multiple cameras or Archivers.
7. If required, protect the restored archives from automatic deletion with the following options:
   - **Protect video from deletion:** Turns protection on or off for the restored video archives.
   - **Indefinitely:** No end date. You must manually remove the protection.
   - **For x days:** The video is protected for the selected number of days.
   - **Until:** The video is protected until the selected date.

   By default, **Protect video from deletion** is enabled and set to 5 days.

   BEST PRACTICE: When restoring old video sequences, it is best practice to protect your video files from being deleted because the retention period might have already passed.
8. Click **Restore**.

Related Topics

Backing up video archives on a schedule on page 673

Archive transfer status and details

You can monitor and review the status of your archive transfers from the *Archive transfer* page in the *Video* task, or view the details of any past transfer using the *Archive transfer history* task report.

The following information is provided for each transfer group:

- **Transfer group:** Group of cameras or Archivers with the same video transfer settings.
- **Type:** Video transfer type. Either *Retrieve from edge*, *Duplicate archives*, or *Backup*.
- **Recurrence:** How often the video transfer reoccurs, based on the defined schedule.
- **Status:** State of the current transfer. The status can be one of the following:
  - **Idle:** The transfer is waiting to start.
  - **Pending:** The transfer will start as soon as a spot opens in the download queue.
  - **Active:** The transfer has started. The progression and bit rate are shown.
  - **Error:** Some cameras could not be processed successfully, but others are still active.
  - **Success:** The transfer was successfully completed.
- **Transferred data size:** Size of the video data that was transferred.
- **Last transfer start:** Date and time the last transfer started.
- **Last transfer end:** Date and time the last transfer finished.
- **Last transfer status:** The status of the last transfer.
- **Next transfer:** Date and time when the next transfer is set to start.
- **Show transfer details (◕):** Transfer information about each camera in the transfer group.
  - **Source:** Name of the camera.
  - **To:** Destination of the transfer (an Archiver or the Archiver’s backup folder).
  - **Status:** State of the transfer.
  - **Transferred data size:** Size of the video data that was transferred.
  - **Last transfer start:** Date and time the last transfer started.
  - **Last transfer end:** Date and time the last transfer finished.
  - **Last transfer status:** The status of the last transfer.
  - **Result:** Result of the last transfer. Can display errors about the transfer, if any occurred.

You can also view the details of any past archive transfer using the *Archive transfer history* task report. The following information is provided for each transfer group.

- **Transfer group:** Group of cameras or Archivers with the same video transfer settings.
- **Trigger date:** Date and time when the selected transfer started.
- **End transfer time:** Date and time when the selected transfer finished.
- **Trigger reason:** How the transfer was triggered, either scheduled or manually.
- **Transfer result:** Result of the selected transfer. Double-click this column for more details on the result status.

Protecting video files from deletion

You can protect important video footage from being deleted by the system when the Archiver's disk space becomes full, or when its normal retention period has ended.

What you should know

Video can be protected against deletion. Protection is applied on all video files needed to store the protected video sequence. Because no video file can be partially protected, the actual length of the protected video sequence depends on the granularity of the video files.

The Archiver cannot protect partial files, so you might protect a larger segment than the one you select.

CAUTION: Too many protected video files on a disk can reduce the storage space available for new files. To avoid wasting storage space, regularly check the percentage of protected video files on each disk.

To free up storage space, you can back up the protected video files or duplicate the protected files on another Archiver using *archive transfer*, and then unprotect the original video file.

To protect a video file:

1 Open the **Archive storage details** task.

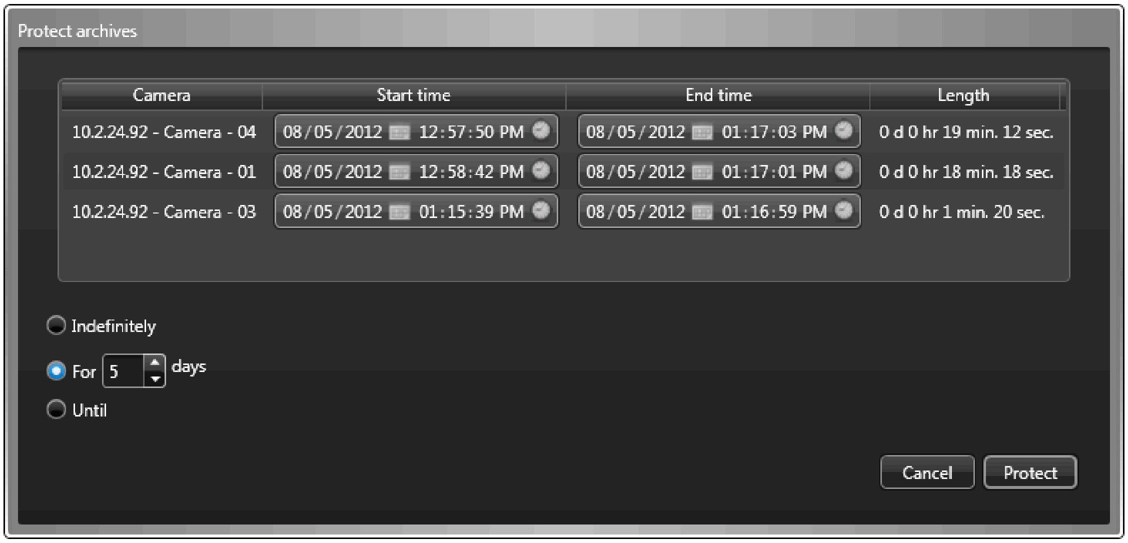
2 Generate your report.

The video files associated with the selected cameras are listed in the report pane.

3 From the report pane, select the video file to protect, and then click **Protect** ().

To select multiple video files, hold the Ctrl or Shift keys.

4 In the *Protect archives* dialog box, set the **Start time** and the **End time** for the video that you want to protect.



Protect archives

Camera	Start time	End time	Length
10.2.24.92 - Camera - 04	08 / 05 / 2012 12 : 57 : 50 PM	08 / 05 / 2012 01 : 17 : 03 PM	0 d 0 hr 19 min. 12 sec.
10.2.24.92 - Camera - 01	08 / 05 / 2012 12 : 58 : 42 PM	08 / 05 / 2012 01 : 17 : 01 PM	0 d 0 hr 18 min. 18 sec.
10.2.24.92 - Camera - 03	08 / 05 / 2012 01 : 15 : 39 PM	08 / 05 / 2012 01 : 16 : 59 PM	0 d 0 hr 1 min. 20 sec.

○ Indefinitely

● For 5 days

○ Until

5 Select how long to protect the video file from one of the following options:

- **Indefinitely:** No end date. You must manually remove the protection by selecting the video file in the report pane, and clicking **Unprotect** ().

  NOTE: If the retention period has passed, unprotected video files are not deleted immediately. If needed, you have 24 hours to restore the video protection.
- **For x days:** The video file is protected for the selected number of days.
- **Until:** The video file is protected until the selected date.

6 Click **Protect**.

The video file is protected.

Related Topics

Archive storage on page 661
Duplicating video archives on page 671
Transferring video archives on demand on page 675

Protecting video files against tampering

If you want to use your video evidence in court, you can enable digital signatures on the Archiver and the Auxiliary Archiver to protect your video against tampering and prove that it was not altered.

What you should know

A digital signature is cryptographic metadata added to video frames by the Archiver or Auxiliary Archiver to ensure their authenticity. If a video sequence is manipulated by adding, deleting, or modifying frames, the signature of the modified content will differ from the original, indicating that the video sequence has been tampered with.

To protect your video files against tampering:

1. Open the *System* task and click the **Roles** view.
2. Select an archiving role, click the **Resources** tab, and click **Advanced settings**.
3. Turn on the **Digital signature** option and click **OK** > **Apply**.

   Digital signatures require a cryptographic key. The required files, *fingerprintEddsa.bin* and *privateEddsa.bin*, are generated automatically and stored in the Security Center installation folder on each server hosting an archiving role.

Setting up a cryptographic key for digital signatures

A cryptographic key for digital signatures is generated automatically. If required, you can generate your own key and set the Archiver and the Auxiliary Archiver to use it.

To set up a cryptographic key for digital signatures:

1. In the Security Center installation folder, run *DigitalSignatureKeyGenerator.exe*.

   The program generates two 1 KB files named *fingerprintEddsa.bin* and *privateEddsa.bin* and saves them in the installation folder. The first file contains a random 20 B fingerprint, and the second file contains a cryptographic signature key. These two files will be different every time the program is executed.
2. In Config Tool, open the *System* task, and click the **Roles** view.
3. Select each archiving role that uses digital signatures, and restart it.
4. If you have a secondary server assigned to an archiving role, copy the same cryptographic files to the Security Center installation folder on that server.

The next time an Archiver or Auxiliary Archiver with **Digital signature** enabled records video to disk, the video files are digitally signed using the new cryptographic key.

Related Topics

Deactivating and activating roles on page 130

Viewing video file properties

You can view the file properties for video archives in local storage, such as file name, start and end time, file size, protection status, and so on, in the *Archive storage details* report. You can also change the protection status of the video files.

To view the properties of a video file:

1. From the homepage, open the *Archive storage details* task.
2. Set up the query filters for the report. Select one or more of the following filters:
   - **Cameras:** Select the camera to investigate.
   - **Custom fields:** Restrict the search to a predefined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
   - **Event timestamp:** Define the time range for the query. You can define the time range for a specific period or a relative period, such as the previous week or the previous month.
   - **Media type:**

     Select the type of media you are looking for:

     - **Video:** Files that contain video recordings.
     - **Audio:** Files that contain audio recordings.
     - **Metadata:** Files that contain metadata, such as overlays.
   - **Origin type:**

     Refine your search by selecting the origin of the files:

     - **Downloaded from the unit's internal storage:** Files created by the camera, downloaded from it by an Archiver, and currently stored on the Archiver's disk.
     - **Duplicated from another Archiver:** Files created by an Archiver and transferred to another one.
     - **On the unit's internal storage:** Files created by the camera and currently stored on it.
     - **Recorded by the Archiver:** Files created and currently stored by an Archiver.
     - **Restored from a backup:** Files restored from an offline backup set; that is, a backup file containing archives that were not accessible from Security Center prior to restoring them.
   - **Source:** The name of the system the camera belongs to.
   - **Status:**

     Select the video file status you want to investigate:

     - **Unprotected:** Video files that are not protected against the Archiver’s routine cleanup. These files can be deleted once their retention period expires, or when the Archiver runs out of disk space, depending on your Archiver role settings.
     - **Protection ending:** Video files that you unprotected less than 24 hours ago.
     - **Protected:** Video files that are protected. They are not deleted even when the disk is full. For these files, you can also specify a protection end date.
3. Click **Generate report**.

   The video files associated with the selected cameras are listed in the report pane, along with their file properties.
4. To view a video sequence in a tile, double-click or drag a video file from the report pane to the canvas.

   The selected sequence immediately starts playing.

After you finish

- To export a video archive in Security Desk, select the item in the report pane, and then click **Export video** (💿).
- To remove a video file, select the item in the report pane, and then click **Delete** (✖).
- To protect a video archive from automatic deletion, select the item in the report pane, and then click **Protect** (🔒).
- To unprotect a video archive, select the item in the report pane, and then click **Unprotect** (🔓).

Related Topics

Protecting video files from deletion on page 678

Report pane columns for the Archive storage details task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Archive storage details task.

- **Camera:** Camera name.
- **Custom fields:** Predefined custom fields for the entity. The columns only appear if custom fields are defined for the entity and were made visible to you when they were created or last configured.
- **Drive:** The drive on the server where the Archiver role is running.
- **End time:** End of the time range, playback sequence, or video sequence.
- **File name:** Name of the video file.
- **File size:** Size of the video file.
- **Length:** Length of the video sequence contained in the video file, in hours, minutes, and seconds.
- **Media type:** Type of media (video, confidential video, audio, metadata) contained in the file.
- **Origin type:** The origin of the file:
  - **Downloaded from the unit's internal storage:** Files created by the camera, downloaded from it by an Archiver, and currently stored on the Archiver's disk.
  - **Duplicated from another Archiver:** Files created by an Archiver and transferred to another one.
  - **On the unit's internal storage:** Files created by the camera and currently stored on it.
  - **Recorded by the Archiver:** Files created and currently stored by an Archiver.
  - **Restored from a backup:** Files restored from an offline backup set; that is, a backup file containing archives that were not accessible from Security Center prior to restoring them.
- **Protection status:** Protection status of the video file.
- **Server:** Name of the server hosting this role.
- **Source (entity):** The name of the system the camera belongs to.
- **Start time:** Beginning of the time range, playback sequence, or video sequence.

Managing the effects of Daylight Saving Time on video archives

Annual time changes to or from Daylight Saving Time (DST) can affect the way video archives are viewed and queried in Security Center.

Time changes do not prevent your cameras from recording video data. The *Archiver* always records using Coordinated Universal Time (UTC), which does not time shift for DST, and archive queries are always sent to the server with UTC timestamps.

Using UTC isolates video archives from the effects of time changes. However, because Security Desk and Config Tool can be configured to use, and display, a time zone other than UTC, side effects can be observed when time is adjusted backward or forward.

NOTE: The Eastern Standard Time (EST) time zone is used as an example, however this applies to all time zones that are subject to DST.

Effects of time adjusted backward

When time is adjusted backward, it changes from Daylight Saving Time (DST) to Eastern Standard Time (EST).

The time shift from DST to EST occurs at 2:00am. Before 2:00am, Security Center uses the DST (UTC-4). Starting from 2:00am, it uses the EST (UTC-5), as shown in the following table:

	DST		Time change	EST	
Local time	12:00am	1:00am	2:00am = 1:00am	2:00am	3:00am
Offset (hours)	-4	-4	-5	-5	-5
UTC	4:00am	5:00am	6:00am	7:00am	8:00am

Because the time was adjusted backward, the following behaviors can be observed when playing back video or exporting archives:

- The time shifts back by 1 hour in the timeline. After 1:59:59am, the displayed time falls back to 1:00:00am.
- The end time of a video sequence can be earlier than the start time.
- Exporting archives between 1:00am and 2:00am always includes an additional hour of video. For example, when exporting archives from 1:50am - 2:00am on the night of a time shift, the exported sequence includes 1 hour and 10 minutes of video. The query includes video from 5:50am - 7:00am UTC.

To prevent the time from shifting back or to export video without an extra hour of footage, configure Security Desk to use UTC. After exporting the sequence, you can revert to the previously configured time zone to view the sequence relative to your local time reference.

Effects of time adjusted forward

When time is adjusted forward, it changes from Eastern Standard Time (EST) to Daylight Saving Time (DST).

The time shift from EST to DST occurs at 2:00am. Before 2:00am, Security Center uses the EST (UTC-5). Starting from 2:00am, it uses the DST (UTC-4), as shown in the following table:

	EST		Time change	DST	
Local time	12:00am	1:00am	2:00am = 3:00am	4:00am	5:00am
Offset (hours)	-5	-5	-4	-4	-4
UTC	5:00am	6:00am	7:00am	8:00am	9:00am

Because the time was adjusted forward, the following behaviors can occur when playing back video or exporting archives:

- The time shifts forward by 1 hour in the timeline. At 1:59:59am, the displayed time advances to 3:00am.
- There are no archives to export between 2:00am and 3:00am, because this period was skipped.

To prevent the time from shifting forward by 1 hour during video playback, you must configure Security Desk to use UTC.

Changing the time zone to UTC

If you are working with archives that were recorded during a time change, and you want to remove the associated impacts from the video timeline, you can set the time zone to Coordinated Universal Time (UTC) in Security Desk before performing your task.

What you should know

Security Desk and Config Tool display time relative to the selected time zone. However, the server uses UTC, and the client application converts the server's UTC timestamps to the selected time zone. You can set client applications to use UTC to skip the time conversion and avoid the impacts when there is a time change.

NOTE: Time and date settings apply only to the client application you configure. Each application must be configured separately.

To change the time zone to UTC:

1. From the homepage, click **Options** > **Date and time**.
2. If required, select **Display time zone abbreviations** to show the selected time zone next to the time in the notification tray.
3. Select **Display time based on the following time zone**, and then select **(UTC) Coordinated Universal Time**.
4. Click **Save**.

The client application now displays current time and archive timestamps relative to the UTC time zone.

Importing external video files to Security Center

To view MOV, AVI, and MP4 video files in Security Center, you must import them using an offline device.

Before you begin

You must set the date and time on the device used to record your video files. Failing to set the date might prevent the files from being imported.

What you should know

Imported filenames must have the following format: *XXXX_YYYY.MM.DD_HH.MM.SS*,where *XXXX* is a descriptive name, and the other values represent the date and time.

The following codecs are supported:

- Video streams: H.263, H.264, MJPEG, and MPEG-4
- Audio streams: G.711, G.721, G.723, AAC (8 kHz or 16 kHz)

To import a video file:

1. From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.
2. Select an Archiver in the role entity tree to manage the offline device.
3. Click **Video unit** (➕).

   The *Manual add* dialog box opens.
4. From the **Manufacturer** list, select **Offline device**.
5. From the **Product type** list, select **Network share**.
6. Enter a **Unit Name**.

   This is the default name for the camera, and will be used to generate a unique identifier (GUID) for it.
7. Enter the **Path** to the location where you will place the video files to import.

   The path can be local or a shared network path. The user account running the Genetec™ Server service must have read and write access to the shared network folder.
8. Select a **Location** for the offline device in Security Center, and click **Add**.
9. In the *Video* task, select the Archiver managing the new offline device, and click the **Camera default settings** tab.
10. Ensure that **Automatic cleanup** is set to a longer duration than the oldest file you want to import.

    For example, if the oldest video file is 30 days old, set **Automatic cleanup** to at least 32 days so the file is not deleted immediately after import.

    IMPORTANT: The **Automatic cleanup** option also specifies the retention period for video from all the cameras that are managed by the selected Archiver. Ensure that any change does not affect your camera recording settings.
11. If required, copy video files to the **Path** set for the offline device.

    As the files are processed, they disappear from the folder. This can take up to 30 seconds, or more, depending on the number of files and their size.

    NOTE:

    - If a file does not disappear from the folder, the import failed.
    - If you see a *FailedAudioImports* folder, then the video files were imported but the audio was not. You can find the original file in this folder.

After you finish

View your imported video files using the *Archives* report. For more information, see the *Security Center User Guide*.

30

Cloud storage

This section includes the following topics:

About Cloud Storage

Cloud storage is a service from Genetec Inc. that extends on premise storage for Security Center Omnicast™ into the cloud. Video archives in Cloud storage benefit from extended retention periods, secure and redundant storage, and seamless retrieval from Security Desk.

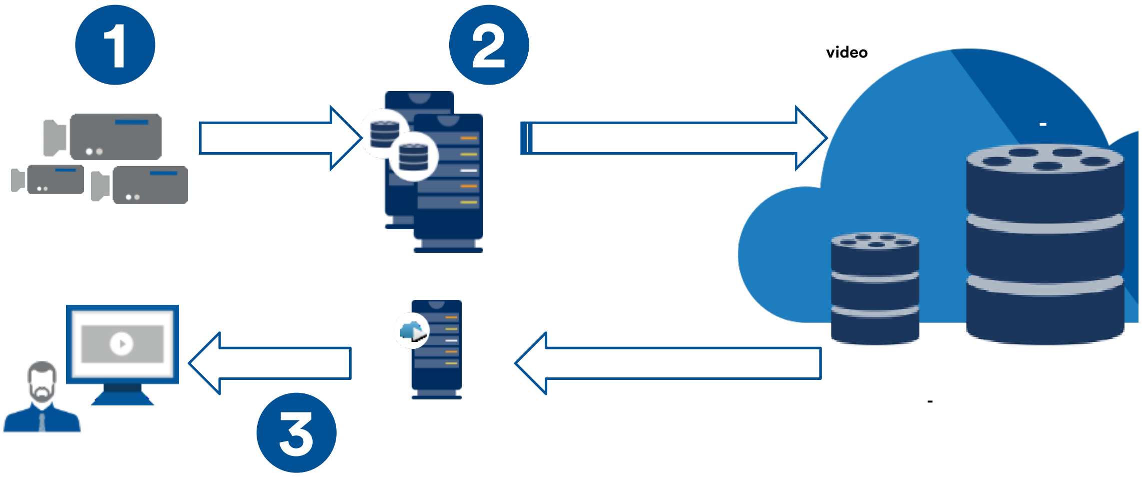
NOTE: Video archives can include video, audio files.

Main features

With a Cloud Storage subscription, you can store video archives in the cloud while continuing to use the full capability of your Security Center system. Cloud Storage offers:

- An extended retention period for your video archives.
- Protection and continued availability of your video archives in case of disaster.
- A flexible storage capacity that can increase or decrease to meet your changing needs.
- Reduced capital expenditures and lower costs to maintain your storage system.

How it works



Cloud Storage is an extension of your video surveillance system. Your cameras continue to be managed by the Archiver role. Cloud Storage works as follows:

1. Video archives are recorded on-premises and kept by the Archiver in accordance with your local retention policy.
2. After a configurable period in local storage, video archives are uploaded to the cloud.

   In the cloud, video archives are assigned to an access tier based on your cloud retention policy.
3. When needed, specific video archives are retrieved from the cloud and streamed by the Cloud Playback role to client stations.

Access tiers

Video archives in Cloud Storage are assigned to an access tier. The tier affects the availability of video archives and the cost of your Cloud Storage subscription. The following tiers are available:

- **Performance tier:** Offers quick playback of your video archives from the cloud. Recordings in the Performance tier are available to all clients and federated users connected to the system.
- **Long-term tier:** Offers low cost storage for retention periods of 180 days and longer. Video archives in the Long-term tier are not available immediately, and must be retrieved from Security Desk. Access to requested files is usually granted within 15 hours, and these files remain available at the Performance tier for seven days.

Depending on your requirements, and to control costs, video archives typically spend a short time in the Performance tier before moving to long-term storage.

Subscription required

Cloud Storage is sold by subscription. For more information on the subscription options, contact Genetec™ Sales.

Related Topics

Activating Cloud Storage on page 691

Applying Cloud Storage policies on page 693

Monitoring Cloud Storage on page 695

Best practices for Cloud Storage

Cloud Storage requires an internet connection. A slow or unstable connection can interrupt cloud services.

Unprotected video archives are automatically deleted depending on the retention policy and disk capacity. Protected video files in local storage are exempt from automatic deletion.

If video is deleted before being uploaded to the cloud, warnings appear in the Archiver diagnostic window. These warnings indicate that you should investigate and take action to prevent further data loss. While investigating the issue, protect video files in local storage from automatic deletion.

To prevent video files from being deleted before uploading to the cloud, consider the following best practices:

- Ensure that each Archiver server connecting to Cloud Storage has a stable internet connection.
- Ensure that the Archiver role has enough internet bandwidth to upload video.
- Evaluate the archive storage requirements and regularly monitor the disk space available for video files.
- If required, extend the retention period of the Archiver or specific cameras.
- Review your Cloud Storage policies and ensure that you transfer video archives before the local retention period ends.
- Back up important video archives regularly.
- If required, manage the effects of Daylight Savings Time (DST) on your video archives.

Limitations for Cloud Storage

Cloud Storage includes the following known limitations.

Issue	Description
No Auxiliary Archiver	Auxiliary Archiver roles are not supported. Only video archives handled by Archiver roles can be uploaded to Cloud Storage.
No camera blocking	*Camera blocking* is only available for video sequences in local storage. After the local retention period, video archives in Cloud Storage are not restricted by camera blocking.
No enrolling specific cameras	Cloud Storage cannot be enabled or disabled for specific cameras. All cameras managed by an Archiver using Cloud Storage are uploaded to the cloud.
No events and actions	Events and actions are not supported for video archives in the cloud. Bookmarks, custom events, motion events, and *video protection* are not available after the local retention period.
No metadata streams	Metadata streams, including those for *automatic license plate recognition (ALPR)* and *body-worn cameras (BWC)*, are only available for video archives in local storage. They are removed at the end of the local retention period.
No in-transit-and-at-rest encryption for files uploaded before 5.10.2.0	Cloud Storage supports in-transit-and-at-rest encryption with Security Center versions 5.10.2.0 and later.
No motion search in the cloud	*Motion search* is only available for video archives in local storage.
No video thumbnails	Thumbnails are only available for video archives in local storage. They are removed at the end of the local retention period.
Migrate from existing Cloud Archives to the new Cloud Storage	To migrate from Cloud Archives to Cloud Storage, you must contact your Genetec representative.

NOTE: If you have external SDK applications or macros that use the video playback functionality and require programming information, contact your sales engineering representative from Genetec Inc.

Activating Cloud Storage

To store video archives in the cloud, you must first activate Cloud Storage in Security Center, and select one or more Archiver roles that will upload data.

Before you begin

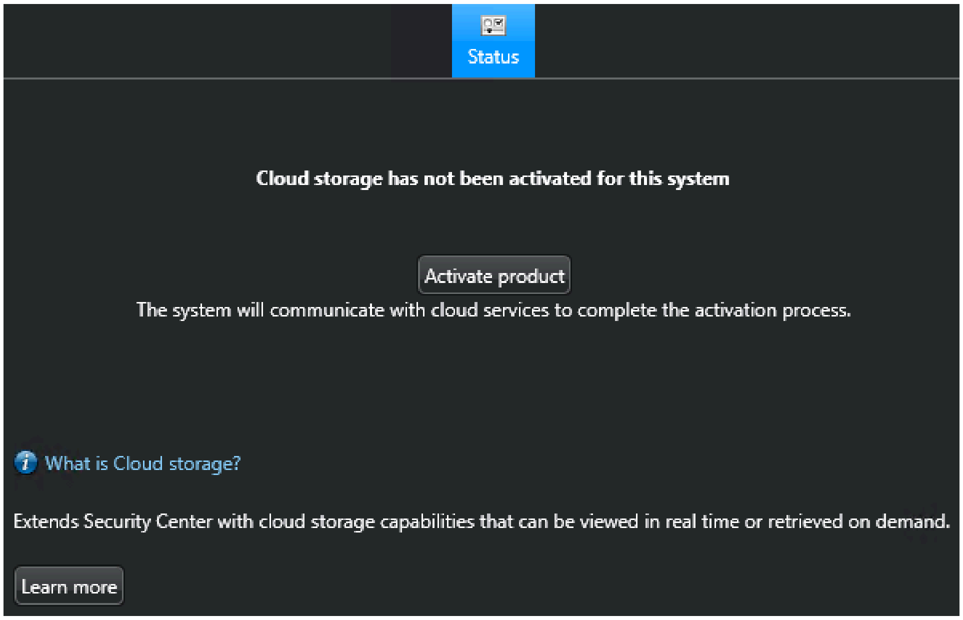
- You must have an active subscription for Cloud Storage.

  NOTE: To activate a Cloud Storage subscription, your representative of Genetec Inc. must confirm that a purchase order for the product has been received. After the confirmation, you will be notified that you can activate the product. You do not need to change your Security Center license to activate the subscription.
- Your user account must be a member of the Administrators group or have the *Cloud storage* privilege.
- Security Center must have access to the Internet and connectivity with the following:
  - **.blob.core.windows.net*
  - **.cloudarchives.geneteccloud.com*
  - **.video.geneteccloud.com*
  - *login.genetec.com*

To activate Cloud Storage:

1 Open the *Video* task and click the **Cloud storage** view.

The Cloud Storage *Status* page opens.



Cloud storage has not been activated for this system

The system will communicate with cloud services to complete the activation process.

Extends Security Center with cloud storage capabilities that can be viewed in real time or retrieved on demand.

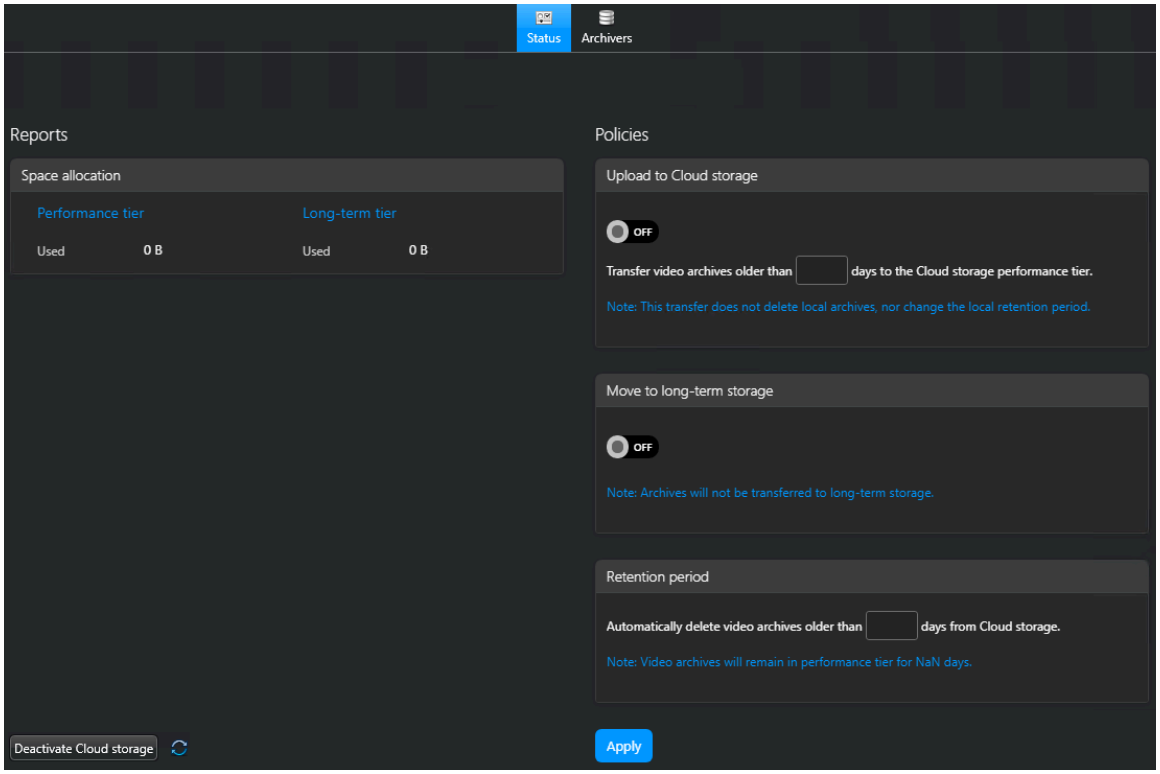
2 Click **Activate product**.

3 If a Cloud Playback role has not been created yet, the *Creating a role: Cloud Playback* wizard opens to create one.

The Cloud Playback role is used by Cloud storage to stream video archives from the cloud to clients and federated users connected to the system. Cloud Playback supports the Real Time Streaming Protocol (RTSP) locally and uses TLS to retrieve video sequences from the cloud.

NOTE: The Cloud Playback role is responsible for creating the link between the cameras and Cloud Storage, which enables the cameras to upload to the cloud. For this reason, you must first create the Cloud Playback role before activating Cloud storage.

Cloud Storage is activated after a few seconds and is ready to configure.



Transfer video archives older than [ ] days to the Cloud storage performance tier.

Note: This transfer does not delete local archives, nor change the local retention period.

Note: Archives will not be transferred to long-term storage.

Automatically delete video archives older than [ ] days from Cloud storage.

Note: Video archives will remain in performance tier for NaN days.

4 Apply your Cloud Storage policies.

5 Click the **Archivers** tab and select one or more Archiver roles that will upload video archives to the cloud.

CAUTION: After activating Cloud Storage, all video archives that meet your criteria for upload to the cloud are transferred immediately, starting with the oldest files. The selected Archiver roles will consume all available bandwidth until the uploads are complete unless a bandwidth limit is specified.

6 Click **Apply**.

Cloud Storage is ready to use.

After you finish

For Archiver roles that use Cloud Storage, we recommend setting the **Maximum length** of video files to 5 minutes and the **Maximum size** to 100 MB in the advanced settings. This will optimize bandwidth usage and ensure smooth playback of video sequences from the cloud. These settings are found in **Archiver** > **Resources** > **Advanced settings**.

Related Topics

About Cloud Storage on page 688

Applying Cloud Storage policies on page 693

Cloud Playback configuration tabs on page 1357

Archiver: Resources tab on page 1344

Applying Cloud Storage policies

To control Cloud Storage, you must apply policies that specify when files are uploaded to the cloud, and how much time those files spend in each Cloud Storage tier.

Before you begin

- Cloud Storage must be activated.
- Your user account must be a member of the Administrators group or have the *Cloud storage* privilege.

What you should know

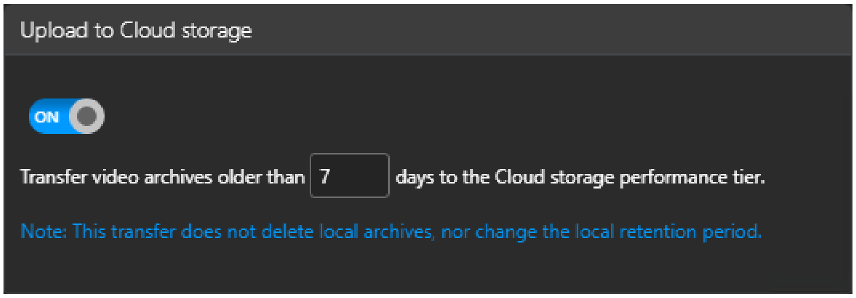
Your Cloud Storage subscription controls which policies are available to you. For example, a subscription that only includes long-term storage does not offer the **Move to long-term storage** policy because the subscription does not offer storage in the performance tier.

To apply Cloud Storage policies:

1 Open the *Video* task and click the **Cloud storage** view.

The Cloud Storage *Status* page opens.

2 Under *Upload to Cloud Storage*, switch Cloud Storage on or off, and specify when video archives are uploaded to the cloud performance tier from local storage.



Upload to Cloud storage

Transfer video archives older than 7 days to the Cloud storage performance tier.

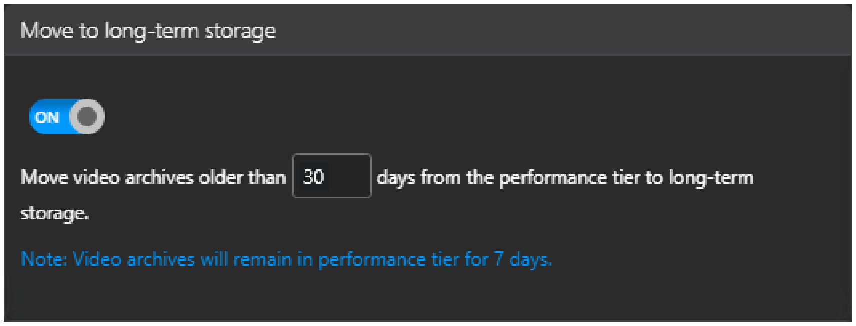
Note: This transfer does not delete local archives, nor change the local retention period.

NOTE: Your subscription controls where video archives can be uploaded. If your subscription includes performance tier storage, video archives must be uploaded to the performance tier before they can be moved to long-term storage.

Video archives must be uploaded to the cloud during the local retention period. Setting the upload policy to **0** days sends video archives to Cloud Storage as soon as possible.

Switch Cloud Storage off to stop uploading video archives. This setting has no affect on files already in the cloud. When switched off, all pending uploads will complete, and video archives in Cloud Storage are preserved in accordance with the cloud retention policy.

3 Under *Move to long-term storage*, turn long-term storage on or off, and specify when video archives are moved from the performance tier to the long-term tier.

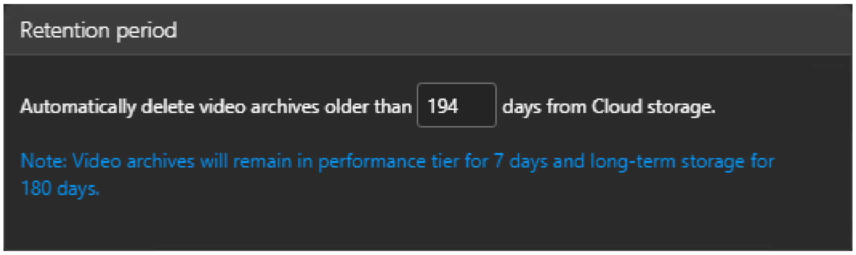


Move to long-term storage

Move video archives older than 30 days from the performance tier to long-term storage.

Note: Video archives will remain in performance tier for 7 days.

4 Under *Retention period*, specify when video archives are deleted from the cloud. This setting specifies the retention period for all video archives in the cloud.



Retention period

Automatically delete video archives older than 194 days from Cloud storage.

Note: Video archives will remain in performance tier for 7 days and long-term storage for 180 days.

IMPORTANT: Some subscriptions require a minimum file retention period. To configure a shorter retention period than the minimum specified by your subscription, contact Genetec™ Sales.

5 Click **Apply**.

Cloud Storage is ready to use.

Related Topics

About Cloud Storage on page 688

Activating Cloud Storage on page 691

Monitoring Cloud Storage

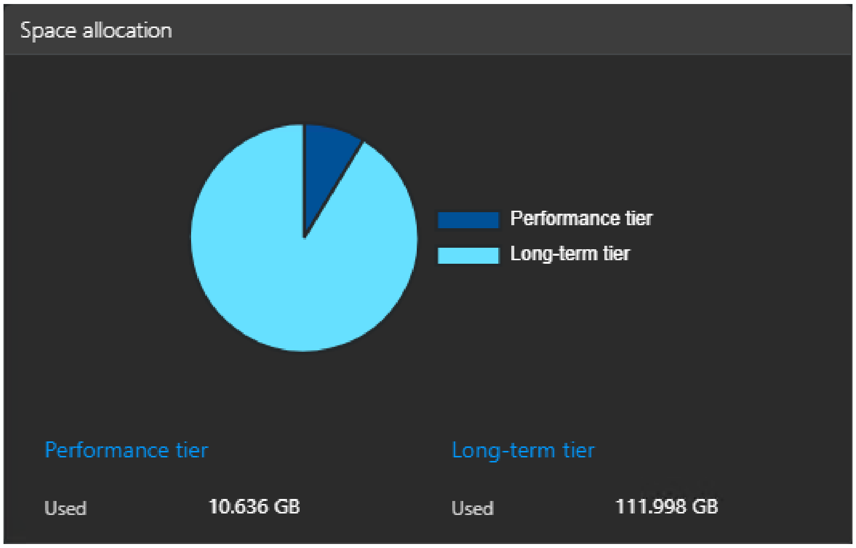
To monitor your use of Cloud Storage, you can view the current operation statistics in the *Space allocation* report.

Before you begin

- Cloud Storage must be enabled, with video archives stored in the cloud.
- Your user account must be a member of the Administrators group or have the *Cloud storage* privilege.

What you should know

The *Space allocation* report shows the storage space occupied by your video archives in the cloud performance tier and long-term tier. If your subscription only includes long-term storage, the report does not include statistics for the unused performance tier.



Performance tier

Used 10.636 GB

Long-term tier

Used 111.998 GB

The cost of your Cloud Storage subscription is partially based on the amount of storage space used in each tier.

To view Cloud Storage statistics:

1 Open the *Video* task and click the **Cloud storage** view.
The Cloud Storage *Status* page opens.

2 Under *Reports*, see the *Space allocation* report.

3 Click **Refresh** to ensure the report is up-to-date.
The Cloud Storage statistics are listed. These statistics are generated once every 24 hours.

After you finish

You can view backlog information and average upload speed for each Archiver role, by going to the *Resources* page of a participating Archiver role in Config Tool and clicking **Statistics** (●).

Related Topics

About Cloud Storage on page 688

Subscribing to Cloud Storage usage reports

To understand your use of Cloud Storage, you can subscribe to monthly data usage reports by email.

Before you begin

- Cloud Storage must be enabled.
- Your user account must be a member of the Administrators group or have the *Cloud storage* privilege.

What you should know

The *Cloud Storage data usage* report summarizes the cloud storage used by your system. It provides daily statistics for each access tier, and monthly averages to help you manage data consumption and control costs.

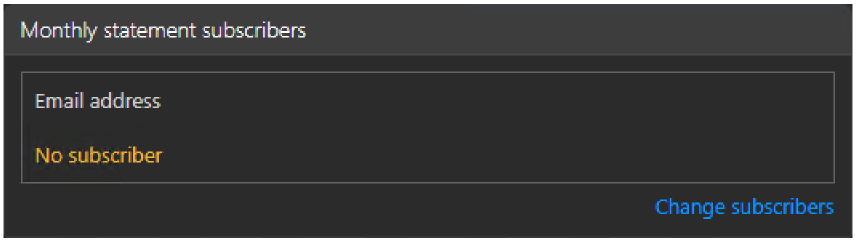
The cost of your Cloud Storage subscription is partially based on the amount of storage space used in each tier.

To subscribe to the *Cloud Storage data usage* report, or to subscribe others:

1 Open the *Video* task and click the **Cloud storage** view.

The Cloud Storage *Status* page opens.

2 Under *Monthly statement subscribers*, click **Change subscribers**.



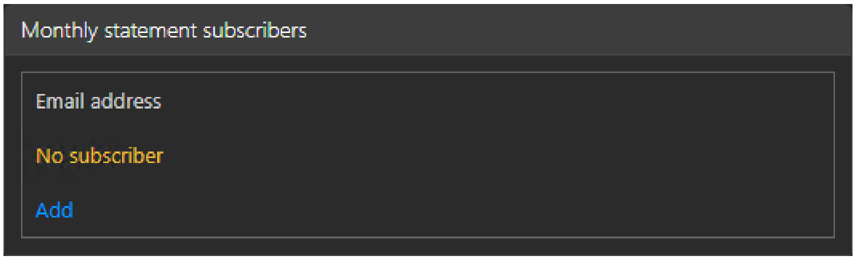
Monthly statement subscribers

Email address

No subscriber

The *Monthly statement subscribers* list opens.

3 Click **Add**.



Monthly statement subscribers

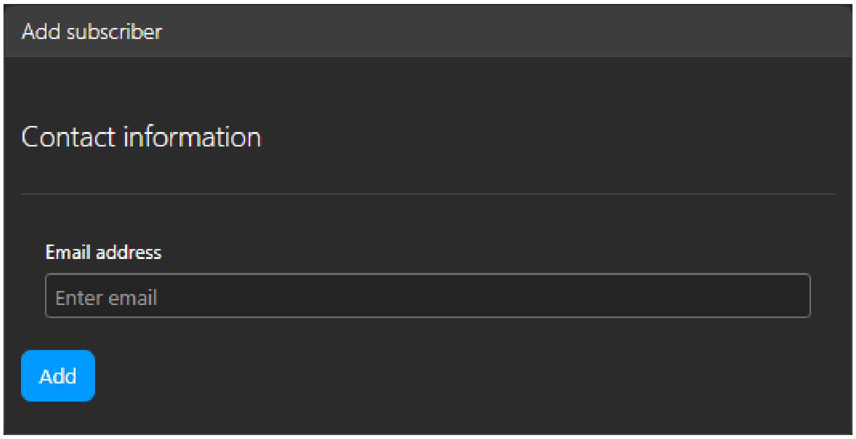
Email address

No subscriber

NOTE: The *Monthly statement subscribers* list supports a maximum of 10 email addresses or public distribution lists.

The *Add subscriber* window opens.

4 Enter a valid email address or public distribution list into the **Email address** field.



5 Click **Add**.

6 Click **Back to status page**.

After you finish

If required, you can unsubscribe recipients by entering the *Monthly statement subscribers* list and clicking **Unsubscribe** next to the corresponding email addresses.

31

Troubleshooting and maintenance for video

This section includes the following topics:

Troubleshooting body-worn cameras

If you are experiencing problems with body-worn camera (BWC) devices in Security Center, learn about the symptoms, potential causes, and solutions to help you troubleshoot the issue.

Symptoms

Here are some common issues you might experience with body-worn cameras in Security Center. To help you solve the issue, click the error message or symptom that you are currently experiencing.

- Archiver cannot have failover when using wearable cameras
- Archives report for body-worn camera is empty on page 699
- Error converting resource on server
- One or more camera station configuration files are obsolete and must be regenerated
- Port already in use

Archives report for body-worn camera is empty

The *Archives* report in Security Desk is empty. This occurs when the download or upload process times out.

Cause

This issue can be caused by one or several of the following:

- Download processing issues when copying from camera to download folder location.
- G64 file conversion processing issues.
- G64 file conversions in progress.
- Upload processing to Security Center archive times out.

Solution

1. In the Genetec Clearance™ Uploader event logs, check that the files were downloaded.
2. In Security Desk check that the downloaded files are in the archives folder.

   For example, *C:\VideoArchives\Archiver\0000166\2018-02-26*.
3. If you see *.G64* mentioned in the archives folder file path, wait a few minutes.

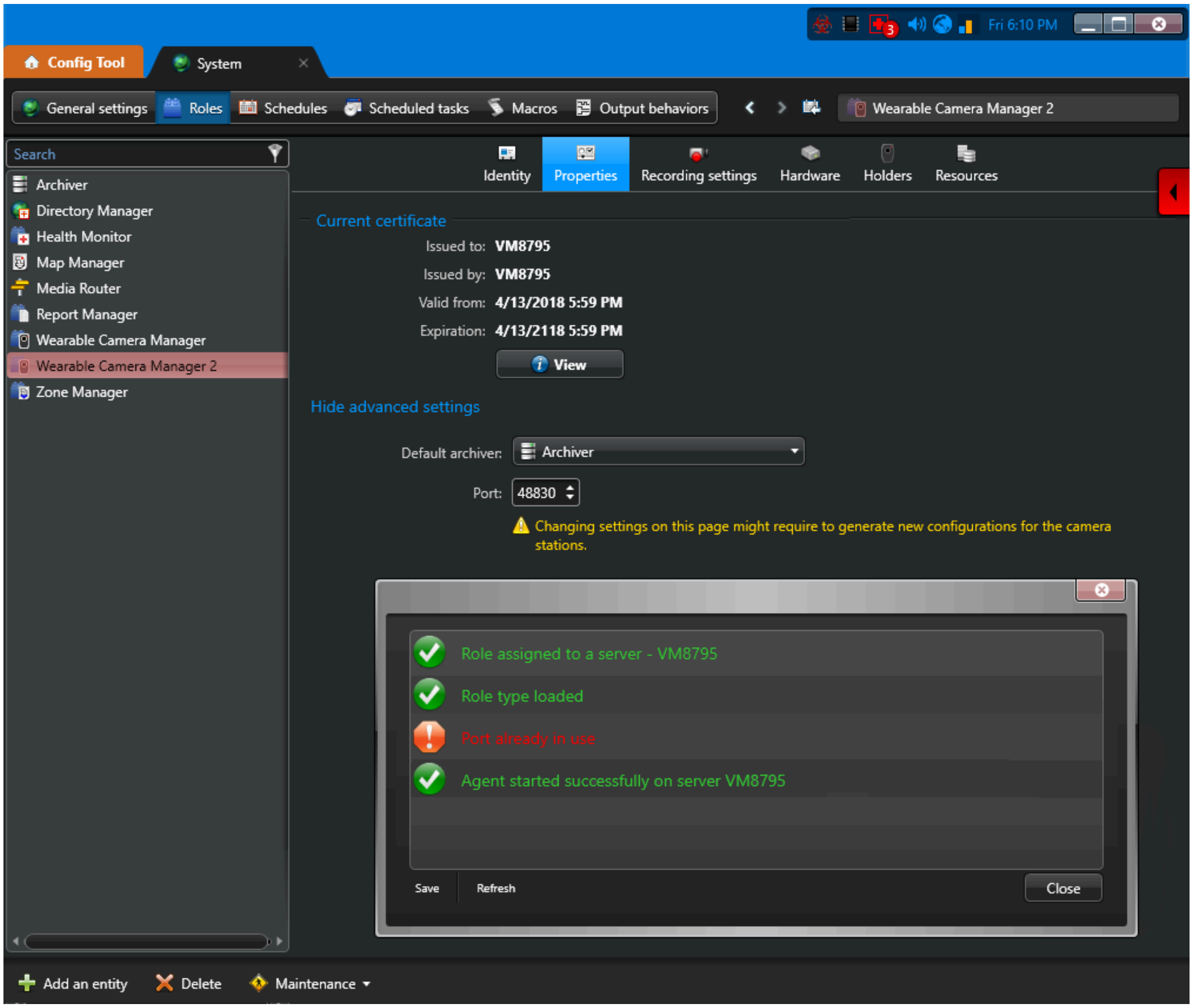
   The role needs time to convert the files so that the Archiver can read them.
4. If the Archiver is still empty or unresponsive, do the following:
   a. In Config Tool, deactivate and activate the Wearable Camera Manager role.
   b. In Config Tool, deactivate and activate the Archiver role.
5. In Security Desk generate the Archives report again.

Body-worn camera port is already in use

The Wearable Camera Manager role is currently offline because the port is already in use. To resolve this issue, change the port specified in the Wearable Camera Manager role.

Cause

The Wearable Camera Manager role cannot open a connection on the specified port because the port is already in use.



Current certificate

Issued to: VM8795

Issued by: VM8795

Valid from: 4/13/2018 5:59 PM

Expiration: 4/13/2118 5:59 PM

Hide advanced settings

Default archiver: Archiver

Port: 48830

Changing settings on this page might require to generate new configurations for the camera stations.

Role assigned to a server - VM8795

Role type loaded

Port already in use

Agent started successfully on server VM8795

Solution

1. In Config Tool, open the *System* task and select the Wearable Camera Manager role.
2. Change the specified port in the Wearable Camera Manager role **Properties** tab.

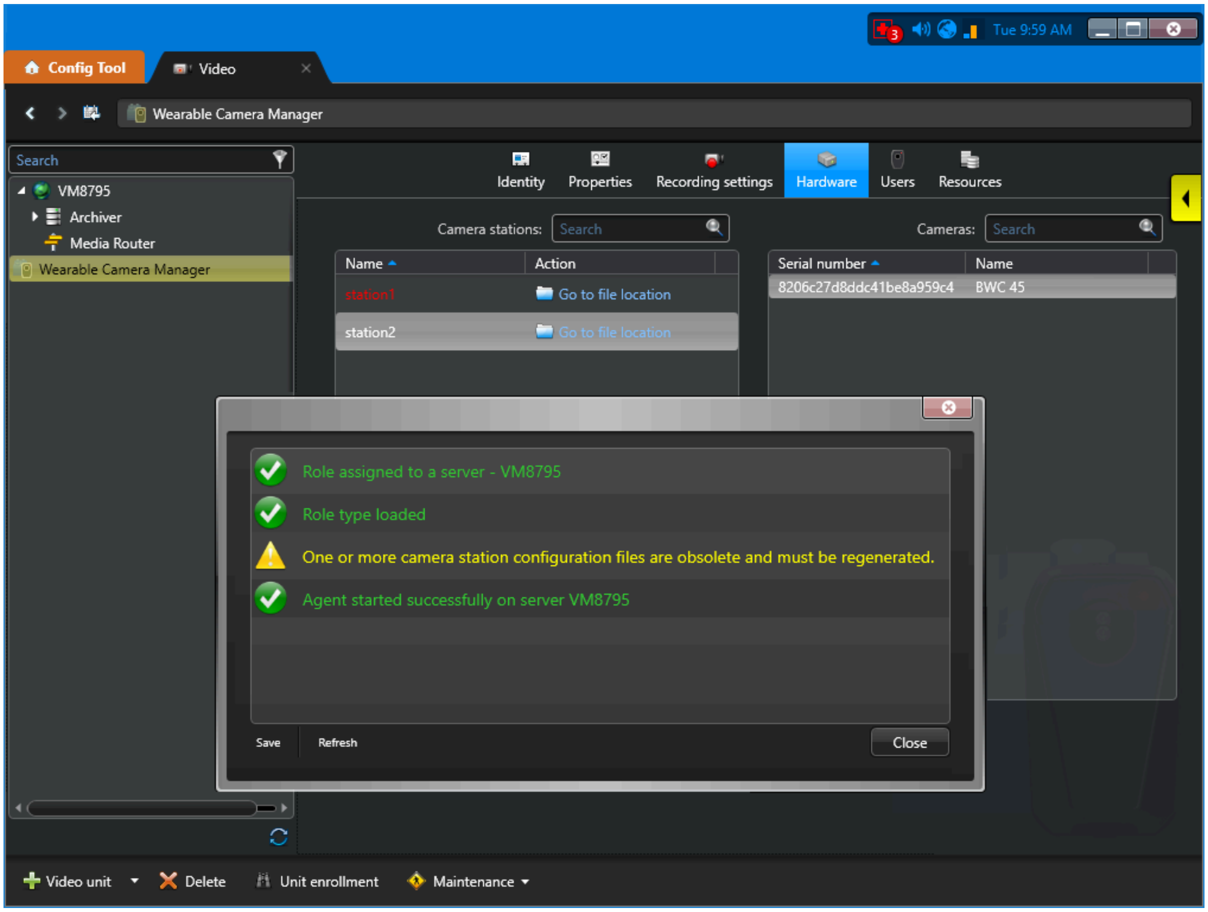
   IMPORTANT: You must generate new configuration files for your camera stations after changing these settings. See Configuration file errors for body-worn cameras on page 701.

Configuration file errors for body-worn cameras

If you receive a One or more camera station configuration files are obsolete and must be regenerated for the Wearable Camera Manager role, one or more configuration files for body-worn camera stations contain errors.

Cause

One or more camera station configuration files are obsolete and must be regenerated.



Name	Action
station1	Go to file location
station2	Go to file location

Serial number	Name
8206c27d8ddc41be8a959c4	BWC 45

Role assigned to a server - VM8795

Role type loaded

One or more camera station configuration files are obsolete and must be regenerated.

Agent started successfully on server VM8795

The obsolete camera station configuration file is highlighted in red.

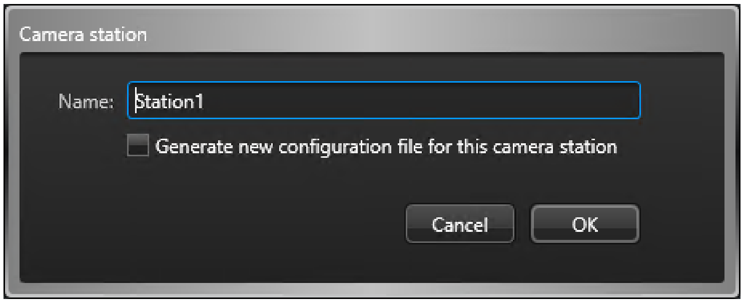
Solution 1

Regenerate one camera station configuration file.

NOTE: Regenerating one file is typically used when the file is obsolete or when you suspect the file has been compromised. Regenerating the configuration file renders all previous instances of the file unusable.

1. From the Config Tool home page, open the *Video* task, select the Wearable Camera Manager role, and click the **Hardware** tab.

2. In the *Camera stations* section, select a camera station and click **Edit the item** (✎).

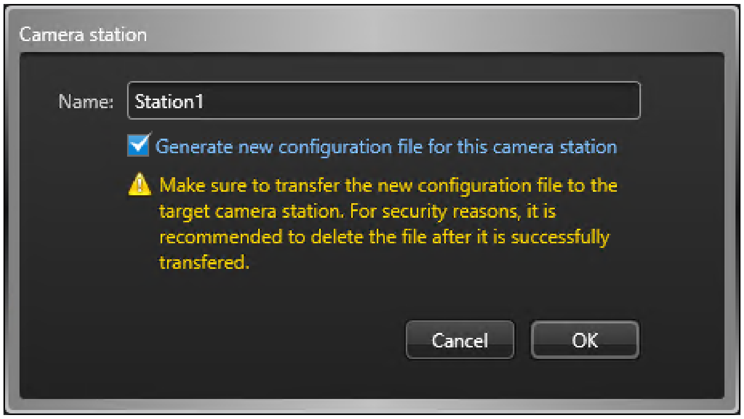


Camera station

Name: Station1

□ Generate new configuration file for this camera station

3. Select **Generate new configuration file for this camera station** and click **OK**.



Camera station

Name: Station1

☑ Generate new configuration file for this camera station

⚠ Make sure to transfer the new configuration file to the target camera station. For security reasons, it is recommended to delete the file after it is successfully transfered.

4. Transfer the new *.json* configuration file to the camera station or the Genetec Clearance™ Uploader.

   IMPORTANT: For security reasons, ensure that the original configuration file is deleted from its original location after it is successfully transferred. For example, *C:\Users\username\AppData\Local\Temp\Genetec*.

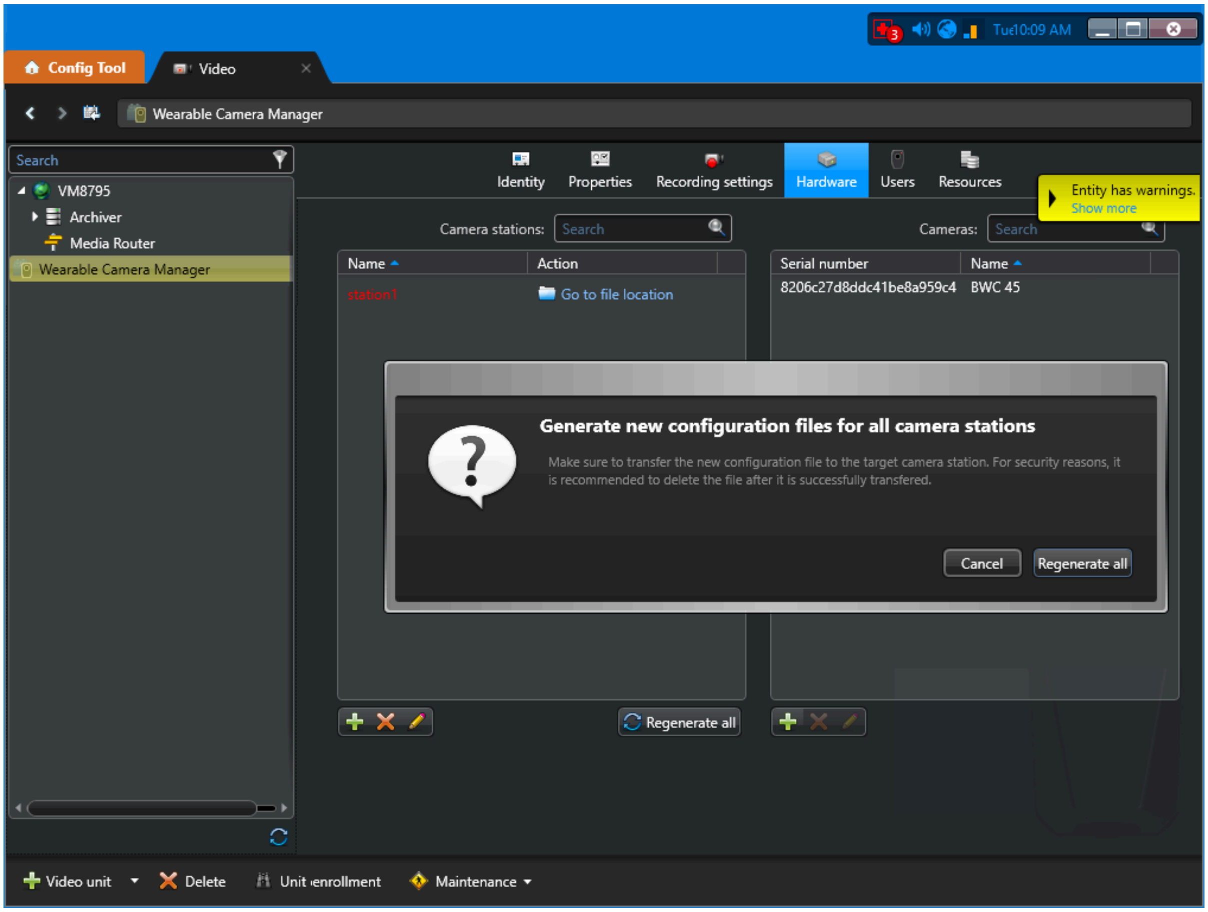
Solution 2

Regenerate all camera station configuration files.

NOTE: Regenerate all is typically used to when the IP address, port, or certificate of the Wearable Camera Manager role has changed. This ensures that all camera stations are able to communicate with the role.

1. From the Config Tool home page, open the *Video* task, select the Wearable Camera Manager role, and click the **Hardware** tab.
2. In the *Camera stations* section, click **Regenerate all** (⟳).

3. In the confirmation dialog box that opens, click **Regenerate all**.



Generate new configuration files for all camera stations

Make sure to transfer the new configuration file to the target camera station. For security reasons, it is recommended to delete the file after it is successfully transfered.

4. Transfer all new *.json* configuration files to the relevant camera stations or the Genetec Clearance™ Uploader.

   IMPORTANT: For security reasons, ensure that the original configuration file is deleted from its original location after it is successfully transferred. For example, *C:\Users\username\AppData\Local\Temp\Genetec*.

Related Topics

Configuring body-worn cameras on page 649

Adding cameras and officers to the Wearable Camera Manager role on page 651

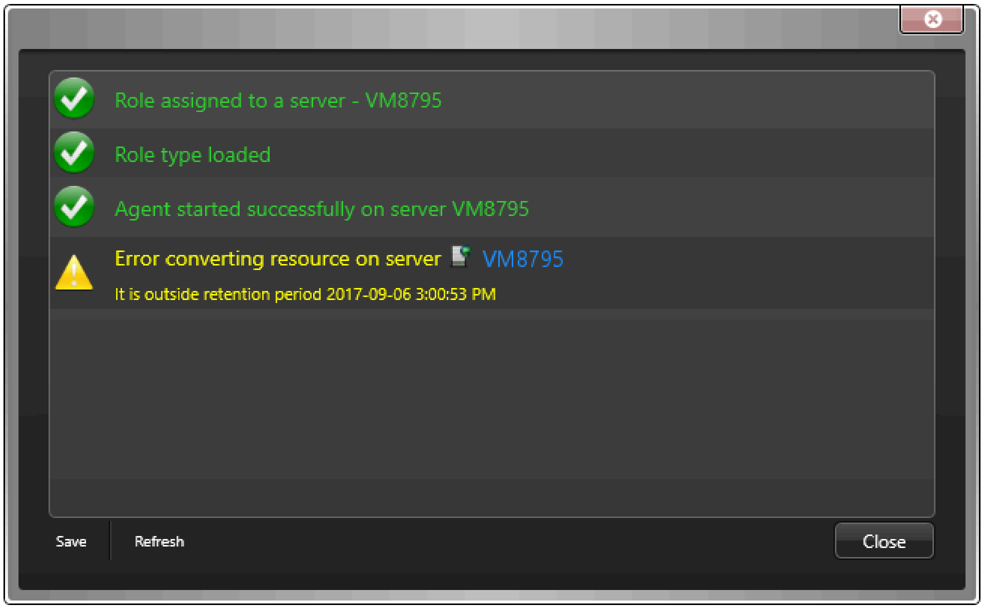
Conversion warnings for body-worn cameras

Conversion warnings are displayed when evidence files cannot be imported or downloaded.

NOTE: All of these conversion warnings disappear after 2 minutes.

Outside retention period

Cause: The wearable camera user, the Archiver role, or the Wearable Camera Manager role are set to only keep files within a specified retention period, but the Genetec Clearance™ Uploader attempted to import a file outside that period.



✓ Role assigned to a server - VM8795

✓ Role type loaded

✓ Agent started successfully on server VM8795

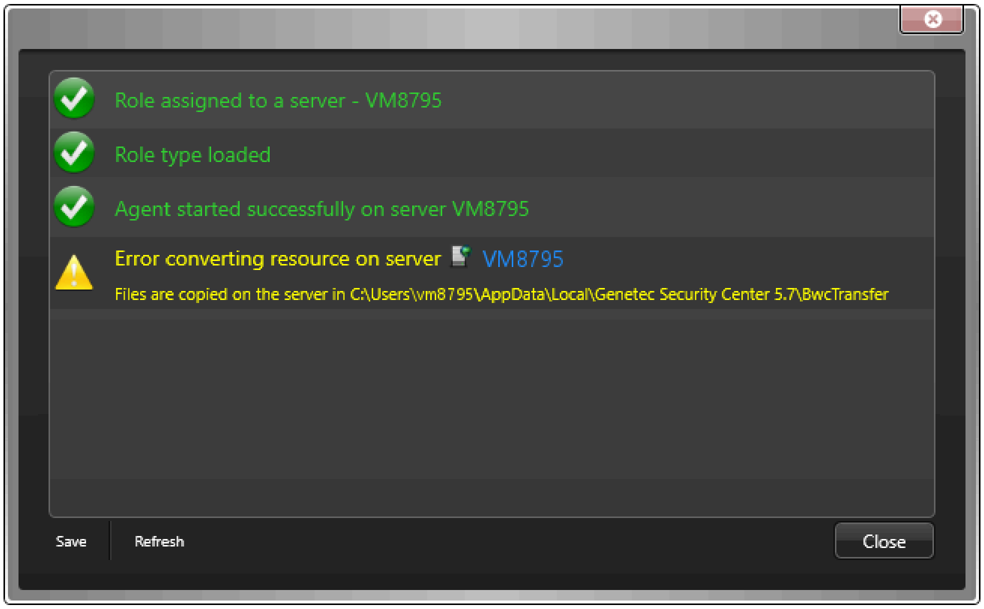
Error converting resource on server VM8795

It is outside retention period 2017-09-06 3:00:53 PM

Solution: To import older files, the retention period must be extended or the **Automatic cleanup** option must be turned off. This can be done in Config Tool, from the Archiver's *Camera default settings* page, the Wearable Camera Manager's *Recording settings* page, or the wearable camera user's *Recording* page.

Error converting resources

Cause: The downloaded file could not be converted because its format is not supported. The downloaded file was copied to the server location specified in the warning message.



✓ Role assigned to a server - VM8795

✓ Role type loaded

✓ Agent started successfully on server VM8795

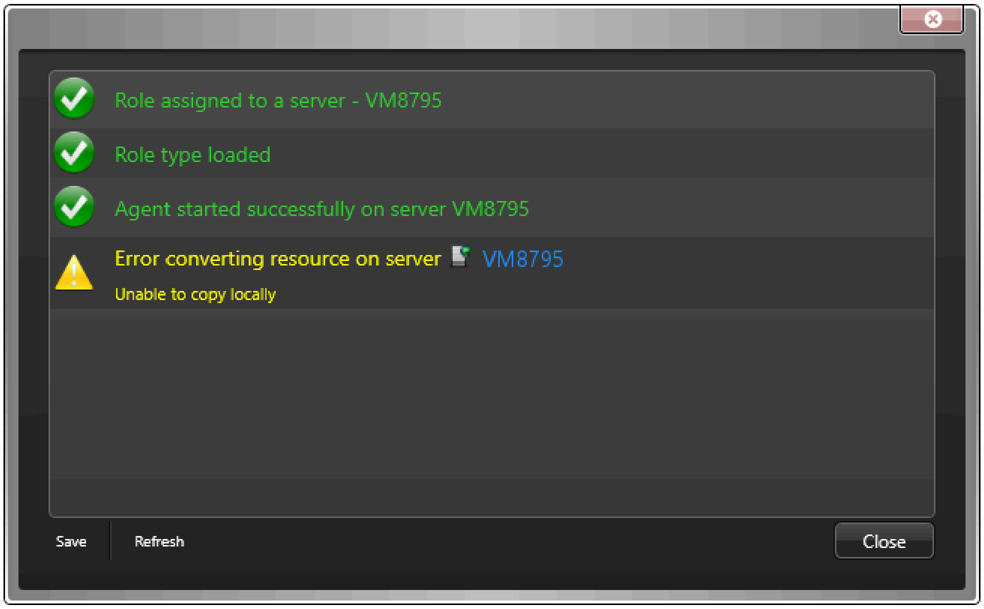
Error converting resource on server VM8795

Files are copied on the server in C:\Users\vm8795\AppData\Local\Genetec Security Center 5.7\BwcTransfer

Solution: Access the files manually at the location specified in the warning message.

Unable to copy locally

Cause: There was a conversion error and the downloaded file could not be copied to the server location specified in the warning message.


✓ Role assigned to a server - VM8795

✓ Role type loaded

✓ Agent started successfully on server VM8795

⚠ Error converting resource on server VM8795
Unable to copy locally

Solution: Check the local disk to ensure that you have enough storage space.

NOTE: A manual intervention is required to recover the file and you must contact Genetec™ Technical Assistance Center.

Failover cannot be configured on Archiver role for body-worn cameras

When failover is configured on the Archiver role that is used by a Wearable Camera Manager role, you receive an Archiver cannot have failover when using wearable cameras warning message.

Cause

Failover and redundant archiving are not supported on Archiver roles used for wearable (or body-worn) cameras.

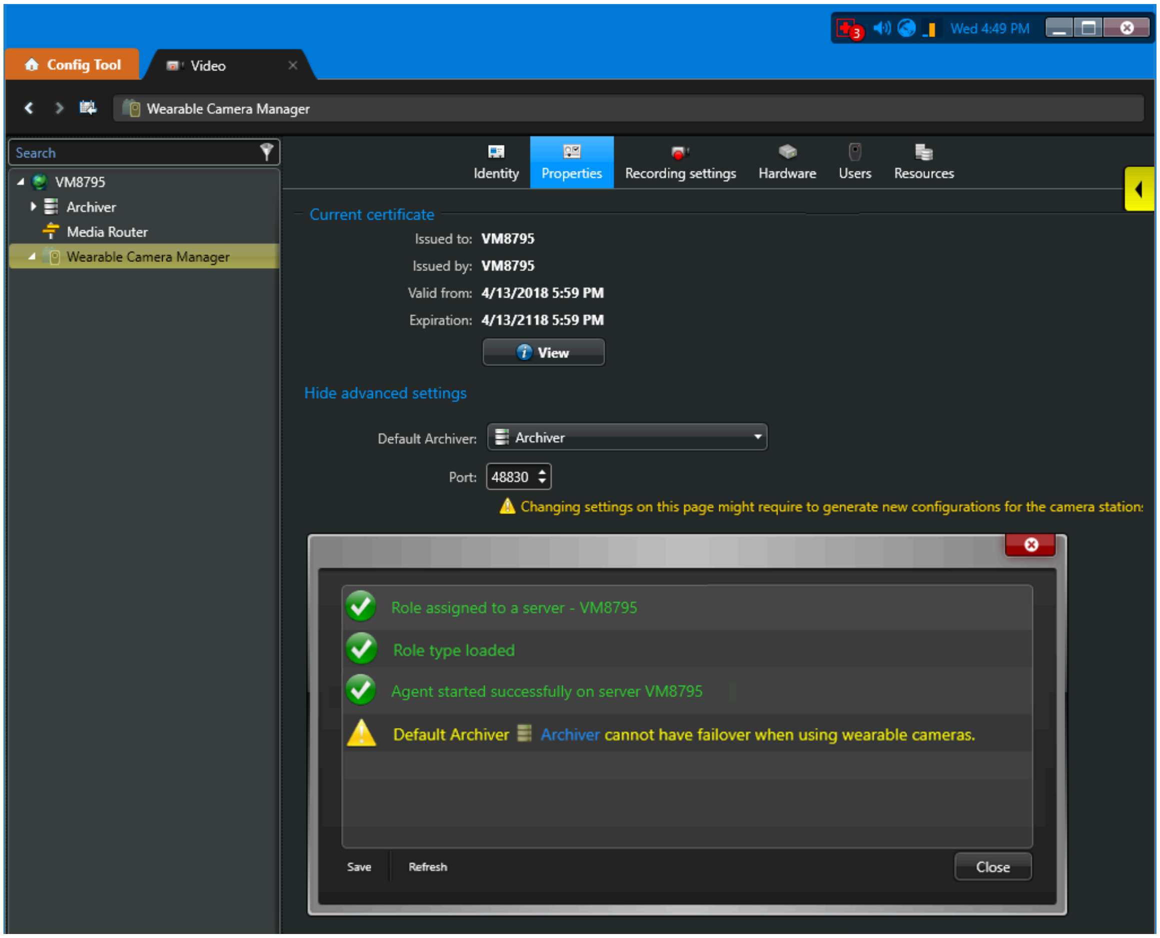
Solution 1

Change the default Archiver role assigned to the Wearable Camera Manager to one that does not have failover configured.

BEST PRACTICE: We recommend using a dedicated Archiver for wearable cameras.

1. In the Config Tool home page, open the *Video* task and select the Wearable Camera Manager role.

2. Click the **Properties** tab and click **Show advanced settings**.



Current certificate

Issued to: VM8795

Issued by: VM8795

Valid from: 4/13/2018 5:59 PM

Expiration: 4/13/2118 5:59 PM

Default Archiver: Archiver

Port: 48830

Changing settings on this page might require to generate new configurations for the camera station:

Role assigned to a server - VM8795

Role type loaded

Agent started successfully on server VM8795

Default Archiver Archiver cannot have failover when using wearable cameras.

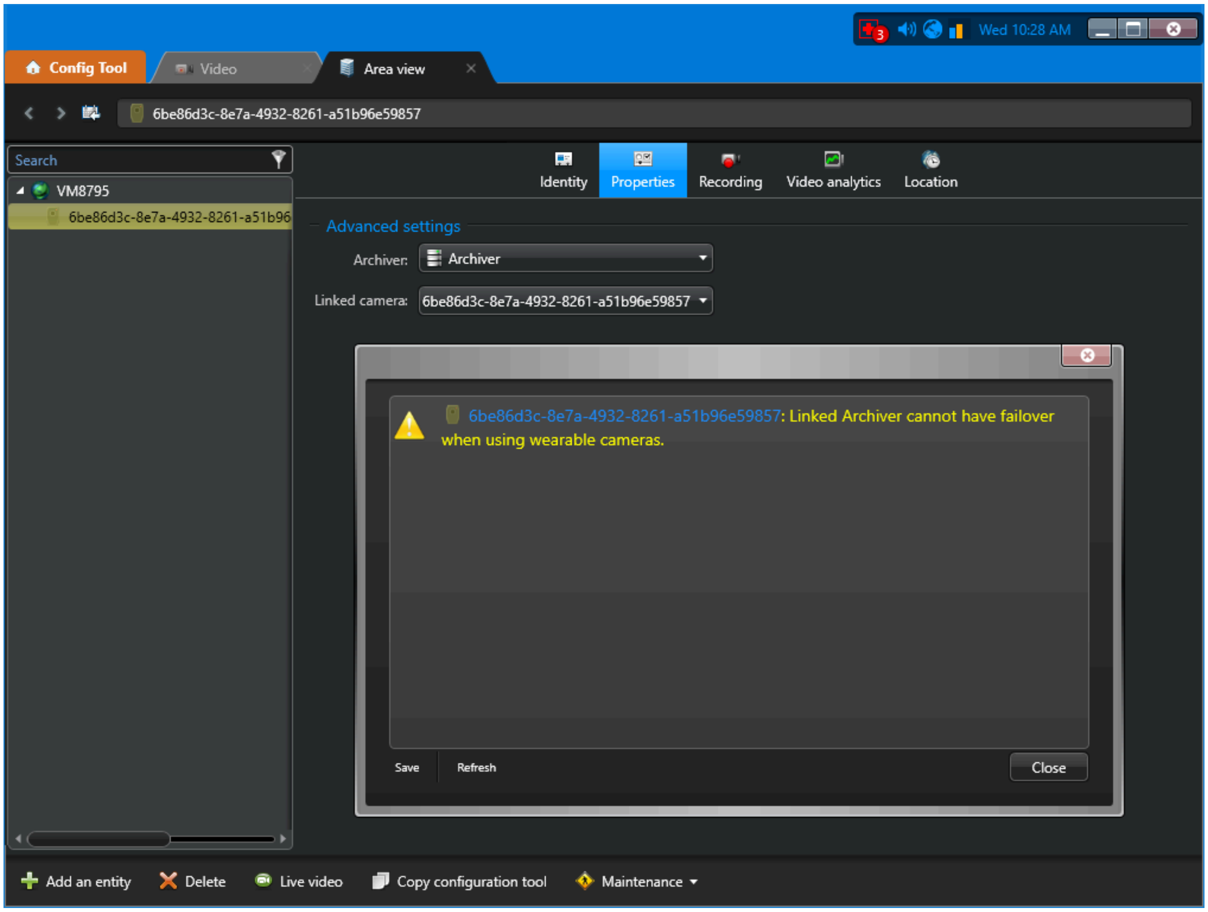
3. From the **Default archiver** list, select an Archiver that does not have failover configured.
4. Select or enter the port that you require.
5. Click **Apply**.

   IMPORTANT: You must generate new configuration files for your camera stations after changing these settings. See Configuration file errors for body-worn cameras on page 701.

Solution 2

Assign a different Archiver to the wearable camera user in the *Area view* task.

1. In Config Tool, open the *Area view* task.



Archiver: Archiver

Linked camera: 6be86d3c-8e7a-4932-8261-a51b96e59857

6be86d3c-8e7a-4932-8261-a51b96e59857: Linked Archiver cannot have failover when using wearable cameras.

2. Select a wearable camera user ( ) and click the **Properties** tab.
3. Under *Advanced settings*, select the **Archiver** and the **Linked camera** from their respective drop-down lists.
4. Click **Apply**.

Body-worn camera evidence is stuck

The evidence from a body-worn camera is stuck and not fully uploaded or converted.

Evidence is stuck in system controller

Cause: Upload process on an Axis station times out.

Solution:

1. If the display of evidence on the system controller does not change after 30 minutes or the status is yellow, reboot the Axis station.
2. If the evidence remains stuck, contact Genetec™ Technical Assistance Center (GTAC).

Evidence is stuck during conversion

Cause: Conversion processing issues.

Solution: If the evidence was converting from mp4 to g64 on the Archiver and the Wearable Camera Manager role server stopped working, contact Genetec Technical Assistance Center (GTAC).

Troubleshooting live video issues

If you are experiencing problems with your live video in Security Center, learn about the symptoms, potential causes, and solutions to help you troubleshoot the issue.

Symptoms

Here are some common issues you might experience with live video in Security Center. To help you solve the issue, click the error message or symptom that you are currently experiencing.

- Cameras stop working with default security options
- Cannot control PTZ cameras while Security Desk is offline
- Cannot watch live video
- H.264 video stream issues
- Image pixelation or poor image quality of cameras
- Impossible to establish video session with the server error on page 714
- Live video takes too much time to load
- Motion detection not working
- Not enough bandwidth error
- Video decoding performance issues
- Video degradation
- Video stream issues

Cameras stop working after installing Security Center with the default security options

After installing Security Center using default security settings, cameras that do not support digest access authentication might not work. To fix this issue, you can reactivate basic access authentication by video unit or by manufacturer.

What you should know

Digest access authentication is the authentication scheme that the majority of recent video unit models support. This authentication scheme is more secure than basic access authentication because the passwords are hashed before sending them over the network. For this reason, basic access authentication is disabled by default. After installation, if you realize that some of your cameras do not support digest access authentication, you can revert them to basic access authentication in Config Tool.

For added security, Security Center remembers whether or not a specific video unit supports the digest authentication scheme. After the system has successfully authenticated to a video unit using the digest scheme, you cannot revert to the less secure basic scheme. You can see the authentication scheme used for each camera in the *Hardware inventory* report.

To revert to the basic authentication scheme on a specific video unit:

1. From Config Tool, open the *Hardware inventory* task.
2. Run the report on the video units that are inactive (in red) in your system.

   You might need to scroll horizontally to the right to see the **Authentication scheme** column.
3. In the report pane, select the video units that are inactive and click **Reset authentication scheme**.

   The **Authentication scheme** changes to **Anonymous**. After the Archiver successfully connects to the video unit, the exact authentication scheme is displayed.

To revert to the basic authentication scheme for a specific manufacturer:

1 From Config Tool, open the *Video* task.
2 Select the Archiver role that controls your cameras and click **Extensions**.
3 Select the manufacturer that you want and set **Refuse basic authentication** to **OFF**.
4 Click **Apply**.

Related Topics

Viewing unit properties on page 229

Cannot watch live video in Security Desk

If you cannot view live video in Security Desk, you can troubleshoot the issue.

What you should know

There are several possible causes for a missing video error:

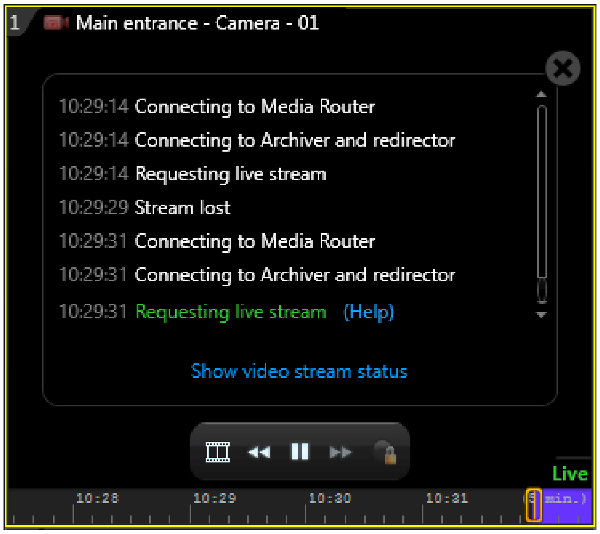
- The network is slow.
- Port connection has issues.
- The video stream was dropped while being redirected to Security Desk.

To troubleshoot why you cannot view live video:

1 Wait to see if the camera connects.

2 If the problem persists for more than 10 seconds, click **Show diagnosis** in the tile, or press `Ctrl+Shift+D`.

Information about the video stream is displayed. The current step is highlighted:



```
10:29:14 Connecting to Media Router
10:29:14 Connecting to Archiver and redirector
10:29:14 Requesting live stream
10:29:29 Stream lost
10:29:31 Connecting to Media Router
10:29:31 Connecting to Archiver and redirector
10:29:31 Requesting live stream   (Help)
```

- **Initializing:** The media player is preparing the required resources to display the video stream.
- **Connecting to Media Router:** The media player is establishing connection with the Media Router to obtain the network location of the stream.
- **Connecting to Archiver and redirector:** The media player is establishing connection with the Archiver and the redirector to request video.
- **Requesting live stream:** The connection is established between the Archiver and the Media Player. The Media Player is now requesting the live stream.
- **Analyzing the stream:** The client workstation requested and received the stream. The media player analyzes the stream to detect the video format and the presence of key frames. After the stream is validated, the video is decoded.

TIP: Click the **Help** link for a list of things that you can do to troubleshoot the issue.

3 Confirm that the unit is online.

If the unit is red in the *Video* task in Config Tool, then troubleshoot why the video unit is offline.

4 Verify that you can ping the unit:

a) In the Config Tool *Video* task, select the red video unit.

b) At the bottom of the *Video* task, click **Unit** > **Ping** ().

If there is no reply, the unit is offline (broken, unplugged, and so on), or there is a problem with your network.

5 Make sure you can connect to the unit, and then click **Unit** > **Unit's web page**.

TIP: You can also determine if you have the correct credentials for the unit.

6 Verify that Security Center supports the unit, and that the unit is running the certified firmware.

For a list of video units supported by Security Center, see our Supported Device List.

7 Change the video unit's connection type to the Archiver:

a) In the Config Tool *Video* task, select the red camera.

b) Click the **Video** tab.

c) From the **Connection type** list in the *Network settings* section, select a different connection type.

d) Click **Apply**.

8 Try viewing playback video from the camera:
   a) In the Security Desk *Archives* task, select the camera.
   b) Select the most recent video archive available and click **Generate report**.
   c) After the report is generated, try to view the video from the archive.
      - If you can view the video, continue with the next troubleshooting step.
      - If you cannot view any video, contact Genetec™ Technical Assistance Center.

9 If you have an expansion server on your system running the Archiver role, try to view video from the expansion server:
   a) Open Security Desk on the expansion server.
   b) In the *Monitoring* task, drag the camera from the area view to a tile in the canvas.
      - If you can view video, it might be a problem with the redirection from the Media Router to your Security Desk. Continue with the next troubleshooting step.
      - If you cannot view any video, contact Genetec Technical Assistance Center.

10 Make sure the correct ports are open on your network so that there is no firewall blocking the video stream. For more information, see the topic *Default ports used by Security Center* in the *Security Center Adminstrator Guide*.

11 Verify that each network on your system is configured properly:
   a) From the Config Tool home page, open the *Network view* task.
   b) Select a network, click the **Properties** tab, and make sure all the settings are correct (IP prefix, subnet mask, routes, network capabilities, and so on).
   c) If required, change the network settings and click **Apply**.

   For more information about configuring network settings, see the *Security Center Administrator Guide*.

12 Force Security Desk to use a different connection type:
   a) From the Security Desk home page, click **Options** > **General**.
   b) In the *Network options* section, next to the **Network** option, select **Specific**.
   c) From the drop-down list, select a different network and click **Save**.
   d) Restart Security Desk.
   e) If changing the network connection does not work, repeat the steps to test using other networks.

13 If you still cannot view video, click **Show video stream status** in the tile, and then troubleshoot the video stream.

14 If the issue persists, contact Genetec Technical Assistance Center.

Configuring Security Center to open live video quickly

You can minimize the time it takes for a camera to open and display live video in the Security Desk *Monitoring* task by adjusting settings in Config Tool and Security Desk.

What you should know

Several factors affect the time that it takes to display live video from a camera in Security Desk:

- Video compression format: MJPEG video streams usually display quicker than H.264 video streams.
- Image quality: a camera usually displays live video quicker with video image quality of 70% than with video image quality of 100% or below 60%.
- Key frame interval: setting a low **Key frame interval** for the camera in Config Tool might produce better results.

To configure a camera to display live video faster:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Select the camera to configure and click the **Video** tab.

3 In the *Stream usage* section, turn on **Live** and **Recording** for the selected stream.

4 In the *Network settings* section, select **Multicast** as the **Connection type**.

5 Click **Apply**.

6 Click the **Recording** tab and select **Continuous** from the **Recording modes** drop-down list.

7 Click **Apply**.

8 From the Security Desk home page, click **Options** > **Video**.

9 Scroll down to the *Video cache* section and turn off **Live video caching**.

10 Under *Advanced settings*, set the **Jitter buffer delay** to 0 ms.

11 Restart Security Desk.

Determining whether the workstation or the network is causing video degradation

If the video you are monitoring is jittery or is dropping frames, use the rendering rate video statistic to determine whether the workstation is the cause.

What you should know

Rendering rate is the comparison of how fast the workstation renders a video with the speed the workstation receives that video from the network. The rendering rate video statistic is made up of:

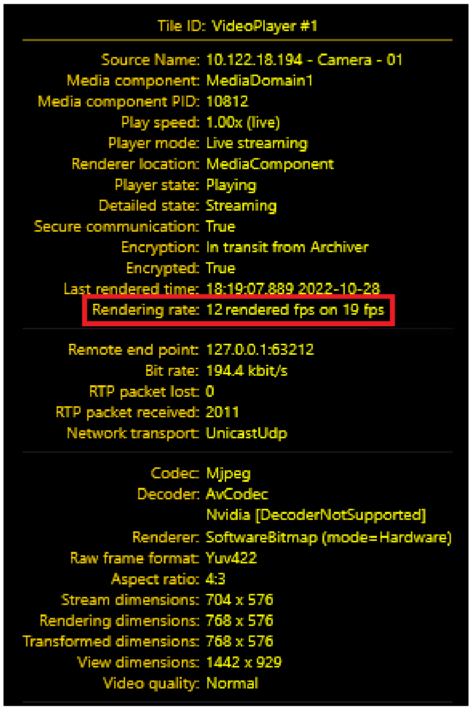
- The speed at which the workstation processes video. This indicates how much load is on the workstation's CPU and memory.
- The speed at which the network is sending video to the workstation.

To view the rendering rate of a video:

1 Select the tile that is playing video.

2 Press Ctrl+Shift+A.

Video stream statistics are displayed in the tile.



```
                      Tile ID: VideoPlayer #1

             Source Name: 10.122.18.194 - Camera - 01
         Media component: MediaDomain1
     Media component PID: 10812
              Play speed: 1.00x (live)
             Player mode: Live streaming
       Renderer location: MediaComponent
            Player state: Playing
          Detailed state: Streaming
    Secure communication: True
              Encryption: In transit from Archiver
               Encrypted: True
      Last rendered time: 18:19:07.889 2022-10-28
          Rendering rate: 12 rendered fps on 19 fps

        Remote end point: 127.0.0.1:63212
                Bit rate: 194.4 kbit/s
         RTP packet lost: 0
     RTP packet received: 2011
       Network transport: UnicastUdp

                   Codec: Mjpeg
                 Decoder: AvCodec
                          Nvidia [DecoderNotSupported]
                Renderer: SoftwareBitmap (mode=Hardware)
        Raw frame format: Yuv422
            Aspect ratio: 4:3
       Stream dimensions: 704 x 576
    Rendering dimensions: 768 x 576
  Transformed dimensions: 768 x 576
         View dimensions: 1442 x 929
           Video quality: Normal
```

Example

If your rendering rate is "12 rendered fps on 19 fps", your workstation is processing 12 fps. However, it is receiving video at 19 fps. The workstation cannot process all the frames it is receiving. Your workstation is the cause of the degraded quality of the video that you are monitoring. In this case, lighten the load and check the hardware and its drivers.

- Reduce the number of cameras that you are monitoring to reduce the load on the workstation.
- Check the hardware requirements to make sure that the workstation can handle the load.
- Check that the graphic card is up to date.
- Check that the network card is up to date.
- Ensure that all drivers are up to date.

If your rendering rate is "12 rendered fps on 12 fps", your workstation is processing every frame that it is receiving from the network. In this case, compare the second value to the camera's configured fps rate. This determines if the network is sending all the frames it is receiving from the camera. If there is a difference in these two rates, either the camera or the network is the cause of the video degradation.

- Check the camera's firmware.
- Check the health of the network.

Enabling offline PTZ mode on a Security Desk workstation

To allow operators to control PTZ cameras while Security Desk is offline (not connected to the Directory), you can enable the offline PTZ mode.

To enable the offline PTZ mode on a workstation:

1. On the computer where you are running Security Desk, open the file *App.SecurityDesk.config* found in the *ConfigurationFiles* folder under the Security Center installation Directory role (default=*C:\Program Files (x86)\Genetec Security Center 5.11* on a 64-bit machine).
2. Add the following child element to the <configuration/> element.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
   ...
   <Ptz DisableThrottling="False" ThrottlingDelay="75" AllowOfflineMode="True"/>
   ...
</configuration>
```

   If the <Ptz/> child element already exists, only add the AllowOfflineMode attribute.

   NOTE: The syntax is case-sensitive.
3. Save your changes and restart Security Desk.

Impossible to establish video session with the server error

If you receive an Error: Impossible to establish video session with the server message, there might be a problem with the server, the Media Router role, the Federation™ role, the Archiver role, or the video unit. To troubleshoot the issue, learn about the possible causes and their respective solutions.

To diagnose an Impossible to establish video session with the server error:

1. Make sure that your server is running.
2. Make sure the Archiver role is online:
   a) In the Config Tool *Video* task, select the Archiver role.
   b) At the bottom of the *Video* task, click **Maintenance** > **Diagnose** (✚).
   c) Fix any issues that are found.

3 If you are trying to view a federated camera, confirm that the *Security Center Federation™* role or the *Omnicast™ Federation™* role is online:If you are trying to view a federated camera, confirm that the Security Center Federation™ role or the Omnicast™ Federation™ role is online:
   a) In the Config Tool *System* task, click the **roles** view.
   b) Select the Federation™ role and click **Maintenance** > **Diagnose** (✚).
   c) Fix any issues that are found.

4 If you are trying to view a federated camera, confirm that the server for the federated Security Center system is online.

5 It might be a Media Router connection problem. Make sure that the Media Router role is online:
   a) In the Config Tool *System* task, click the **Roles** view.
   b) Select the Media Router role and click **Maintenance** > **Diagnose** (✚).
   c) Fix any issues that are found.

6 Restart the Media Router role:
   a) In the Config Tool *System* task, click the **Roles** view.
   b) Select the Media Router role and click **Maintenance** > **Deactivate role** (🚦).
   c) In the confirmation dialog box that opens, click **Continue**.
      The Media Router turns red.
   d) At the bottom of the *System* task, click **Maintenance** > **Activate role** (🚦).

7 Make sure the unit is online.
   If the unit is red in the *Roles and units* view, then troubleshoot why the video unit is offline.

Motion detection is not working in Security Center

If motion detection is not working for some cameras in Security Center, you can troubleshoot the issue.

What you should know

This information used to be found in the deprecated knowledge base article KBA-00965.

To troubleshoot motion detection in Security Center:

1 Verify that Security Center supports the unit, and that the unit is running the certified firmware.
   For a list of video units supported by Security Center, see our Supported Device List.

2 Confirm that there are no known issues or limitations related to motion detection for your camera in the *Security Center Release Notes*.

3 Confirm that the motion detection settings are configured properly for the camera. For more information, see the topic *Configuring motion detection* in the *Security Center Adminstrator Guide*.

4 Verify that you are receiving motion events in Security Desk:
   a) From the Security Desk home page, click **Options** > **Events**.
   b) Verify that the *Motion on* and *Motion off* events are selected, and click **Save**.
   c) Open the *Monitoring* task.
   d) At the bottom of the *Monitoring* task, click **Monitoring** (🔭) and click **Add** (✚).
   e) In the *Select an entity to monitor* dialog box, select a camera and click **Add**.
      The entities you selected are added to the **Event monitoring** list.
   f) Create some motion near the camera to confirm that motion events show up in the event list of the *Monitoring* task.

5 If you do not receive any motion events, lower the **Motion on threshold** value in the camera's **Motion detection** tab, and try creating motion near the camera again.

6 Do one of the following:

- If you receive the motion events, verify that motion detection is working by configuring the camera to record on motion:
  a. From the Config Tool home page, open the *Video* task.
  b. Select the camera to configure and click the **Recording** tab.
  c. In the **Recording modes** list, select **On motion/Manual**.
  d. Click **Apply**.
- If you still do not receive any motion events, it might be an issue with your camera. Contact Genetec™ Technical Assistance Center.

Optimizing video decoding performance on your computer

Security Desk can detect and use compatible hardware to accelerate video decoding. Hardware acceleration enhances performance, especially when viewing multiple high-definition H.264 streams.

What you should know

For information on recommended video cards and performance benchmarks, see the *Security Center System Requirements Guide*.

NOTE: Security Desk does not support hardware acceleration in Windows XP.

To optimize video decoding performance on your computer:

1 To optimize the operation with NVIDIA video cards, ensure the following:

- The video card is a compatible model.
- The monitor or projector used to display video is plugged into this video card.
- The installed driver is the latest available from NVIDIA's official website.

2 To optimize the operation with Intel Quick Sync, ensure the following:

- Your CPU supports Quick Sync; see http://ark.intel.com to confirm.
- The integrated video card on your CPU is a compatible model.
- A monitor is plugged into the system board's integrated output.
- The Intel integrated graphics is enabled in the BIOS.
- The installed driver is the latest available from Intel's official site.

NOTE: On high-performance computers, NVIDIA GPU decoding works better when Quick Sync is disabled.

3 To troubleshoot problems with multiple screens and multiple GPUs, ensure the following:

- If Scalable Link Interface (SLI) mode is available, disable it.
- If you have multiple NVIDIA video cards, connect each monitor to its own card to use the monitors in parallel.
- If you have video cards using different drivers (AMD, NVIDIA, Intel), set the monitor that is connected to the NVIDIA card as the primary monitor.
- If both integrated and discrete video cards are available, and if your NVIDIA video card meets the recommended requirements, disable your integrated video card in the BIOS. Having the integrated card available hinders the discrete video card performance.
- After installing Security Center on laptops using NVIDIA OPTIMUS technology (combined Intel and NVIDIA GPUs), you must launch each video-intensive application (Security Desk, Genetec™ Video Player, and so on). This registers them as applications that require NVIDIA GPU. After the initial setup, the application always uses the NVIDIA GPU.

Related Topics

Hardware information dialog box on page 378

Troubleshooting H.264 video stream issues

If you are having problems viewing H.264 video streams, you can disable the *AVCodec_ErrorRecognition* advanced Archiver role setting.

To troubleshoot H.264 video stream issues:

1 In the Config Tool *Video* task, select the Archiver to configure.

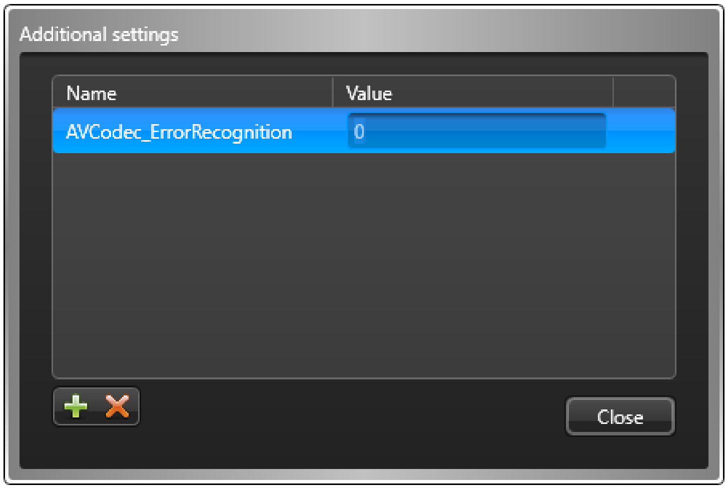
2 Click the **Resources** tab.

3 At the bottom of the **Resources** tab, click **Advanced settings**.

4 Click **Additional settings**.

5 In the *Additional settings* dialog box, click **Add an item** (➕).

6 In the **Name** column, type `AVCodec_ErrorRecognition`.



Name	Value
AVCodec_ErrorRecognition	0

7 In the **Value** column, type 0.

8 Click **Close** > **OK** > **Apply**.

9 When you are asked to restart the Archiver, click **Yes**.

You should see improvement with the video stream. If there is no change, you can try other values (1-4).

Troubleshooting image pixelation or poor image quality of cameras in Security Center

If you are experiencing pixelation or poor image quality when viewing live video in Security Center, there are troubleshooting steps you can perform to determine the cause and fix the issue.

What you should know

This information used to be found in the deprecated knowledge base article KBA-00984.

To troubleshoot image pixelation or bad image quality of cameras in Security Center:

1 Check if the video quality issue is happening on all or most of the cameras.

- If the issue is happening on all or most cameras, continue with the next step.
- If the issue is only happening on a few cameras or one camera, go to step 6.

2 On the server hosting the Archive role that is managing the video units, open the Windows Task Manager.

3 Click the **Performance** tab and check if the CPU or memory usage is high.

   If the CPU or memory usage is high, check if other processes are the cause; if they are, end the processes.

4 In the Windows Task Manager, click the **Networking** tab.

5 Check if the network usage for the network adapter is over 300 Mbps, or over 100 Mbps if you are on the Directory server.

   If the network usage is high, reduce the number of cameras to below 300 on the Archiver role (below 100 if the Archiver role is on the Directory server), or reduce the video quality settings on the cameras in Config Tool. If your quality issues persist, continue with the next step.

6 On the server hosting the Archiver role, check if there are many *RTP Packet Lost* events in the Archiver role logs in *C:\ArchiverLogs*.

   - If there are many events, the cause is most likely an unreliable network. Follow the steps in KBA-00546 (*Camera streams freeze or pixelate over a wireless or unreliable network in Security Center*). to try to resolve the issue. If the quality issues persist, contact the Genetec Technical Assistance Center.
   - If there are only a few events, continue with the next step.

7 Verify that Security Center supports the video unit, and that the unit is running certified firmware.

   For a list of video units supported by Security Center, see our Supported Device List.

8 On the camera web page, view the live video and check if the image is pixelated there also.

   - If the image is pixelated, there are issues with the camera hardware. Contact your camera manufacturer.
   - If the image looks fine, continue with the next step.

9 On the Archiver server, view the recorded video and check if the playback image is also pixelated.

   - If the image is pixelated, follow the steps in KBA-00546 (*Camera streams freeze or pixelate over a wireless or unreliable network in Security Center*). If the quality issues persist, contact the Genetec Technical Assistance Center.
   - If the image looks fine, continue with the next step.

10 In Security Desk, check the video stream information of the camera as follows:

   a) Open a Monitoring task and view the affected camera in a tile.

   b) Press `Ctrl+Alt+A` or `Ctrl+Alt+D` to see the video stream statistics and the *RTP Packet Lost* value.

      If you see that many RTP packets were lost, follow the steps in KBA-00875 (*How to reduce video stream quality issues by configuring AvCodec Error Recognition*) to try and resolve the issue. If you cannot find the network issues that caused the RTP packet loss, contact the Genetec Technical Assistance Center.

Troubleshooting "Not enough bandwidth" errors

If you receive a Not enough bandwidth error message while viewing video or when requesting a video stream in Security Center, you can try to resolve the issue.

What you should know

The Not enough bandwidth message appears when a maximum bandwidth limit is set for a redirector server from Config Tool, or specifically set for the redirected live or playback streams, and the video streams coming from the remote site have exceeded the bandwidth limit. You can receive the error message for one of two reasons:

- You are requesting a new live or playback video stream, but the bandwidth limit is exceeded.
- You are viewing video when the bandwidth limit is reached and a user with a higher user level requests a stream. If you have the lowest user level of all the users who are viewing redirected video streams from that redirector, or if you all have the same user level but you were the last user to request a video stream, then you lose your video stream connection.

To troubleshoot the Not enough bandwidth error, you can try the following:

- If you were not aware that there was limited bandwidth on your network and you think this is incorrect, you can ask your administrator to confirm whether your network configuration is supposed to have limited bandwidth.
- If you often lose your video stream connection and receive the Not enough bandwidth error because another user is requesting a stream, you can ask your administrator if they can give you a higher user level.

Troubleshooting video stream issues

In Security Desk, you can diagnose the status of video streams displayed in the canvas.

What you should know

Diagnosing the video stream helps you to determine the point along the network path where the flow of information is broken. Each component is displayed with incoming and outgoing traffic information. This information can be used to identify potential problems with the video unit, the archiving role, or with redirection to Security Desk, and so on.

To troubleshoot the possible causes of video stream issues:

1. In Config Tool or Security Desk, display a camera in a tile.
2. Press `Ctrl+Shift+R`.

   Diagnostic information about the video stream is overlaid in the tile.
3. Click **OK** to view information about each of the following video stream connections:
   - **Archiver or Auxiliary Archiver or Federation™ redirector:** The streaming status from the source camera to the Archiver role, Auxiliary Archiver role, or Federation™ redirector initially providing the stream.
   - **Redirector:** The streaming status from the Archiver role, Auxiliary Archiver, or Federation™ redirector to the redirector routing the stream to the next hop.

     NOTE: All redirectors involved in the routing are listed.
   - **Media player:** The streaming status from the last redirector involved in the routing to your Security Desk workstation.
4. Click **Close**.

Troubleshooting playback video issues

If you are experiencing problems with your playback video in Security Center, learn about the symptoms, potential causes, and solutions to help you troubleshoot the issue.

Symptoms

Here are some common issues you might experience with playback video in Security Center. To help you solve the issue, click the error message or symptom that you are currently experiencing.

- Cameras not recording on page 720
- Cannot watch playback video
- Quick search does not show thumbnails in Security Desk

Cameras not recording

If you cannot record video, or if there are missing video archives or gaps in the archives, you can determine the cause of the issue.

What you should know

If live video from a camera can be viewed but not recorded, it might be due to one of the following:

- The recording mode of the camera
- The Archiving schedule
- The Archiver role database
- CPU usage

Here are some ways to identify if the camera is not recording:

- When viewing live video, the recording status of the camera in the lower-right corner appears as Live.
- You are unable to view playback video that should exist for a specific date and time.
- The **Record** button is yellow (!) in the camera widget or in the tile video controls of the *Monitoring* task.

To troubleshoot why a camera is not recording:

1 Verify that Security Center supports the unit, and that the unit is running the certified firmware.

For a list of video units supported by Security Center, see our Supported Device List.

2 Verify the camera recording type to ensure that the camera set to record video on the correct schedule:

a) In the Config Tool *Video* task, select your camera.

b) Click the **Recording** tab.

- If the **Recording settings** option is set to **Custom settings**, ensure that all the recording settings are correct, and then click **Apply**.
- If the **Recording settings** option is set to **Inherit from Archiver**, continue with the next substep.

c) In *Video* task, select the Archiver.

d) Click the **Camera default settings** tab.

e) In the *Recording modes* section, make sure that the Archiver is set to record on the correct **Schedule**, and that the recording **Mode** is not set to **OFF**.

f) If the **Custom settings per server** option is enabled, make sure that archiving is enabled on the server the Archiver should be recording on.

3 If the camera recording mode is set to **On motion / Manual**, ensure that motion detection settings are configured properly:

a) In the Config Tool *Video* task, select your camera.

b) Click **Video analytics** > **Motion detection**.

c) Verify the motion detection settings.

For more information, see the *Security Center Adminstrator Guide.*

4 Check the status of the Archiver role database:

a) In the Config Tool *Video* task, select the Archiver.

b) Click the **Resources** tab.

- If the Archiver database status is **Connected**, go to the next troubleshooting step.
- If the Archiver database status is **Disconnected** or **Unavailable**, continue with the next substep.

c) Switch to a different archive database or create a new one.

CAUTION: Perform this step at a noncritical time, because all the units connected to the Archiver will temporarily go offline. Do not delete or overwrite the existing database, or your video archives will be deleted.

1. In the **Database** field, enter a different name and click **Apply**.
2. Wait for the role to connect to the new database. If the database does not exist, it will be created.
3. If the camera can record using the new database, you can continue to use the new database.

   CAUTION: When you switch to a different database, the video archives referenced in the old database are no longer included in Security Center searches, and will not be deleted by the Archiver's automatic cleanup.
4. If the camera is still not recording, revert back to the original database, and continue with the next troubleshooting step.

5 Check how much disk space is available for archiving:

a) In the Config Tool *Video* task, select the Archiver.

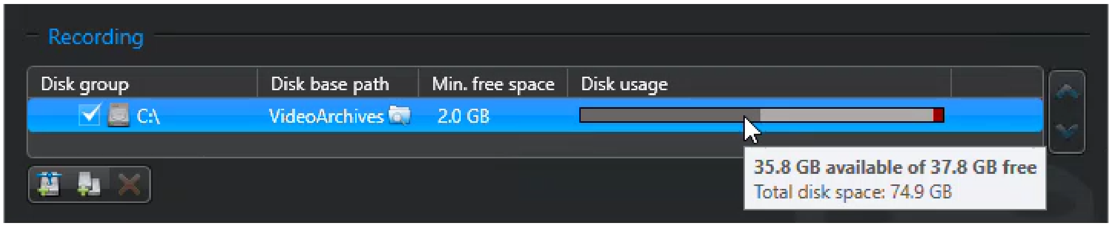
b) Click the **Resources** tab.

c) In the disk information table, make sure the **Min. free space** value is at least 0.2% of the total disk space.

The **Min. free space** is the minimum amount of free space that the Archiver must leave untouched on the disk.

d) If the **Min. free space** value is less than 0.2% of the total disk space, click the value and increase it.

To see the total disk space, point the mouse cursor to the **Disk usage** meter.



Recording

Disk group	Disk base path	Min. free space	Disk usage
☑ C:\	VideoArchives	2.0 GB	

35.8 GB available of 37.8 GB free
Total disk space: 74.9 GB

6 Check for *Archiving stopped* and *Recording stopped* events that occurred on your system.

In Windows, on the server where the Archiver role is running, open the *.log* files, found in *C:\ArchiverLogs*.

If there are *Archiving stopped* or *Recording stopped* events in the **Entry type** column, restart the Genetec™ Server service:

a) Open your Windows Control Panel.

b) Click **Administrative Tools** > **Services**.

c) Right-click the **Genetec™ Server** service and click **Restart**.

7 Check for *Transmission lost* and *RTP packets lost* events that occurred on your system.

In Windows on the server where the Archiver role is running, open the *.log* files, found in *C:\ArchiverLogs*.

- If there are many Transmissions *lost* and *RTP packets lost* events in the **Entry type** column, there could be a CPU usage or network issue. Continue with the next troubleshooting step.
- If there are not many *Transmission lost* and *RTP packets lost* events, then skip the next troubleshooting step.

8 Check your CPU usage:

a) Right-click the Windows taskbar and open *Windows Task Manager*.

b) Click the **Performance** tab, and check that the **CPU Usage** is below 60%.

If the **CPU usage** is over 60%, restart the server, and consider adding more CPU to the server.

c) Click the **Networking** tab, and make sure the network **Link speed** is not over 300 Mbps.

9 If you are only experiencing recording problems with one video unit, try the following:

a) In the Config Tool *Video* task, right-click the red video unit and click **Delete**.

b) In the confirmation dialog box, choose whether you want to keep the video archives from the unit.

The video unit is removed from the Archiver.

c) Add the video unit.

After you finish

If you still cannot record video on the camera, contact Genetec™ Technical Assistance Center.

Cannot watch playback video in Security Desk

If you cannot view playback video or video archives in Security Desk, you can troubleshoot the issue.

To troubleshoot why you cannot view playback video:

1 Try viewing live video from the same camera by dragging the camera from the area view to a tile in the canvas in the Security Desk *Monitoring* task.

- If you can view live video, continue with the next troubleshooting step.
- If you cannot view any video, then it is probably a network issue. See Video units offline in Security Center on page 734.

2 Try viewing playback video from the *Archives* task:

a) In the Security Desk *Archives* task, select your camera.

b) Search for video archives at different dates and times and click **Generate report**.

c) After the report is generated, try to view video from the archives.

d) Repeat the steps with other cameras that are connected to the same Archiver.

- If you can view the video from some of the video archives, continue with the next troubleshooting step.
- If you cannot view any video, skip the next troubleshooting step.

3 Verify that Security Center supports the unit, and that the unit is running the certified firmware.

For a list of video units supported by Security Center, see our Supported Device List.

4 Try viewing playback video from the *Archives* task on another Security Desk, and on the server where the Archiver role is running.

- If you can view video, it might be a problem with the redirection from the Media Router to your Security Desk. Continue with the next troubleshooting step.
- If you cannot view any video, contact Genetec™ Technical Assistance.

5 Make sure the correct ports are open on your network so that there is no firewall blocking the video stream. For more information, see the topic *Default ports used by Security Center* in the *Security Center Adminstrator Guide*.

6 If you still cannot view playback video, contact Genetec Technical Assistance Center.

Quick search does not show thumbnails in Security Desk

Users do not see thumbnails when they use *Quick search* in Security Desk if the recording is performed on the edge device. To resolve this issue, you must disable thumbnail queries from Security Desk to the Archiver by adding a setting to the *SecurityDesk.exe.gconfig* file. If the recording is done by the Archiver, make sure that thumbnail requests are enabled on the Archiver role.

NOTE: Thumbnails are not supported by cameras that use fusion stream encryption for video streams that are in transit and at rest.

Recording is performed on the edge devices

Description: By default, Security Desk queries the Archiver for video thumbnails. However, if the recording is not done by the Archiver, no thumbnails can be returned by the latter.

Solution: Turn off the default behavior so Security Desk would stop asking the Archiver for thumbnails and generate the thumbnails itself.

1. On the Security Desk workstation, go to the Security Center installation folder.

   The default on a 64-bit machine is *C:\Program Files (x86)\Genetec Security Center 5.11*.
2. Open with a text editor, the file *SecurityDesk.exe.gconfig*.
3. Add the following line immediately after the line containing `<visitorManagement .../>`.

   ```
   <quickSearch thumbnailQuery="false"/>
   ```
4. Save your changes and close the file.
5. Restart Security Desk.

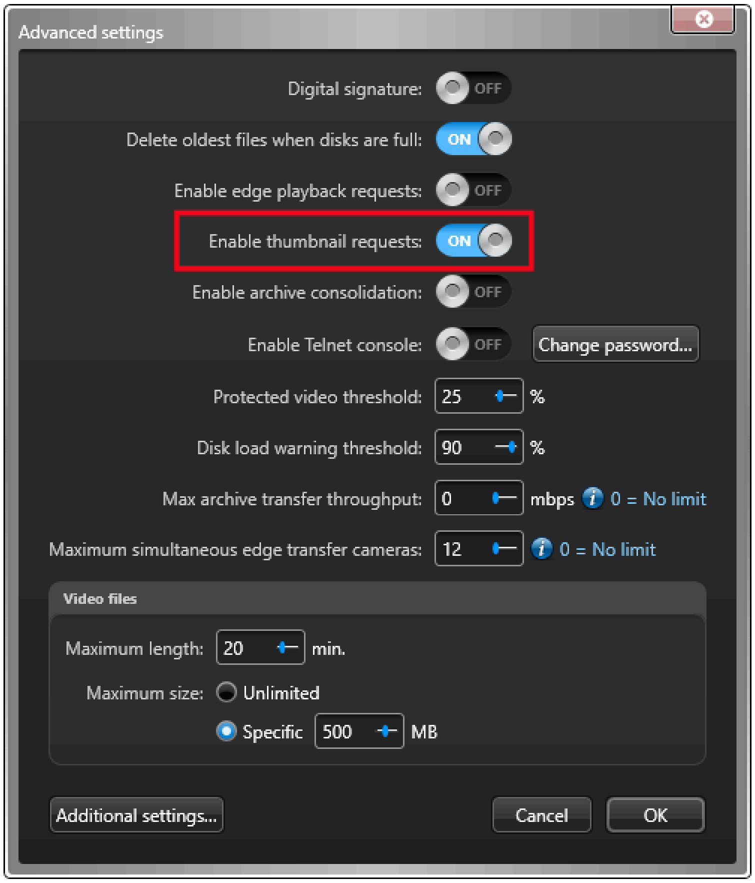
Thumbnail requests are not enabled on the Archiver role

Description: Thumbnail requests are enabled on all Archiver roles by default. If you are sure that the recording is done by the Archiver, verify that thumbnail requests are enabled.

Solution: To enable thumbnail requests on an Archiver role:

1. From the Config Tool home page, open the *Video* task.
2. Select the Archiver role to configure, and then click the **Resources** tab.
3. Click **Advanced settings**.

4. In the dialog box that opens, turn on the **Enable thumbnail requests** option.



Advanced settings

Digital signature: OFF

Delete oldest files when disks are full: ON

Enable edge playback requests: OFF

Enable thumbnail requests: ON

Enable archive consolidation: OFF

Enable Telnet console: OFF

Protected video threshold: 25 %

Disk load warning threshold: 90 %

Max archive transfer throughput: 0 mbps 0 = No limit

Maximum simultaneous edge transfer cameras: 12 0 = No limit

Video files

Maximum length: 20 min.

Maximum size: ○ Unlimited

● Specific 500 MB

5. Click **OK** > **Apply**.

   The Archiver automatically restarts. This should take 1-3 seconds.

Troubleshooting video unit issues

If you are experiencing problems with your video units in Security Center, learn about the symptoms, potential causes, and solutions to help you troubleshoot the issue.

Symptoms

Here are some common issues that you might experience with video units in Security Center. To help you solve the issue, click the error message or symptom that you are currently experiencing.

- Cannot add video units
- Cannot delete video units
- Moving video units to a different Archiver on page 733
- Replacing video units on page 733
- Video units offline

Cannot add video units in Security Center

If a video unit cannot be added in Config Tool, there might be an issue with your hardware, network, or credentials. To troubleshoot the issue, learn about the possible causes and their respective solutions.

Unit is offline

The video unit is offline and might be broken or unplugged.

Solution:

1. Open a Windows Command Prompt.
2. Type `ping <IP ADDRESS>`.
3. Press Enter.
4. If there is no response from the unit, check that the unit is plugged in.
5. If the video unit must be replaced, contact the unit manufacturer.

Issue communicating with unit

Communication with the video unit is lost.

Solution:

1. On the Archiver server that manages the video unit, open a web browser.
2. In the address bar, type the IP address of the unit.
3. Verify that you can connect to the unit web page.
4. From the unit web page, reboot the unit.
5. Add the unit in Config Tool again.

Unsupported hardware or firmware

The video unit or firmware is not supported in Security Center.

Solution: Verify that the unit is supported by Security Center and that it is running the certified firmware. If required, update the unit firmware.

For information about upgrading the firmware on a unit, see the manufacturer documentation.

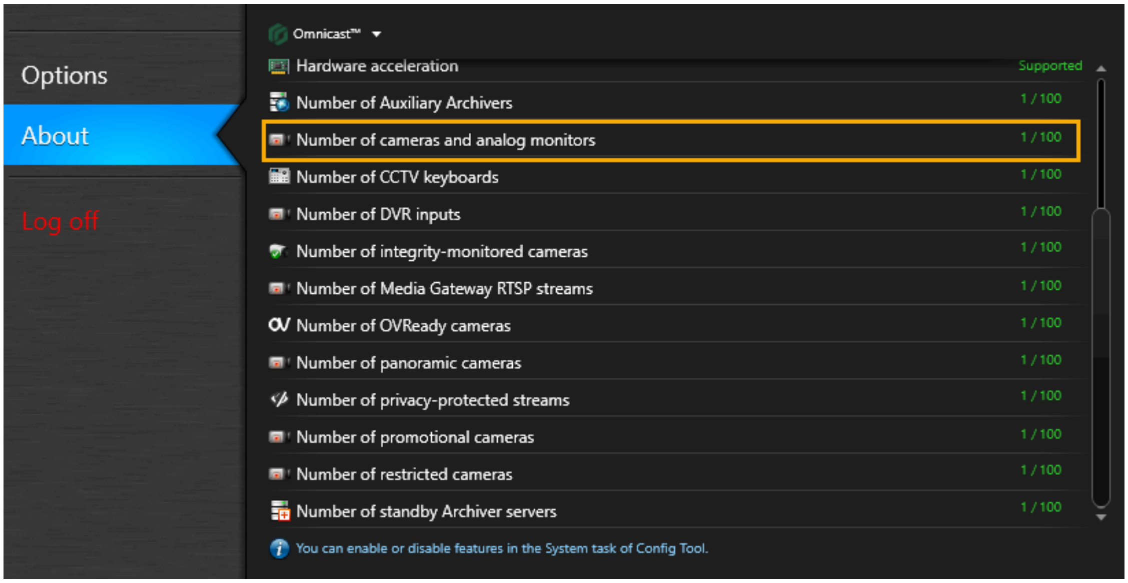
No camera connections in license

There are no camera connections available in your Security Center license.

Solution:

1. From the Config Tool home page, click **About**, and then click the **Omnicast™** tab.
2. Check if a camera connection is available for the **Number of cameras and analog monitors** license option.

   NOTE: The *promotional cameras* license option cannot be used when adding regular cameras.



Options

About

Log off

Omnicast™

Hardware acceleration	Supported
Number of Auxiliary Archivers	1 / 100
Number of cameras and analog monitors	1 / 100
Number of CCTV keyboards	1 / 100
Number of DVR inputs	1 / 100
Number of integrity-monitored cameras	1 / 100
Number of Media Gateway RTSP streams	1 / 100
Number of OVReady cameras	1 / 100
Number of panoramic cameras	1 / 100
Number of privacy-protected streams	1 / 100
Number of promotional cameras	1 / 100
Number of restricted cameras	1 / 100
Number of standby Archiver servers	1 / 100

You can enable or disable features in the System task of Config Tool.

3. If there are no camera connections available, contact your sales representative to modify your license. Alternatively, you can submit a purchase order to customerservice@genetec.com.

Incorrect license options

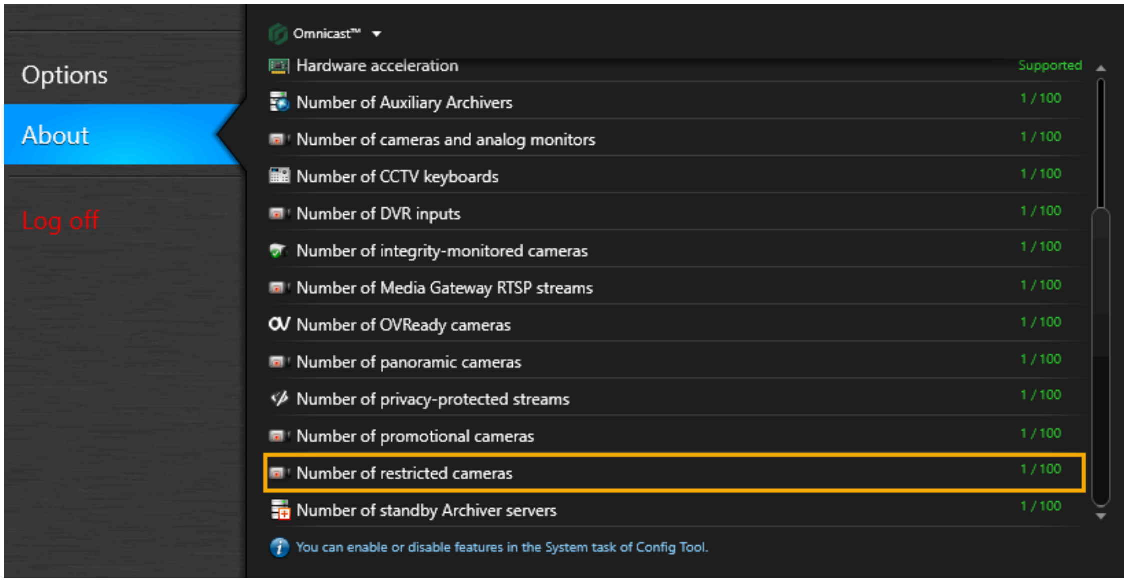
You do not have the correct license options required for your camera.

If you are trying to add a restricted camera, you require a regular camera license and a restricted camera license in Security Center. To view a list of manufacturers that require a restricted license, go to our Supported Device List, click **License type**, and select the **Restricted** checkbox.

Solution:

1. From the Config Tool home page, click *About*, and then click the **Omnicast™** tab.

2. Check if a camera connection is available for the **Number of restricted cameras** license option.



Hardware acceleration	Supported
Number of Auxiliary Archivers	1 / 100
Number of cameras and analog monitors	1 / 100
Number of CCTV keyboards	1 / 100
Number of DVR inputs	1 / 100
Number of integrity-monitored cameras	1 / 100
Number of Media Gateway RTSP streams	1 / 100
Number of OVReady cameras	1 / 100
Number of panoramic cameras	1 / 100
Number of privacy-protected streams	1 / 100
Number of promotional cameras	1 / 100
Number of restricted cameras	1 / 100
Number of standby Archiver servers	1 / 100

You can enable or disable features in the System task of Config Tool.

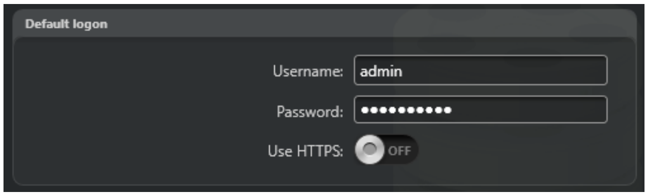
3. If there are no camera connections available, contact your sales representative to modify your license. Alternatively, you can submit a purchase order to customerservice@genetec.com.

Incorrect unit credentials

You tried to add the unit with incorrect credentials. For some manufacturers, you must set the default credentials on the Archiver role *Extensions* page.

Solution:

1. From the Config Tool home page, open the *Video* task.
2. Select the Archiver that you want to add the video unit to and click the **Extensions** tab.
3. To add the extension for the video unit, click **Add an item** (➕), select the extension type, and click **Add**.
4. Select the extension.
5. In the *Default logon* section, enter the **Username** and **Password** for the unit and click **Apply**.



Default logon

Username: admin

Password: ●●●●●●●●●●●

Use HTTPS: OFF

6. Add the unit in Config Tool again.

Issue with Archiver role

The Archiver role that you want to add the unit to is offline or not running properly.

Solution:

1. From the Config Tool home page, open the *Video* task.
2. Right-click the Archiver role and click **Maintenance** > **Diagnose** (✚).
3. Fix any issues that are found.
4. Add the unit in Config Tool again.

Issue with Archiver role database

The Archiver role that you want to add the unit to is connected to the wrong database.

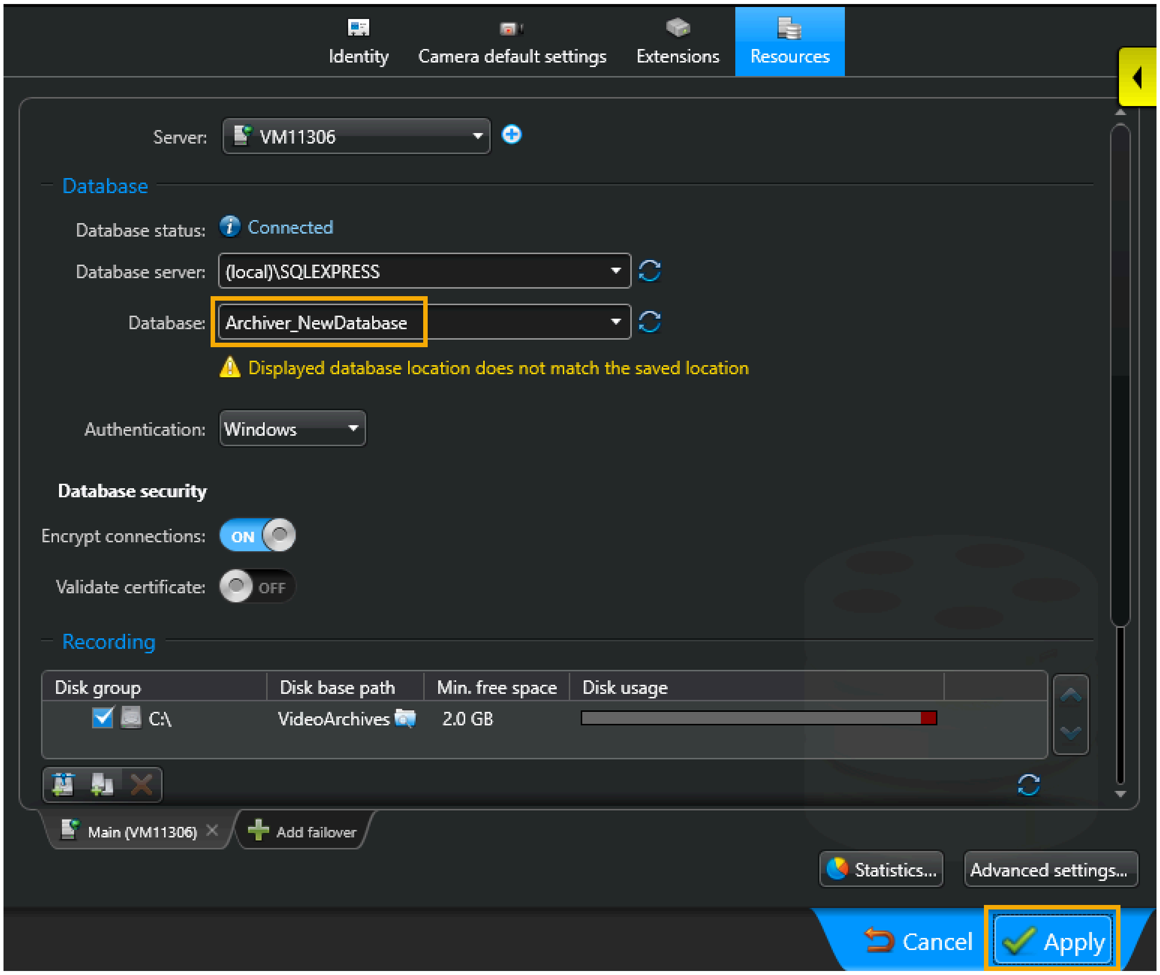
Solution:

1. From the Config Tool home page, open the *Video* task.
2. Select the Archiver role and click the **Resources** tab.
3. If the database status is *Disconnected* or *Unavailable*, switch to a different archive database, or create one as follows:

   CAUTION: Perform this step at a non-critical time, as all the units connected to the Archiver role will temporarily go offline. Do not delete or overwrite the existing database or your video archives will be deleted.

   a. In the **Database** field, enter a different database name.
   b. Click **Apply** and wait for the role to connect to the new database.

      If the database does not exist, it will be created.



Server: VM11306

Database status: Connected

Database server: (local)\SQLEXPRESS

Database: Archiver_NewDatabase

Displayed database location does not match the saved location

Authentication: Windows

Encrypt connections: ON

Validate certificate: OFF

Disk group	Disk base path	Min. free space	Disk usage
☑ C:\	VideoArchives	2.0 GB	

4. Add the unit in Config Tool again.
   - If the unit is added successfully, continue using the new database.

     CAUTION: When you switch databases, video archives in the old database are no longer included in Security Center searches, and are not deleted by the **Automatic Cleanup** settings of the Archiver role.
   - If you still cannot add the unit, revert to the original database.

Issue with Media Router role

The Media Router role is offline or not running properly.

Solution:

1. From the Config Tool home page, open the *Video* task.
2. Right-click the Media Router role and click **Maintenance** > **Diagnose** (✚).
3. Fix any issues that are found.
4. Add the unit in Config Tool again.

Issue with Media Router role database

The Media Router role is connected to the wrong database.

Solution:

1. From the Config Tool home page, open the *Video* task.
2. Select the Media Router and click the **Resources** tab.
3. If the Media Router status is *Disconnected* or *Unavailable*, click **Create a database** (✚).
4. Add the unit in Config Tool again.

Firewall blocking communication

There is a firewall is blocking communication to the unit, preventing you from adding it.

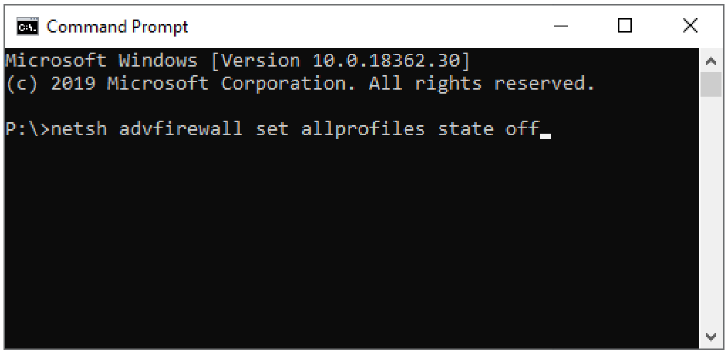
Solution:

1. On the Archiver server that will manage the video unit, disable Windows Firewall:

   IMPORTANT: We recommend re-enabling the Windows firewall after troubleshooting.

   a. Open a Windows Command Prompt as administrator.

   b. Type `netsh advfirewall set allprofiles state off` and press Enter.

   ```
   Microsoft Windows [Version 10.0.18362.30]
   (c) 2019 Microsoft Corporation. All rights reserved.

   P:\>netsh advfirewall set allprofiles state off_
   ```

   If the command is successful, you receive a confirmation message.

   c. To verify that Windows Firewall is disabled, type `netsh advfirewall show allprofiles` and press Enter.

   All the profile states should be **OFF**.

2. After the Windows Firewall service is stopped, restart all Security Center applications and services, and then add the unit in Config Tool again.
3. Re-enable Windows Firewall.

Incorrect port configuration

The HTTP or HTTPS port configuration is incorrect. The issue might be one of the following:

- You are using the wrong discovery port.
- You are using HTTPS protocol, but the certificates for the unit are not accepted by the Archiver role. The certificate is untrusted, expired, or does not match the IP address or hostname of the unit.

Solution:

1. Make sure you have the correct HTTP or HTTPS discovery port number for your unit.

   NOTE: For Bosch units, additional configuration is required to use HTTP or HTTPS protocol. See the topic *Enrolling Bosch units using HTTP or HTTPS* in the *Security Center Adminstrator Guide*.
2. If you are using HTTPS protocol, make sure that HTTPS is enabled on the unit web page and do one of the following:
   - Acquire and install valid certificates for the unit.

     For information about setting up fusion stream encryption in Security Center, see the topic *What is fusion stream encryption?* in the *Security Center Adminstrator Guide*.
   - (Not recommended) Use a self-signed certificate and disable the security settings for the video unit extension in Config Tool. See the topic *Configuring HTTPS for video unit extensions* in the *Security Center Adminstrator Guide*.
3. Add the unit in Config Tool again.

Incorrect network configuration

Your network configuration is incorrect.

Solution:

1. Verify that each network on your system is configured properly:
   a. From the Config Tool home page, open the *Network view* task.
   b. Select a network, click the **Properties** tab, and make sure all the settings are correct (IP prefix, subnet mask, routes, network capabilities, and so on).
   c. If required, change the network settings and click **Apply**.

   For more information about configuring network settings, see *About networks* in the *Security Center Adminstrator Guide*.
2. Make sure that the Archiver role, Media Router role, and all redirectors areArchiverand using the correct network interface card (NIC):
   a. From the Config Tool home page, open the *Video* task.
   b. Select the Archiver role click the **Resources** tab.
   c. From the **Network card** list, select the appropriate NIC.
   d. In the entity browser, select the **Media Router** role and click the **Resources** tab.
   e. In the *Servers* section, click **Advanced** (⚙).
   f. Select the appropriate **Network card** for each server and click **Apply**.
   g. Click the **Properties** tab.
   h. Select a redirector and click **Edit the item** (✏).
   i. From the **Multicast interface** list, select the appropriate NIC and click **Save**.
   j. Set the appropriate NIC for each redirector.

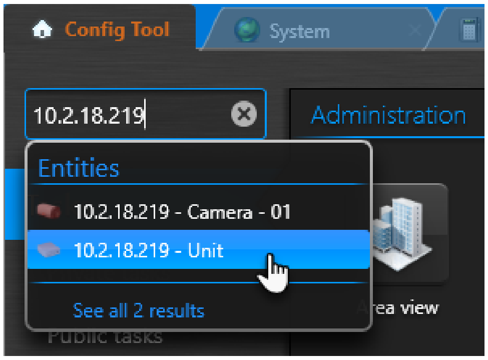
3. Verify the NIC priority in Windows:
   a. In Windows, click **Start** > **Run** and type `ncpa.cpl`.
   b. In the *Network Connections* window, click the **Advanced** menu and select **Advanced Settings**.
   c. Note which NIC on your server is configured as network priority one (top of the connection list) and which is configured as priority two.
   d. If required, use the arrow buttons on the right side to reposition the connections in the list.
4. Add the unit in Config Tool again.

Unit already exists

The unit is already part of the Directory, but it is offline or was added with a different IP address or hostname. If this is the reason you cannot add the video unit, you receive a Unit already exists error message when you try to add the unit.

Solution:

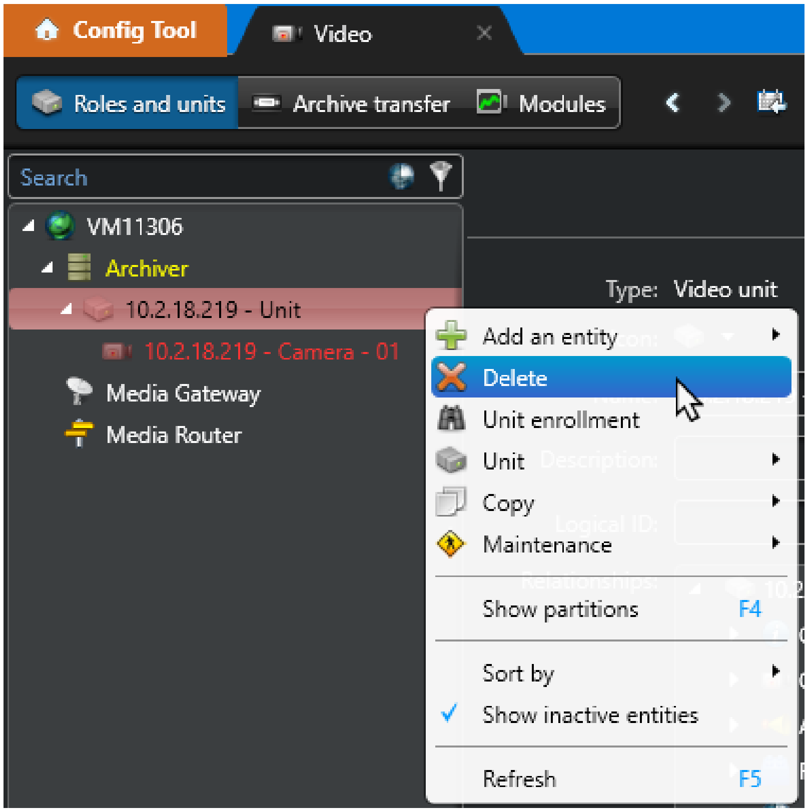
1. Search for the video unit using the global search box in Config Tool.
   - If you find the unit and it is red (offline), go to the next step.



   - If you cannot find the unit, it might be under a different name. Try the following:
     a. In the Config Tool *Video* task, expand all the roles in the entity browser.
     b. Open the unit web page and restart the unit.
     c. In Config Tool, note whether any of the video units go offline.

        The video unit that goes offline is the unit you are looking for.

2. In the *Video* task, right-click the video unit in the entity browser and click **Delete**.



3. Add the unit in Config Tool again.
4. If you still cannot add the unit, restart the Genetec™ Server service and add the unit again.

   IMPORTANT: When you restart the Genetec™ Server service, all entities disconnect from Security Center. Perform this step at a non-critical time.

Cannot delete video units

If you cannot delete a video unit, you can temporarily deactivate the Archiver.

To delete a video unit:

1 In the Config Tool *Video* task, select the Archiver role.

2 At the bottom of the *Video* task, click **Maintenance** > **Deactivate role** (🚦).

3 In the confirmation dialog box, click **Continue**.
The Archiver role and all video units controlled by the role turn red.

4 Select the video unit, and at the bottom of the *Video* task, click **Delete** (✕).

5 Select the Archiver role, and at the bottom of the *Video* task, click **Maintenance** > **Activate role** (🚦).

Moving video units to a different Archiver

If you want a different Archiver role to manage and control a video unit, for load distribution or another purpose, you can move the unit to another Archiver using the *Move unit* tool.

Before you begin

- The Archiver role must be on the same LAN as the video unit it controls.
- If you are using custom settings for the unit extension, such as custom logon credentials, you must configure the same extension settings on the new Archiver role.

What you should know

Existing archives are not moved with the video unit to the new Archiver role. They remain associated with the old Archiver until their retention period ends.

To move a video unit to a different Archiver:

1 From the Config Tool home page, click **Tools** > **Move unit**.

2 From the **Unit type** list, select **Video unit**.

3 Select the units that you want to move.

4 Under **Archiver**, select the new Archiver role to control the unit.

5 Click **Move** > **Close**.

After you finish

Move any important video archives over to the new Archiver at a convenient time. For more information, see the topic *Duplicating video archives* in the *Security Center Adminstrator Guide*.

Related Topics

Archiver: Extensions tab on page 1341

Replacing video units

If a video unit fails and is offline in Security Center, displayed red in the area view, you can replace the unit with a compatible one using the same settings.

Before you begin

- Before replacing the unit using the Unit replacement tool, copy the configuration settings of the old video unit and the cameras it controls to the new video unit.
- If you are replacing a SharpV ALPR unit, the new unit must have a unique IP and Port configuration. If the unit is behind a NAT, configure a unit on a different port. If the unit is not behind a NAT, configure a new IP address. If you do not configure a new IP address and port combination, you receive the error: *Unit creation failed (The unit located at the following address: xxx.xxx.xxx, already belongs to another role)*

What you should know

To ensure that the *video archives* associated to the old unit are not lost, the Unit replacement tool re-associates them to the new unit.

IMPORTANT: Cameras controlled by the new video unit are treated as new cameras by the system. If associations exist between old cameras and other entities in the system, these associations must be manually re-created for the new cameras.

To replace a video unit:

1 Add a new video unit to the Archiver controlling the old unit.

The new unit must be compatible with the old unit in terms of settings and cameras they control.

2 Copy the configuration settings of the old video unit to the new video unit, using the Copy configuration tool. For more information, see the topic *Copying configuration settings from one entity to another* in the *Security Center Administrator Guide*.

3 Copy the configuration settings of the cameras controlled by the old video unit to the new cameras, using the Copy configuration tool. For more information, see the topic *Copying configuration settings from one entity to another* in the *Security Center Administrator Guide*.

4 From the homepage, click **Tools** > **Unit replacement**.

5 In the **Unit type** option, select **Cameras**.

6 For each old camera, do the following:

a) Select the **Old** camera and the **New** camera.

b) Click **Swap**.

The video archives and event logs associated to the old cameras are now associated to the new cameras.

7 If the old cameras were associated with entities such as doors and alarms, represented on maps, or used for *visual tracking*, you must manually replace these associations.

For each old camera, do the following:

a) Select the camera in the area view.

b) Click **Identity** > **Part of...**

c) Click a related entity and click **Jump to** (➔).

d) In the entity configuration page, remove the association to the old camera and add the association to the new camera.

e) If the camera is represented on a map or used for visual tracking, replace the old camera with the new camera.

8 Verify that the video archives are associated with the new video unit:

a) In Security Desk, open the *Archives* task.

b) Select a camera that is controlled by the new video unit.

All days that include video archives for the selected camera are listed in the **All available** tab.

c) Select a day and click **Generate report**.

9 After everything is verified, return to the Config Tool *Video* task.

10 Right-click the old unit and click **Delete** (✖).

11 Click **Continue** to confirm deletion.

Video units offline in Security Center

When a camera is red in the area view, it means that the video unit is offline or has lost communication with the Archiver. To troubleshoot the issue, learn about the possible causes and their respective solutions.

What you should know

When a unit goes offline in Security Center, it typically coincides with a *Unit lost* event in Security Desk. This can be the result of an unstable network connection, or issues with the unit.

To troubleshoot why a unit is offline:

1 Verify that you can ping the unit:
   a) In the Config Tool *Video* task, select the red video unit.
   b) At the bottom of the *Video* task, click **Unit** > **Ping** ( ).

   If there is no reply, the unit is offline (broken, unplugged, and so on), or there is a problem with your network.

2 Make sure you can connect to the unit, and then click **Unit** > **Unit's web page**.

   TIP: You can also determine if you have the correct credentials for the unit.

3 Restart the unit:
   a) In the Config Tool *Video* task, select the red video unit.
   b) At the bottom of the *Video* task, click **Unit** > **Reboot** ( ).

4 Verify that Security Center supports the unit, and that the unit is running the certified firmware.

   For a list of video units supported by Security Center, see our Supported Device List.

5 Restart the Archiver role controlling the unit:

   IMPORTANT: Perform this step at a non-crucial time, because all the units connected to the Archiver go offline temporarily.
   a) In the Config Tool *Video* task, select the Archiver role.
   b) At the bottom of the *Video* task, click **Maintenance** > **Deactivate role** ( ).
   c) In the confirmation dialog box, click **Continue**.

      The Archiver role and all video units controlled by the role turn red.
   d) At the bottom of the *Video* task, click **Maintenance** > **Activate role** ( ).

After you finish

If the video unit is still offline, contact Genetec™ Technical Assistance Center.

Finding missing files on your system

To find video files that are still referenced by your archive database but are no longer accessible from the storage device, you can use the *VideoFileAnalyzer.exe* tool.

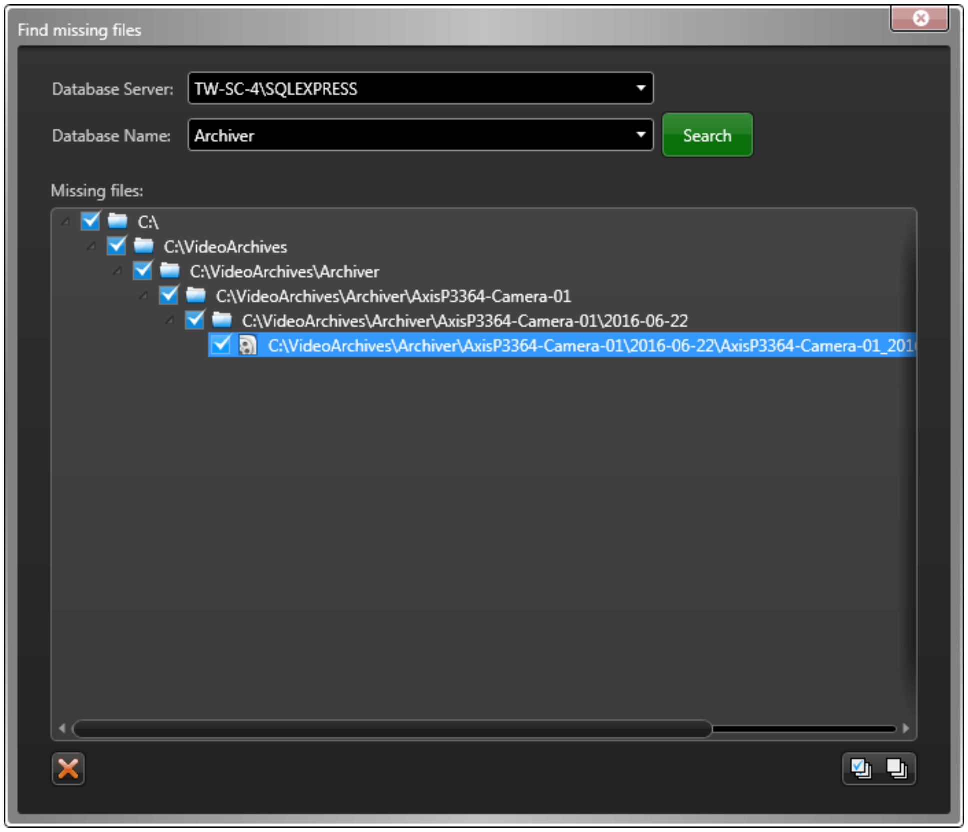
What you should know

A missing file is a video file that is still referenced by an archive database, but cannot be accessed anymore. This situation occurs when video files are deleted manually without using the *Archive storage details* task, creating a mismatch between the number of video files referenced in the database and the actual number of video files stored on disk.

To find missing files on your system:

1. Open the *VideoFileAnalyzer.exe* tool.
   - *C:\Program files (x86)\Genetec Security Center 5.11* (64-bit computer)
   - *C:\Program files\Genetec Security Center 5.11* (32-bit computer)
2. At the bottom of the *Video File Analyzer* dialog box, click **Find missing files**.
3. In the *Find missing files* dialog box, specify the **Database Server** and the **Database Name** you want to check for missing video files.

   You can find the database server and database name in the *Resources* page of the Archiver or Auxiliary Archiver role in Config Tool.
4. Click **Search**.
5. When the scan is complete, select files in the *Missing files* section and click **Delete files** (✖).



Find missing files

Database Server: TW-SC-4\SQLEXPRESS

Database Name: Archiver

Missing files:

☑ C:\
☑ C:\VideoArchives
☑ C:\VideoArchives\Archiver
☑ C:\VideoArchives\Archiver\AxisP3364-Camera-01
☑ C:\VideoArchives\Archiver\AxisP3364-Camera-01\2016-06-22
☑ C:\VideoArchives\Archiver\AxisP3364-Camera-01\2016-06-22\AxisP3364-Camera-01_201

The selected file indexes are permanently removed from your archive database.

Finding orphan files on your system

To find video files that are no longer referenced by your Archiver database, you can use the *VideoFileAnalyzer.exe* tool found in the Security Center installation folder.

What you should know

An orphan file is a video file that is no longer referenced by any archive database. Orphan files remain on the disk until they are manually deleted. This situation occurs when the archive database is changed inadvertently, creating a mismatch between the number of video files referenced in the database and the actual number of video files stored on disk.

To avoid this problem perform a full archives backup before changing the database, and restore the backup after changing the database.

To find orphan files on your system:

1 Open the *VideoFileAnalyzer.exe* tool.

- *C:\Program files (x86)\Genetec Security Center 5.11* (64-bit computer)
- *C:\Program files\Genetec Security Center 5.11* (32-bit computer)

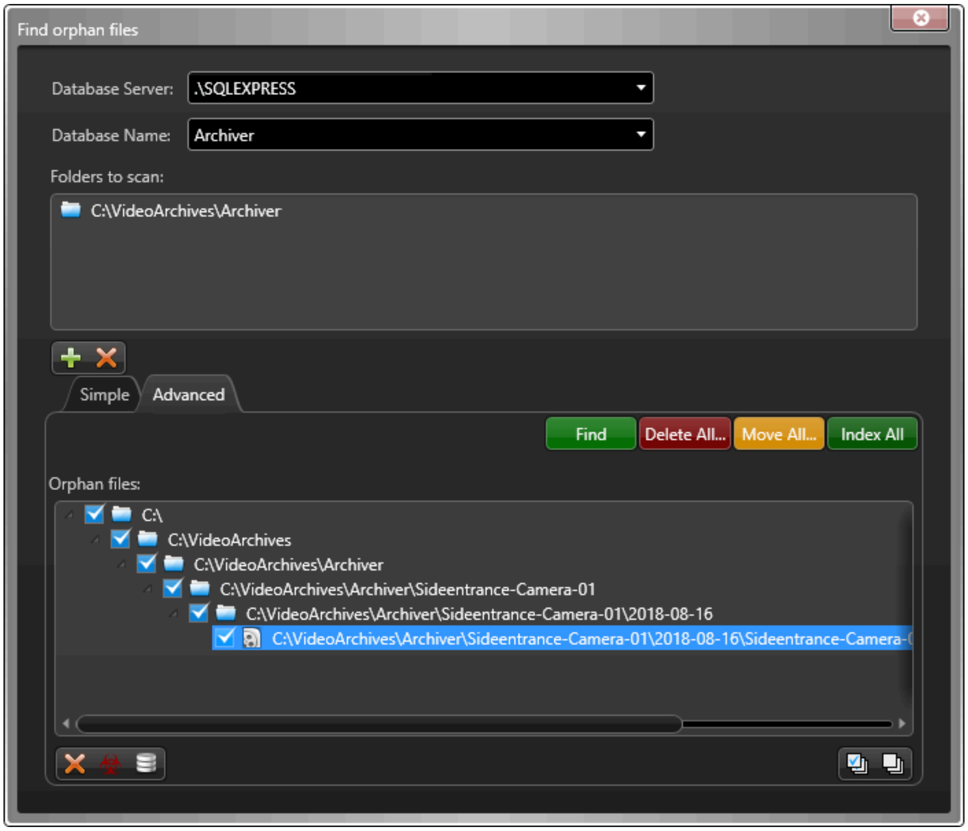
2 At the bottom of the *Video File Analyzer* dialog box, click **Find orphan files**.

3 In the *Find orphan files* dialog box, specify which archive database you want to check for orphan files.

You can find the database server and database name in the *Resources* page of the Archiver or Auxiliary Archiver role in Config Tool.

4 Under the *Folders to scan* section, click **Add** (➕) to add the folders you want to scan, and click **OK**.

5 Click **Advanced** > **Find**.



Find orphan files

Database Server: .\SQLEXPRESS

Database Name: Archiver

Folders to scan:

C:\VideoArchives\Archiver

Orphan files:

☑ C:\
☑ C:\VideoArchives
☑ C:\VideoArchives\Archiver
☑ C:\VideoArchives\Archiver\Sideentrance-Camera-01
☑ C:\VideoArchives\Archiver\Sideentrance-Camera-01\2018-08-16
☑ C:\VideoArchives\Archiver\Sideentrance-Camera-01\2018-08-16\Sideentrance-Camera-

6 Select files in the *Orphan files* section, and do one of the following:

- To permanently remove the selected files from your system, click **Delete files** (✖).
- To move the selected files to another location and free up archive storage space, click **Move files to another folder** (☣).

  By moving the files, you can examine them and decide what to do with them later without affecting the archiving role's operation.
- To index the selected files in the archive database again, click **Add files to the database** (🛢). This ensures that they can be found using the *Archives* report in Security Center.

  NOTE: Only basic information, such as recording start time and end time is retrieved. This operation should only be used as an emergency measure; therefore, it is recommended to back up your database before you index the files again.

To delete, move, or index all the files found in the folders you added, click the corresponding colored button.

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

Related Topics

Backing up databases on page 147

Upgrading video unit firmware

Camera manufacturers frequently upgrade their products and fix security vulnerabilities within new firmware. So, it is best practice to upgrade video units with the latest firmware certified by Genetec Inc.

Before you begin

- If *Genetec™ Update Service (GUS)* is running, the status of the firmware upgrade is indicated in the unit's *Identity* page and in the **Proposed firmware description** column of the *Hardware inventory* report:
  - **Up to date:** No firmware upgrade is necessary.
  - **Optional:** The firmware upgrade is not urgent.
  - **Recommended:** The firmware upgrade is recommended.
  - **Security vulnerability:** The firmware upgrade fixes a security vulnerability issue and is highly recommended.
- Download the recommended firmware from the manufacturer's website. If GUS is not running, you can find the recommended firmware for your unit from our Supported Device List.

  NOTE: For certain video unit models, GUS can download for you the recommended firmware so you don't have to do it yourself. When the download option is available, the recommended firmware version is indicated in the *Upgrade firmware* dialog box. The downloaded firmwares are kept in a central storage managed by GUS, called the *Firmware Vault*, for seven days.
- Take note of the unit’s configuration settings. For some manufacturers, the unit is reset to its default settings after the firmware upgrade.

What you should know

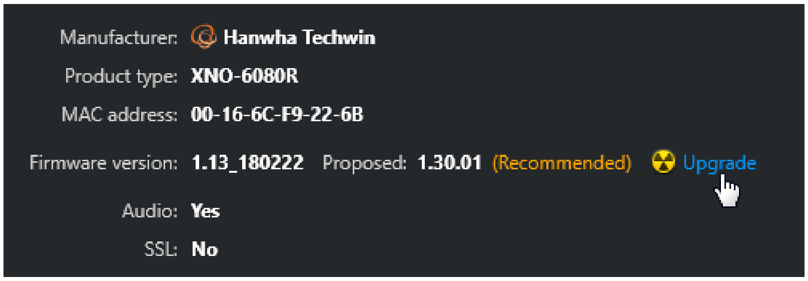
For some manufacturers, you cannot upgrade the unit’s firmware from Config Tool. For manufacturer-specific information, see the manufacturer's documentation.

To upgrade the firmware of a single video unit:

1 From the Config Tool home page, open the *Video* task.

2 Select the video unit to upgrade, and click the **Identity** tab.

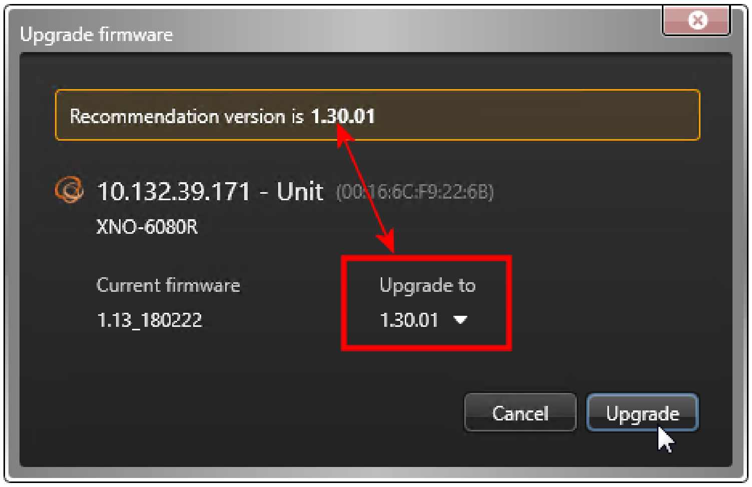
3 Click **Upgrade** (☢).



Manufacturer: Hanwha Techwin
Product type: XNO-6080R
MAC address: 00-16-6C-F9-22-6B
Firmware version: 1.13_180222 Proposed: 1.30.01 (Recommended)
Audio: Yes
SSL: No

4 In the *Upgrade firmware* dialog box that opens, do one of the following:

- If the recommended firmware is shown under the label **Upgrade to**, it means that GUS can download the firmware for you. Click **Upgrade** to start the upgrade.



Upgrade firmware

Recommendation version is **1.30.01**

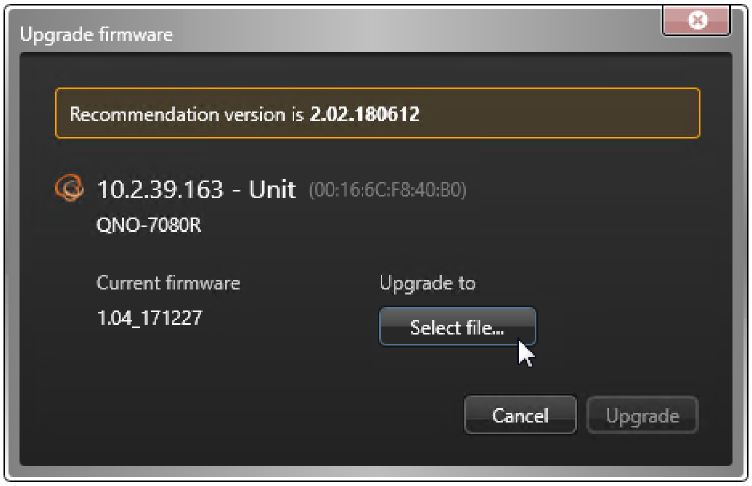
10.132.39.171 - Unit (00:16:6C:F9:22:6B)

XNO-6080R

Current firmware: 1.13_180222

Upgrade to: 1.30.01

- If the **Select file** button is displayed instead, click that button and browse to the firmware file you downloaded yourself, and click **Open** > **Upgrade**.



Upgrade firmware

Recommendation version is **2.02.180612**

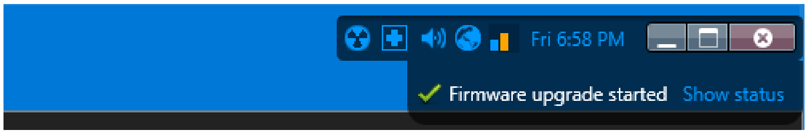
10.2.39.163 - Unit (00:16:6C:F8:40:B0)

QNO-7080R

Current firmware: 1.04_171227

Upgrade to

A message is displayed in the notification tray telling you that the firmware upgrade has started.



✓ Firmware upgrade started

When the firmware upgrade completes, the unit restarts.

After you finish

Reconfigure the units if they were reset to default settings during the upgrade.

Related Topics

Viewing unit properties on page 229

Part V

Access control

This part includes the following chapters:

32

Access control at a glance

This section includes the following topics:

About Security Center Synergis

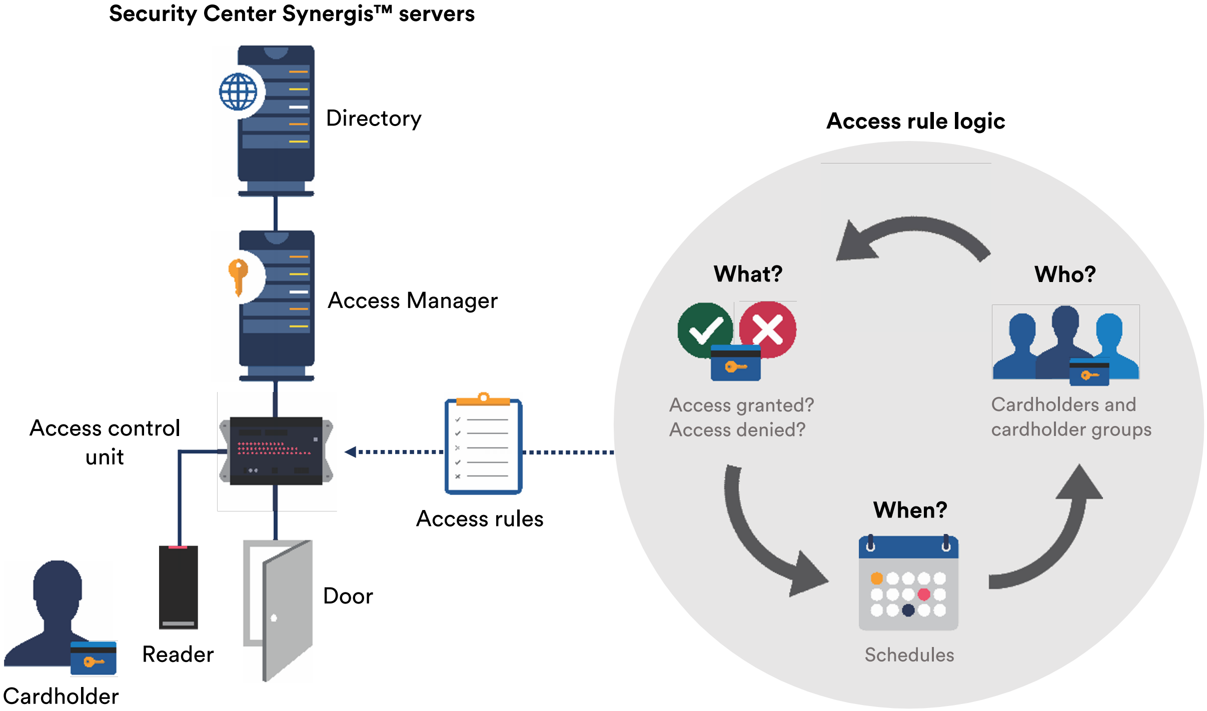
Security Center Synergis™ is the IP access control system (ACS) that heightens your organization's physical security and increases your readiness to respond to threats. Synergis™ supports an ever-growing portfolio of third-party door control hardware and electronic locks. Using Synergis™, you can leverage your existing investment in network and security equipment.

Synergis™ was designed with an open and distributed architecture. You can build your system with new IP readers or use what you already have. Integrate your access control system with other third-party systems, like intrusion or building management, and distribute Synergis server components on many different network machines to optimize bandwidth and workload.

Synergis *Enterprise* supports an unrestricted number of doors, controllers and client workstations. You can grow your system one door at a time or scale your system across multiple buildings using the Federation™ feature.

How Synergis works

Synergis architecture is based on the server role known as the *Access Manager*, which controls the physical door controllers.



The following provides a general description of how Synergis architecture works:

- System configurations are saved by the Directory role.
- The Directory pushes configurations to the Access Manager.
- Access Manager communicates directly with the physical door controllers, called access control units, over TCP/IP.
- Access Manager pushes schedules, cardholder information, and access rules to the door controllers.
- When a cardholder presents their credential to a reader, the controller refers to the access rule to determine whether the user should be granted or denied access.
- After controllers have synchronized with the Access Manager, they can operate autonomously, even if they lose the network connection to the Access Manager.

With additional configuration, a cardholder can belong to a cardholder group, a door can be part of an area, and there can be multiple schedules and rules pushed to a unit.

Benefits of Synergis

Unlike other access control solutions, Synergis does not use *clearance codes* or *access levels* to grant or deny access. Instead, the basic logic used by Synergis to grant or deny access is defined by *access rules*.

The biggest difference between an *access rule* approach and an *access level* approach is that access rules are applied to the access points of the physical locations we want to protect, whereas access levels are applied to people. Access rules specify *who* can pass through a door and *when* they can do so. An access level defines *where* and *when* a person can gain access.

An access rule contains the three W's:

- Who? (Who can pass through - *cardholders* or *cardholder groups*)
- What? (Whether access is granted or denied)
- When? (The *schedule* when the access rule is applied)

Notice that Synergis does not grant access to a card or credential. Rather, access is granted or denied based on the cardholders themselves. This subtle, but fundamental shift in the applied logic has a significant benefit in managing lost and stolen cards. The access rules that have been pushed to the door controllers do not have to be modified. If you associate a new credential with a cardholder, the old rule is still valid.

Entities related to access control

The Synergis™ access control system supports many of the entities that are available in Security Center.

Icon	Entity	Description
	Access control unit	Door controller that a reader is attached to.
	Access Manager (role)	Role that manages the door controllers in the system.
	Unit Assistant (role)	Manages system-wide operations on access control units.
	Access rule	Logic used to determine whether or not to grant access.
	Badge template	Custom-designed printing template for user credentials.
	Cardholder	Individual who has a credential.
	Cardholder group	Group of cardholders sharing common characteristics.
	Credential	Claim of identity, such as card, PIN, biometric scan, and so on.
	Door	Physical barrier controlled by an access control unit.
	Elevator	A single elevator cabin.
	Mobile Credential Manager (role)	Role that manages the mobile credentials in the system.
	Partition	Group of entities on the system visible only to a group of users.
	Schedule	Date and time range.
	Secured area	Physical location whose access is controlled by *access rules* and other access control behavior, such as antipassback, interlock, first-person rule, two-person rule, and so on.
	User	Individual who uses Security Center applications.
	User group	Group of users sharing common characteristics.

33

Access control deployment

This section includes the following topics:

Preparing to deploy your access control system

To make sure that your access control deployment goes smoothly, you need to perform a series of pre-configuration steps.

Before deploying your access control system:

1. Have a network diagram showing all public and private networks used within your organization, and their IP address ranges.

   For public networks, you also need the name and public IP address of their proxy servers. Ask your IT department for this information.

2. Install the following Security Center software components:
   a) Security Center Server software on your main server.

      The main server is the computer hosting the Directory role.

   b) (Optional) Security Center Server software on expansion servers.

      An expansion server is any other server on the system that does not host the Directory role. You can add expansion servers at any time.

   c) Security Center Client software on at least one workstation.

      For more information about installing Security Center, see the *Security Center Installation and Upgrade Guide*.

3. Have a list of *partitions* (if any).

   Partitions are used to organize your system into manageable subsystems. This is especially important in a multi-tenant environment. If, for example, you are installing one large system in a shopping center or, office tower, you might want to give local administration privileges to the tenants. By using partitions, you can group the tenants so that they can only see and manage the contents of their store or office, but not the others.

4. Have a list of all known users with their names and responsibilities.

   To save time, identify users who have the same roles and responsibilities, and organize them into user groups.

   NOTE: For large installations, users and user groups can be imported from a Windows Active Directory.

5. Install all *access control units* (door controllers and edge readers) on your company's IP network, and wire them to your doors, all the while collecting the following information:

   - Manufacturer, model, and IP address of each unit.
   - Manufacturer and model of the *interface modules* connected to each unit.
   - Login credentials (username and password) for each unit.
   - Which *access points* is each unit or interface module connected to.
   - Are the doors *Card-in/Card-out* or *Card-in/REX-out*?
   - Which inputs are connected to the door sensors, REX, and manual stations?
   - Which outputs are connected to the door locks, buzzers, our push buttons?

   TIP: A site map or floor plan showing door, elevator, controller and reader locations would be helpful.

6. Have a list of secured areas with their perimeter doors where access is controlled.

7. Have a list of all known cardholders (and cardholder groups where applicable).

   Cardholders are people who have physical access to the monitored site.

   NOTE: For large installations, cardholders can be imported from a CSV file or from a Windows Active Directory.

8. Have a list of available credentials with their facility codes and card numbers.

9. Have a list (and details) of all required schedules (office hours, holidays, and so on).

10. Have a list (and details) of all required *access rules* (*who* is allowed *where* and *when*).

11 If you are integrating Omnicast™, have a list indicating which cameras will be associated with which access points (door side and elevator floors).

   NOTE: A camera can be associated with more than one door, and vice versa.

Deploying your access control system

To integrate a variety of access control capabilities and provide end-to-end IP connectivity, you can deploy your access control system once the pre-configuration steps are completed.

Before you begin

Perform the pre-configuration steps.

What you should know

A Security Center system can be deployed with access control only (Synergis™ alone), or access control with video integration (Synergis with *Omnicast*™). It does not matter whether the video or the access control system is set up first.

NOTE: Unless otherwise specified, you can perform the following steps in any order.

To deploy your access control system:

1. Use the *Admin* account on Config Tool to connect to your system.
2. Create a partition for each independent group of entities.
   By defining the partitions first, you will not have to move entities around after you have created them.
3. To organize the entities in your system (areas, doors, and so on), configure the area view.
4. Configure the system-wide settings for access control.
5. Configure the Access Manager roles.
6. Define custom fields for your system entities.
7. Discover and enroll access control units.
   The Access Manager role needs to detect the door controllers over the IP network.
8. Configure the newly enrolled access control units and the interface modules that are attached to them.
9. Create doors and configure the wiring of the readers, sensors, locks, and so on to the access control units.
10. Create elevators and configure the wiring of the cabin reader and floor buttons to the access control units.
11. Create schedules, such as open and closed hours, holidays, and so on.
12. Create access rules and link the rules to doors and schedules.
13. Transform the areas in the area view into secured areas with access rules, perimeter doors, and advanced access control behaviors.
14. Create cardholder groups and create cardholders, and then link them to the access rules.
15. Create badge templates.
16. Create credentials.
17. Create user groups and create users.
18. Create alarms.
19. Create threat levels.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

This video shows you how to set up your Synergis access control system in Config Tool. A Mercury controller is used as an example, but the rest of the configuration applies to all manufacturers.

To learn how to add a different controller, see the *Synergis™ Softwire Integration Guide*.

After you finish

Test your configuration.

Deploying your access control system with video

Once your Omnicast™ and Synergis™ systems are available, you can integrate the two systems.

Before you begin

Do the following:

- Set up your access control system.
- Set up your Omnicast system.

To deploy your access control system with video:

1. If the Omnicast *Archiver* and the Synergis *Access Manager* are found on the same Security Center system, do the following:
   a) Assign the Omnicast cameras to your doors.
   b) Assign the Omnicast cameras to your elevators.
2. If the Omnicast Archiver and the Synergis Access Manager are found on independent systems, do the following:
   a) Federate the Omnicast cameras with your access control system.
   b) Assign the Omnicast cameras to your doors.
   c) Assign the Omnicast cameras to your elevators.

About the Access Manager role

The Access Manager role manages and monitors access control units on the system.

The Access Manager keeps the units updated with the access control settings configured in Security Center, in real-time or on a schedule, so that they can make independent access control decisions whether they are connected to the Access Manager or not.

The Access Manager also logs the access control events in the database for access control investigation and maintenance reports. All events generated by the units (access granted, access denied, door open, and so on) are forwarded by the Access Manager, through the Directory, to the concerned parties on the system.

NOTE: Starting in Security Center 5.10.2.0, events beyond a time threshold in the future do not get reported to the Access Manager role database, but warnings are shown in the Windows Event Viewer logs that these future events were filtered out.

Multiple instances of this role can be created on the system.

Configuring Access Manager roles

To monitor the units, keep them in sync with the access control settings in Security Center, and allow them to make access control decisions independently, you can configure an Access Manager to control the units.

What you should know

When Synergis™ is enabled in your license, an Access Manager role is created by default and hosted on the main server.

To configure an Access Manager role:

1 From the Config Tool home page, open the *Access control* task, and click the **Roles and units** view.

2 Select the Access Manager role to configure, and click **Resources**.

3 If necessary, configure the database required to run this Access Manager.

If you plan on setting up Access Manager failover, see Setting up role failover on page 164.

4 Click **Properties** and configure the general settings of the Access Manager.

- **Keep events:** Specify how long you want to keep the events in the Access Manager database before deleting them. The access control event are used for reporting and maintenance purposes (they include events related to doors, elevators, areas, and other access control entities).
  - **Indefinitely:** Keep the events until you manually delete them.
  - **For:** Select the number of days for the retention period.

  CAUTION: If you are using the *SQL Server 2014 Express* database engine (included with the Security Center installation files), the database size is limited to 10 GB. A door event uses (on average) 200 bytes in the database. If you configure the Access Manager to keep door events indefinitely, the database eventually reaches the 10 GB limit and the engine stops.
- **Activate peer-to-peer:** Select this option to enable the communication between Synergis units managed by this Access Manager. Up to 15 units can be connected as peers, supporting a maximum of 512 outputs and 128 inputs in I/O linking configurations.

  BEST PRACTICE: Only enable peer-to-peer communication if you plan to create I/O zones that involve multiple Synergis units, or apply antipassback to areas controlled by multiple Synergis units. Leave this option off for better system security and performance.
- **Activate global antipassback:** Select this option if you need to apply antipassback to areas controlled by multiple Synergis units. To enable this option, you must first enable peer-to-peer.

  BEST PRACTICE: If all your antipassback areas are controlled by a single unit, do not enable global antipassback. Enabling global antipassback increases the communication between Synergis units.
- **Include identifiable personal data in synchronization:** (Synergis units only) Select this option to sync cardholder names with the Synergis units. If this option is cleared (default), only credentials without personal data are synced. Enable this option when you have devices that can display cardholder names and you want them to appear.
- **Minimal cardholder synchronization:** Select this option to minimize the number of cardholders the Access Manager needs to synchronize with its units. This option is only recommended for large systems and requires following specific design guidelines. It is disabled by default.

5 If necessary, add the extensions for the access control unit types that you want this Access Manager to manage.

6 Add the access control units that you want this Access Manager to manage.

After you finish

If you need more than one Access Manager role on your system, you can create additional Access Manager roles and host them on separate servers.

Related Topics

About the Access Manager role on page 752
Creating I/O zones on page 1210
Applying antipassback to areas on page 796

Configuring access control events to have multiple source entities

You can reduce network traffic and improve system performance by reducing the number of events that the Access Manager role must send to the Directory role by enabling a feature in the *AccessManager.gconfig* configuration file. This feature is useful for large access control systems with many levels of nested areas and cardholders in multiple cardholder groups.

What you should know

- This feature is also applicable to ACaaS systems.
- By default, the feature is disabled, and each event the Access Manager sends has a single source entity. For example, when a cardholder is granted access, *Access granted* events are generated for the cardholder, the door, the area, and so on, for each related entity. Enabling the feature allows the Access Manager to generate events with multiple source entities.
- This feature is backward compatible with 5.9, 5.10.1.0, and 5.10.2.0, but not with 5.10.0.0.

  CAUTION: Before enabling the feature, ensure that none of your client workstations are using 5.10.0.0. Using 5.10.0.0 with this feature can result is events missing from the *Monitoring* task.

To configure access control events to have multiple source entities:

1. Open the *AccessManager.gconfig* configuration file in a text editor.

   The default location is *C:\Program Files (x86)\Genetec Security Center 5.x\ConfigurationFiles*.
2. Set the `EnableMultisourceEvents` attribute to `true`.

   Example: `EnableMultisourceEvents="false"`
3. Save and close the file.
4. Restart the Access Manager role:
   a) From the Config Tool home page, open the *Access control* task, and click the **Roles and units** view.
   b) Right-click the Access Manager role, and click **Maintenance** > **Deactivate role** (🚦).
   c) In the confirmation dialog box that opens, click **Continue**.
   d) Right-click the Access Manager role, and click **Maintenance** > **Activate role** (🚦).

When the role comes back online, the change is applied.

Adding access control unit extensions

For the Access Manager to communicate with access control units, you must add the manufacturer-specific extensions.

What you should know

Extensions are added by default when the Access Manager is created. However, the Genetec™ Synergis™ extension required by Synergis units is created with the default discovery port, 2000. If you configured your Synergis units with a different port number, you must also change or add it to the Access Manager.

BEST PRACTICE: If you have two or more Access Manager roles controlling Synergis units on the same subnet, make sure that they use different discovery ports. Otherwise, you might experience performance issues with your Synergis units.

To add an extension to the Access Manager:

1 Open the *Access control* task, and click the **Roles and units** view.

2 Select the Access Manager, and click the **Extensions** tab.

3 At the bottom of the extensions list, click **Add an item** (➕).

4 In the *Add extensions* dialog box, select the extension types you need and click **Add.**

NOTE: If you only selected **HID VertX**, the procedure ends here.

5 Select the Genetec Synergis extension you added.

6 To add a discovery port, click **Add an item** (➕), at the bottom of the *Discovery ports* section.

7 In the *Discovery port* dialog box, enter the port number configured for your Synergis units and click **Create**.

The port number must match the discovery port configured on your Synergis units. The default value is 2000.

8 Click **Apply.**

Related Topics

Access Manager configuration tabs on page 1306

34

Access control units

This section includes the following topics:

About access control units

An access control unit entity represents an intelligent access control device, such as a Synergis™ appliance or an HID network controller, that communicates directly with the Access Manager over an IP network. An access control unit operates autonomously when it is disconnected from the Access Manager.

Supported types of access control units

Security Center supports the following types of access control units:

- **Synergis™ appliances:** A Synergis™ appliance is an IP-ready security appliance manufactured by Genetec Inc. that is dedicated to access control functions. All Synergis™ appliances come pre-installed with Synergis™ Softwire and are enrolled as access control units in Security Center.

  There are different types of Synergis appliances:

  - Synergis™ Cloud Link
  - Legacy Synergis Cloud Link

  All Synergis appliances support a variety of third-party interface modules over IP and RS-485. For a complete list of supported interface modules and limitations, see the *Synergis™ Softwire Release Notes* and the *Synergis™ Softwire Integration Guide*.
- **HID network controllers:** The HID network controllers include the VertX EVO (V1000, V2000), Edge EVO controllers, and the legacy VertX and Edge controllers. HID controllers are intelligent IP devices that can acquire their network address automatically when your network has a DHCP server (the default). They can also be configured with static addresses (recommended).

Synergis appliances are also called *Synergis units*, and HID network controllers are called *HID units*.

About interface modules

An access control unit typically controls sub-panels, such as HID VertX-series sub-panels, and Mercury MR-series sub-panels, which in turn connect to door sensors and readers. In the case of Synergis appliances, the unit is also capable of managing other intelligent devices, such as intelligent locks and other controllers.

In Security Center, all devices directly connected to the access control unit are referred to as interface modules. An interface module is a third-party security device that communicates with an access control unit over IP or RS-485, and provides additional input, output, and reader connections to the unit.

Related Topics

HID features and models supported by Security Center on page 1489
About unit synchronization on page 759
How access control units operate on page 760
Applying antipassback to areas on page 796
About the Unit enrollment tool on page 226
About the Unit Assistant role on page 233
Viewing unit properties on page 229

About unit synchronization

Unit synchronization is the process of downloading the latest Security Center settings to an access control unit. These settings, such as access rules, cardholders, credentials, unlock schedules, and so on, are required so that the unit can make accurate and autonomous decisions in the absence of the Access Manager.

A unit is synchronized for the first time when you enroll it to your system. The Access Manager through which the unit is enrolled automatically takes care of this process. Only the settings necessary for the unit to make autonomous decisions are downloaded. When synchronizing a unit, the Access Manager knows how much memory the unit has, and fills it with as much information as it can handle.

The Access Manager roles automatically synchronizes the units assigned to it when a change is made in Security Center. For HID units, you can configure the synchronization to occur periodically, or only on request.

You can request a manual synchronization at any time if you suspect that a unit is not perfectly in sync with the system by going to the unit's **Synchronization** tab in Config Tool, and clicking **Synchronize now**.

While the unit is synchronizing, the synchronization icon (⇅) appears over the unit and the entities it controls, such as doors, elevators, and zones.

IMPORTANT: All synchronization errors are displayed in yellow. Pay attention to these errors to avoid any disruption in the operation. For example, HID VertX units are limited to 65,000 credentials. Exceeding this limit causes the synchronization to fail and the unit to reset.

Related Topics

About access control units on page 758

How access control units operate on page 760

Access control unit - HID - Synchronization tab on page 1233

Access control unit - Synergis - Synchronization tab on page 1240

How access control units operate

All access control units make autonomous decisions by default, relying on the access control settings downloaded from Security Center during unit synchronization. The unit only falls back on the Access Manager when it is presented with an unknown credential.

Online operation

The access control unit is operating online when it is connected to its Access Manager. The unit makes decisions on its own, based on the access control settings (access rules, cardholders, credentials, unlock schedules, and so on) downloaded from Security Center when it was last synchronized.

When the access control settings are changed in the system, the Access Manager automatically updates the units that are affected by the change, every 15 seconds. For HID units, you also have the option to configure the synchronization to be carried out daily, weekly, or on demand. When an unknown credential is presented, the unit immediately queries its Access Manager in order to carry out the correct decision, and thus, updates its memory at the same time.

As long as the unit remains connected to its Access Manager, it reports every decision it makes (*Access granted* and *Access denied*) and all activities (*Door opened*, *Door closed*, *Entry detected*, and so on) in real time to the Access Manager. The Access Manager can override a decision to deny access if it contradicts the current settings in Security Center.

Server mode

The server mode is a special online operation mode restricted to Synergis™ units, in which the unit allows the Access Manager (the server) to make all access control decisions. The unit must stay connected to the Access Manager at all times to operate in this mode.

NOTE: Do not enable this mode unless instructed by one of our representatives. When the unit operates in server mode, certain access control features are no longer supported.

Offline operation

The access control unit is said to operate offline when the connection to its Access Manager is lost. When operating offline, the unit appears in red in Config Tool and Security Desk.

Although offline, the unit continues to make access control decisions based on the information previously downloaded through the Access Manager during synchronization. The difference is that the Access Manager is no longer able to override any deny decisions, nor to update the unit when settings are changed in Security Center. All activities are logged locally on the unit, and are uploaded to Security Desk when the connection with the Access Manager is re-established.

Related Topics

About access control units on page 758

About unit synchronization on page 759

About minimal cardholder synchronization

Minimal cardholder synchronization is a feature designed for large systems to optimize cardholder synchronization between Access Manager roles and their access control units. When the feature is enabled, Access Manager roles take into consideration the access rules cardholders are part of before pushing their updates to their units. Without this feature, all active cardholders are synced with all access control units.

System design guidelines

To make the most out of using the minimal cardholder synchronization feature, consider the following:

- This feature is only recommended for systems with at least 250,000 active cardholders. It would not benefit smaller systems.
- Because this feature works per Access Manager role, ensure that your access control units are optimally distributed among your Access Manager roles, and that the correct access control units control your areas and doors.

  For example, if your system is used to manage sites in different cities, create one Access Manager role per city, and then add the access control units that control the doors for that city.

  BEST PRACTICE: To maximize the benefits of this feature, keep the unit type under each Access Manager role consistent.
- An access rule should only be applied to doors and elevators that are controlled by access control units managed by the same Access Manager role. Do not apply an access rule to doors that are controlled by access control units managed by different Access Manager roles.
- Do not assign the *All cardholders* cardholder group to access rules. If you use this cardholder group for your access rules, all the cardholders in your system will be synchronized to each of your access control units.

How cardholder synchronization works when this feature is disabled

All access control units have the same number of cardholders synchronized, even if the units are managed by different Access Manager roles.

- When a cardholder or its credential is modified, all access control units in your system are synchronized with the same set of cardholders. Cardholders are pushed when they meet the following criteria:
  - Their status is *Active*.
  - They have at least one active credential.
  - They are part of any access rule applied to any door or elevator, regardless of whether or not they are controlled by an access control unit managed by the Access Manager role.

How cardholder synchronization works when this feature is enabled

Only access control units that are managed by the same Access Manager role have the same number of cardholders synchronized.

- When a cardholder or its credential is modified, or when access rules, doors, elevators, and areas related to cardholders are modified, each Access Manager role synchronizes a set of cardholders to the access control units that it manages. Cardholders are pushed when they meet the following criteria:
  - Their status is *Active*.
  - They have at least one active credential.
  - They are part of an access rule applied to a door or elevator controlled by an access control unit managed by the Access Manager role.

Enabling minimal cardholder synchronization

You can minimize the number of cardholders an Access Manager role must synchronize with its access control units by enabling the **Minimal cardholder synchronization** option.

Before you begin

Apply the design guidelines recommended for minimal cardholder synchronization.

To enable the minimal cardholder synchronization feature:

1. From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.
2. Click the Access Manager role, and then click the **Properties** tab.
3. In the *Synergis™ units only* section, select the **Minimal cardholder synchronization** option.
4. Click **Apply**.
5. Restart the Access Manager role:
   a) Right-click the Access Manager role, and click **Maintenance** > **Deactivate role** (🚦).
   b) In the confirmation dialog box that opens, click **Continue**.
   c) Right-click the Access Manager role, and click **Maintenance** > **Activate role** (🚦).

When the role comes back online, the change is applied.

Changing access control unit passwords in Config Tool

For the security of your system, you should always change the unit password again after enrolling the unit. You can change the passwords of your Synergis™ units and Axis Powered by Genetec units directly from Config Tool.

Before you begin

If you need to change the passwords on a large number of units, you can update them in batches from the *Hardware inventory* task.

What you should know

IMPORTANT: If you change the password using the Unit Assistant role, do not try to change the password through the web portal later. This action is not supported.

- You need the *Update access control unit password* privilege to perform this operation.
- This procedure only applies to the following types of access control units:
  - Synergis units running Synergis™ Softwire 11.0 or later
  - Axis Powered by Genetec units

To change an access control unit password:

1 From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.

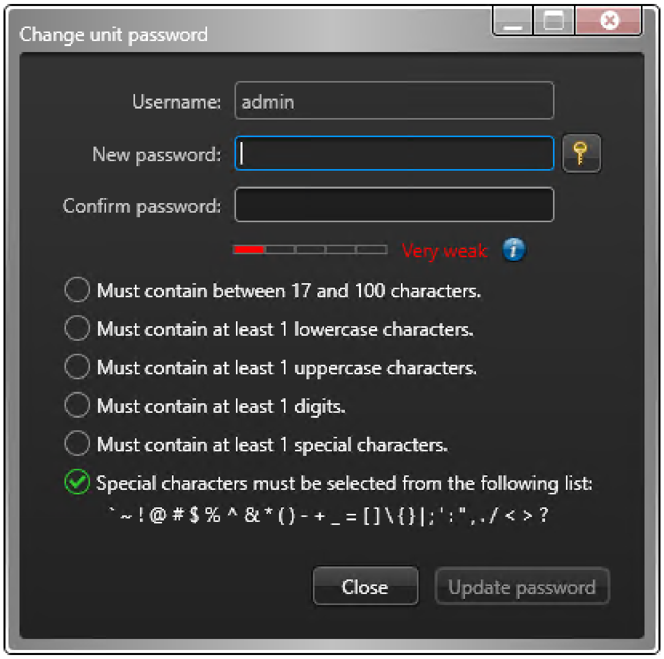
2 Select the access control unit that you want and click the **Properties** tab.

3 In the *Connection settings* section, click **Change unit password**.

4 In the *Change unit password* dialog box, do one of the following:

- (Recommended) Click **Generate secure password** (🔑) for the system to generate a secure password.
- Enter the new password manually, and then confirm it. The password must comply with the password policies that are displayed. Ensure that the password strength gauge indicates at least **Strong**.

  NOTE: Because Synergis Softwire and Security Center do not share the same password strength policies, in rare cases, it is possible for the password you enter to meet all the Security Center password strength requirements and still be rejected by Synergis Softwire.



Username: admin

New password:

Confirm password:

Very weak

○ Must contain between 17 and 100 characters.

○ Must contain at least 1 lowercase characters.

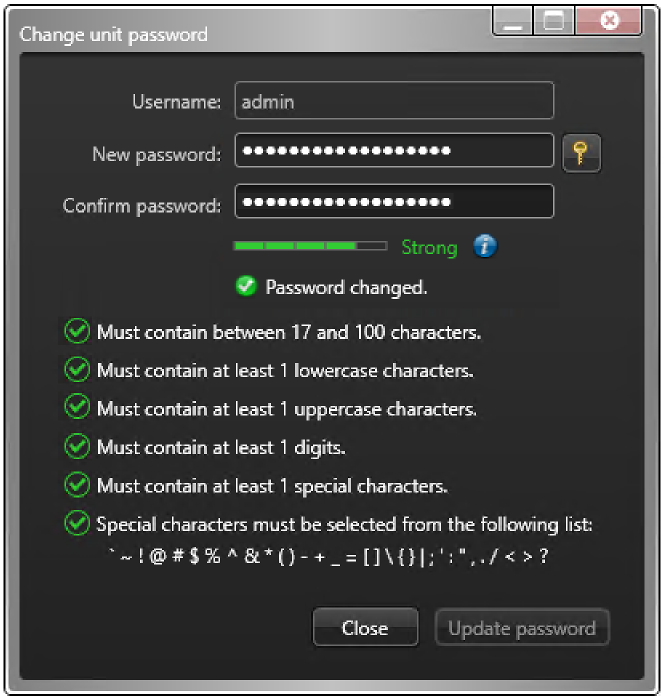
○ Must contain at least 1 uppercase characters.

○ Must contain at least 1 digits.

○ Must contain at least 1 special characters.

✓ Special characters must be selected from the following list:
` ~ ! @ # $ % ^ & * ( ) - + _ = [ ] \ { } | ; ' : " , . / < > ?

5 Click **Update password**.
If the update is successful, the message *Password changed* is displayed.



Username: admin

New password: ••••••••••••••••••

Confirm password: ••••••••••••••••••

Strong

✓ Password changed.

✓ Must contain between 17 and 100 characters.

✓ Must contain at least 1 lowercase characters.

✓ Must contain at least 1 uppercase characters.

✓ Must contain at least 1 digits.

✓ Must contain at least 1 special characters.

✓ Special characters must be selected from the following list:
` ~ ! @ # $ % ^ & * ( ) - + _ = [ ] \ { } | ; ' : " , . / < > ?

After you finish

Change more unit passwords if necessary, then export the new passwords and keep them in a safe place.

IMPORTANT: We strongly recommend that you export your passwords if they are generated by the system. If you ever delete these units from Security Center, you will not be able to connect to these units through their web portal if you do not have a copy of their passwords.

When opening the portal through the *Access control* task, you are automatically logged in to the unit if you have the *View/export unit passwords* privilege. If the portal session expires or the unit restarts, you are logged out. To log back in automatically, select a different entity from the entity tree, and then go back to the unit's *Portal* page. Switching between tabs or tasks does not reload the *Portal* page.

Related Topics

Unit password management on page 251

Viewing access control unit password history

You can view the password change history of Synergis™ unit and Axis Powered by Genetec units made through Security Center using the Unit Assistant role. You can use this information to diagnose problems that might have occurred during a password change.

What you should know

- You need the *View/export unit passwords* privilege to perform this task.
- Password history details include when a unit's password was changed, what the previous password was, and what the password was changed to. You can use this information to resolve connectivity issues by retrying old passwords.

To view access control unit password history:

1. From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.
2. Select an access control unit, and then click the **Properties** tab.
3. In the *Connection settings* section, click **Unit password history**.

   The *Unit password history* dialog box opens showing the details of the five previous password change attempts including the date, the previous password, and the new password.
4. Click **Recover password** to recover all previous passwords.

   NOTE: The **Recover password** button is only available if there is a connection issue between the unit and Security Center.

   If the Unit Assistant role is able to communicate with a password in the history, Security Center uses this password and reconnects the unit.

Updating access control unit passwords in batches

If you have a large number of Synergis™ units or Axis Powered by Genetec units in your system, you can update their passwords in batches from the *Hardware inventory* task.

Before you begin

Back up the Unit Assistant role database. It is used to store the last five password change requests of all units.

What you should know

- You need the *Update access control unit password* privilege to perform this operation.
- Always test this feature on a few units before applying it to a large batch of units of the same brand and model.

To update access control unit passwords in batches:

1. From the Config Tool homepage, open the *Hardware inventory* task.
2. Generate a *Hardware inventory* report to list the units in the report pane.
3. Ensure that the units whose password you want to update are online.
4. Select the units that you want to update and click **Update password** (🔑).

   A warning dialog box opens with the message *The password for each selected unit will be changed*.
5. Click **OK**.

   The system automatically generates a strong password for each selected unit and sends a password change request to each.
6. Confirm that the passwords have been updated by waiting a minute and then regenerating the report.

   In the **Last password change result** column, the message *Password changed successfully* is displayed.

   NOTE: You can verify the password by clicking **Show password** (👁) in the **Password** column.
7. Export the new unit passwords and keep them in a safe place.

Preparing to add HID access control units

Before you can add an HID unit in Security Center, you must know its IP address and login credentials. To find this information, you can use the *Unit enrollment* tool.

What you should know

HID VertX (V1000, V2000), and Edge devices are IP devices that can acquire their network address automatically when your network has a DHCP server. If no DHCP server is present on your network, you must assign a static IP configuration to the unit (recommended).

To change the unit's initial IP configuration if necessary, you can use the *HID Discovery GUI*. For more information about the *HID Discovery GUI*, see your HID documentation.

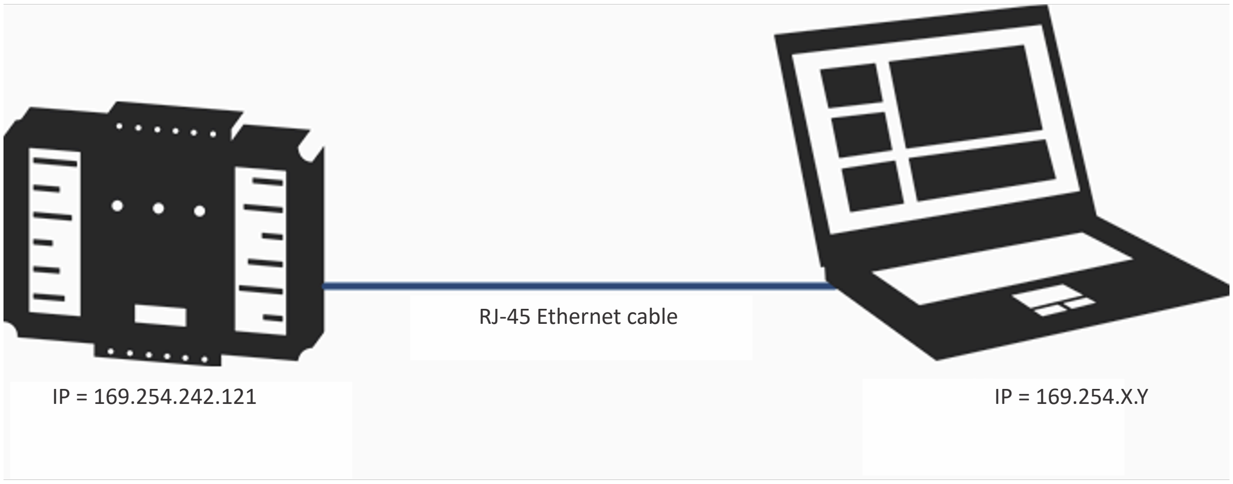
For more information about initial HID hardware setup, see the HID device documentation in the *Documentation\Controllers* folder of your Security Center installation package, or download the documentation from http://www.HIDglobal.com.

To prepare to add an HID unit in Security Center:

1 Discover the access control units on your network.

2 If the HID unit you want is not found, disconnect your workstation's network cable and plug it directly into the HID unit. For PoE units, such as Edge or Edge EVO, connect your laptop and unit to a standalone switch.

The address 169.254.242.121 is the factory-assigned default address for every HID device. Even if the unit has been configured with an IP configuration, it still listens on this address for possible troubleshooting needs.



3 Type *http://169.254.242.121* in your web browser.

4 To log on, enter the default username (root) and password (pass).

NOTE: The web interface for EVO units can only be accessed with the *admin* account. By default, the password is blank. Change it after changing the IP settings. To enroll the unit into Security Center, you must use root/pass.

5 On the *Basic Setup* page, assign the device's IP configuration.

CAUTION: If no DNS server is present on your network, you must use the unit's own *IP address* for the **Primary DNS Server** value, and the **Basic Central Station**'s IP address should be set to the IP address of your Security Center server running the *Access Manager* role.

6 (Optional) Click **Change Login Password**, and then change the password.
  Changing the password applies to the *admin* user not the *root* user.

7 Click **Submit**.

The new IP configuration is applied to the unit and it restarts. You can now add the unit in Security Center.

Adding HID access control units

To control access in your system, and monitor access control-related events in Security Center, you must add access control units to an Access Manager.

Before you begin

- Add the extensions for the access control unit.
- The HID units you plan to add must be online, and you must know their IP addresses and login credentials (username and password).

What you should know

This section only covers adding HID units. For information about adding Synergis units, see the *Synergis™ Appliance Configuration Guide*.

To add an HID unit:

1. Open the *Access control* task, and click the **Roles and units** view.
2. Click **Access control unit** (+).
3. From the **Network endpoint** list in the *Unit information* page, select the Access Manager that will manage the unit.
4. Click **Unit type** and select **HID VertX**.

   If the HID VertX unit type is not available, it means that the extension has not been added in the Access Manager.
5. Enter the IP address of the HID unit.
6. Verify that the **Secure mode** option is enabled.

   Enabling secure mode disables the insecure protocols FTP and Telnet. It also makes the connection between the Access Manager and HID units less susceptible to network impairments. Ensure that your HID unit meets the minimum supported firmware specified on that page. If not, the enrollment will fail. HID Legacy units cannot be added with secure mode enabled on Windows 10 or Windows Server 2016 and later; SSL 3.0 (RC4 cipher) is disabled by default on these Windows operating system versions.

   NOTE: As of Security Center 5.8, HID EVO units running firmware version 3.7.0.108 or later in secure mode communicate with the Access Manager using TLS 1.2 encryption and need port 4433 to be open instead of port 4050. HID units running an earlier firmware version communicate with the Access Manager using HID encryption.
7. Enter the **Username** and **Password**.

   NOTE: If secure mode is enabled, you must provide the admin password. If secure mode is not enabled, you must provide the root password (the default root password is pass).
8. If there is an NAT router between the unit and its Access Manager, select **Use translated host address** and specify the NAT router IP address that is visible from the unit.
9. Click **Next**.
10. Review the *Creation summary*, and click **Create**.

    The Access Manager attempts to connect to the unit and enrolls it in your system. When the process is successfully completed, a confirmation message appears.
11. Click **Close**.

    The newly added access control unit appears under the Access Manager it was assigned to in the **Roles and units** view.

    NOTE: It might take a few minutes before the unit can be used, as it undergoes automatic synchronization. This process involves the Access Manager sending schedules, access rules, and cardholder information to the unit. The unit saves the information locally so that it can operate even if the Access Manager is unavailable.

12 Confirm that the unit successfully synchronized with Access Manager:
   a) Click the **Roles and units** view, and select the access control unit that was added.
   b) Click the **Synchronization** tab, and check the date and time of the **Last update**.

Configuring access control unit settings

For optimal performance, configure your access control unit settings after they have been added in Security Center.

What you should know

Security Center provides default settings; however, it is recommended that you carefully go through the configuration of each entity in order to get the best results.

HID and Synergis™ units have different capabilities, therefore different configuration requirements. For information about configuration requirements for Synergis units, see the *Synergis™ Appliance Configuration Guide*.

TIP: To save time configuring your access control units, you can configure one, and then copy the settings they have in common to the rest of the units.

To configure an access control unit's settings:

1. Open the *Access control* task, and click the **Roles and units** view.
2. Select the access control unit (HID or Synergis) to configure, and click the **Properties** tab.
3. In the **Properties** tab, do one of the following:
    - Configure the properties of the HID unit.
    - Configure the properties of the Synergis unit.
4. Configure the wiring of entities controlled by this unit:
    - Configure the wiring of doors.
    - Configure the wiring of elevator floors.
    - Configure the wiring of hardware zones.
5. Click the **Peripherals** tab of the access control unit.

    This is where you configure the properties of the peripherals attached to the unit, such as the reader type and the input contact type. Validate your wiring configuration and give meaningful names to the devices if necessary.

    - Configure the peripherals attached to the HID unit.
    - Configure the peripherals attached to the Synergis unit.
6. (HID units only) Select the **Synchronization** tab, and choose how often you want to synchronize the unit:
    - **Automatically:** This is the recommended setting.

        Any configuration change is sent to the access control unit 15 seconds after the change is saved by the Config Tool, Web Client, Genetec Web App, or Security Desk. Only configurations that affect that particular unit are sent.
    - **Daily:** The unit is synchronized daily, at the specified times.
    - **Every:** The unit is synchronized weekly, at the specified day and time.
    - **Manual:** The unit is only synchronized when you click **Synchronize now**.

        Make sure you synchronize the unit before the configuration expires.
7. Click **Apply**.

Related Topics

Enabling reader supervision on HID VertX controllers on page 773

Resetting the trusted certificate

If the Access Manager cannot connect to a previously enrolled Synergis™ unit because the certificate that the Access Manager trusts has been changed, you can reset it in Config Tool so the new certificate can be accepted.

What you should know

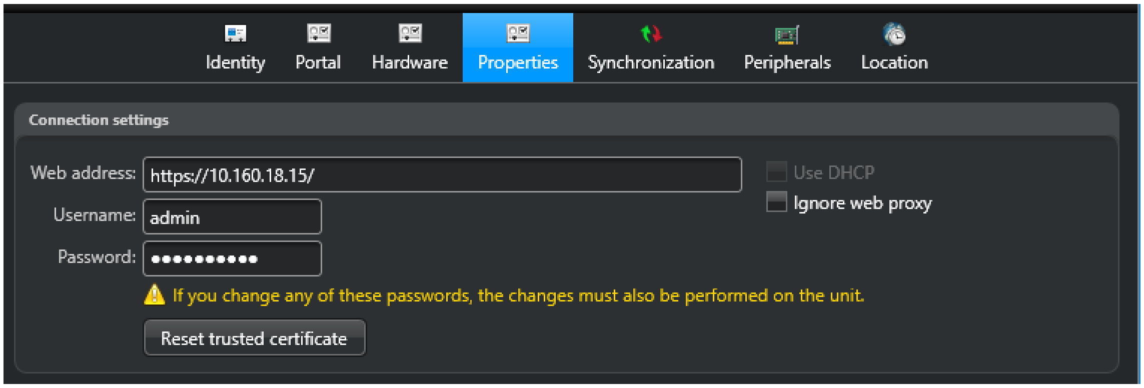
There are two legitimate cases where the unit might change its certificate after being enrolled in the Access Manager:

- When you install a CA-signed on the unit after the unit has been enrolled.
- When the unit is an SV appliance, and you upgraded the Security Center software on the appliance. A new certificate might be installed because the SV appliance also acts as a Security Center server.

To reset a unit certificate trusted by an Access Manager:

1 From the Config Tool home page, open the *Access control* task, and click the **Roles and units** view.

2 Select the unit that the Access Manager cannot connect to (displayed in red ■), and click **Properties**.



Connection settings

Web address: https://10.160.18.15/

Username: admin

Password: ●●●●●●●●●●

□ Use DHCP

□ Ignore web proxy

⚠ If you change any of these passwords, the changes must also be performed on the unit.

3 Click **Reset trusted certificate**.

Enabling reader supervision on HID VertX controllers

To be able to monitor readers going offline on doors controlled by HID units in Security Desk and Config Tool, you must enable reader supervision on the HID unit in Config Tool and present the HID configuration card to each reader.

Before you begin

Make sure you have at your disposal the HID configuration cards for Wiegand readers. For example, for iCLASS SE readers, the configuration cards would be:

- SEC9X-CRD-0-043J to enable supervision
- SEC9X-CRD-0-0000 to disable supervision

What you should know

In Security Desk, you get the *Door offline: Device is offline* event on a door when one of the readers associated to that door has gone offline.

TIP: The *Door offline: Device is offline* event is triggered by both unit disconnections and reader disconnections. Therefore, you cannot tell which is which unless you also monitor the access control units. If you have two readers on a door, you must go to Config Tool and check the *Peripherals* page to find out which reader is offline.

To enable reader supervision on an HID VertX unit:

1. From the Config Tool home page, open the *Access control* task, and click the **Roles and units** view.
2. Select the HID unit you want to modify and click the **Properties** tab.
3. Under the *General settings* section, select **Reader supervision**.

   All readers connected to this HID unit must be configured for supervision.
4. Set the **Timeout** used to detect that the reader is offline.

   We recommend that you set the timeout value to be at least three times the cycle time of the *I'm alive* signal (default=10 seconds) configured on the reader.
5. Click **Apply**.
6. Configure each physical reader for supervision.
   a) Power cycle the reader.
   b) On power up, when the reader LED is purple, present and hold the HID configuration card to the reader until the reader stops beeping.
   c) Repeat the same process for each reader connected to the HID unit.

To disable reader supervision on an HID VertX unit:

1. In the unit's *Properties* page, clear **Reader supervision** and click **Apply**.
2. Disable supervision from each physical reader by presenting the second card.

Enabling external access control devices

You can enable and disable external access control devices, such as USB readers, signature pads, card scanners, and so on, from the *Options* dialog box.

What you should know

These settings are saved locally for your Windows user profile. For information about the access control devices available, see your manufacturer documentation.

To enable or disable external access control devices:

1. From the homepage, click **Options** > **External devices**.
2. Next to each external device, set the option **ON** or **OFF**.
3. Click **Save**.
4. Restart your application.

Related Topics

Setting up smart card encoding stations on page 831

Using signature pads on page 835

35

Areas, doors, and elevators

This section includes the following topics:

About doors

A door entity represents a physical barrier. Often, this is an actual door but it could also be a gate, a turnstile, or any other controllable barrier. Each door has two sides, named *In* and *Out* by default. Each side is an access point (entrance or exit) to a secured area.

There are three basic door configurations:

- **Card In/Card Out:** Two readers are required.
- **Card In/REX Out:** One reader is required.
- **Readerless doors:** No readers are required.

Readerless doors

If a reader is not required for a door configuration, the I/Os on the interface modules, such as HID VertX V200 and V300, can be used to control the REX, door sensor, and door lock. You do not need to link access rules to a readerless door, but you can still assign unlock schedules to readerless doors.

The following are examples of where readerless doors might be used:

- **Fire exits:** Locked from the outside, with a push-bar to open the door from the inside using a REX.
- **Stadiums, theaters, arenas:** Everyone must enter through the ticket booth but once the event is finished, many exits become available to decrease congestion at the main entrance.

Door wiring

It is a best practice to have an electrician verify the functionality between all door sensors and actuators.

Door buzzers

You can assign an access control unit output to sound a buzzer from the door *Hardware* page. The buzzer does not refer to the reader’s beeper, but an external buzzer that is wired to an output relay on the access control unit. The buzzer output is triggered by the *Sound buzzer* and *Silence buzzer* actions.

Entry sensors

You can configure an entry sensor on each side of a door to increase the accuracy of people counting and the application of advanced access restriction rules on areas, such as antipassback and first-person-in rule. The system can only generate the *Entry detected* event when an entry sensor is triggered. In the absence of an entry sensor, the door sensor is used, and entry is assumed when the door sensor is triggered. If both types of sensors are absent, entry is assumed when an access is granted.

Lock sensors

You can configure a lock sensor alongside a door sensor and a door lock to monitor when the lock is in an *unsecured* state (⚠). When the three are configured, the system can generate the *Door unsecured* event if the following occurs:

- The door sensor indicates the door is closed, and the door lock indicates the door is locked, but the lock sensor indicates the door is unlocked.
- The *Door forced open* event is generated.
- The *Door open too long* event is generated.

Two-person rule

You can protect a highly secured area with the *two-person rule*. The two-person rule is the access restriction placed on a door that requires two cardholders (including visitors) to present their credentials within a certain delay of each other in order to gain access.

NOTE: A visitor that requires a host cannot be counted as one of the two people in the two-person rule.

TIP: A door can be configured in Security Center to protect a physical area (a room) without necessarily configuring a secured area if no other types of access restrictions need to be enforced.

Related Topics

About secured areas on page 792

About door templates

A door template defines the wiring for a specific door configuration, which simplifies and accelerates the door creation process by eliminating the need to manually map the physical wiring for a door entity.

Included templates

Door templates are available in the Config Tool door creation wizard for the following interface modules:

- ASSA ABLOY Aperio
- ASSA ABLOY Corbin Russwin
- ASSA ABLOY Persona
- ASSA ABLOY Sargent
- AXIS A1001
- HID Edge Evo
- Honeywell PW5K1R1
- Honeywell PW5K1R2
- Honeywell PW6K1R2
- Mercury EP1502
- Mercury LP1502
- Mercury MR50
- Mercury MR51e
- Mercury MR52
- Mercury MR62e
- Schlage AD300
- Schlage AD400
- Schlage Engage
- SimonsVoss Cylinder
- SimonsVoss Cylinder With Inputs
- SimonsVoss Padlock
- SimonsVoss Smart Handle
- SimonsVoss Smart Handle With Inputs
- Synergis IX Controller CTRL DIN
- Synergis IX Controller CTRL DIN 1D
- Synergis IX Reader Expander RDM2 DIN
- VertX V100

Example

Selecting **VertX V100** as your interface module gives you two configuration options:

- **Card in, Card Out:** Selecting this template automatically defines the following hardware mapping:
  - Door side In reader: Reader 1
  - Door side Out reader: Reader 2
  - Door lock: Reader 1 - Output DoorStrikeRelay
  - Door sensor: Reader 1 - Input DoorSwitch
- **Card In, REX:** Selecting this template for the same configuration results in the following mapping:

- Door side In reader: Reader 1
- Door side Out Request to exit: Reader 1 - Input RexSwitch
- Door lock: Reader 1 - Output DoorStrikeRelay
- Door sensor: Reader 1 - Input DoorSwitch

Custom templates

If there is no door template in Config Tool for the configuration you want, you can create custom templates using the Security Center SDK. You can contact us for help developing door templates:

- Contact our Custom Solutions department through your sales representative for a quote
- Call one of our regional offices around the world.
- Visit our website at www.genetec.com.

Related Topics

Creating doors on page 780

Creating doors

When the doors and access control units are physically wired, you can create and configure the door entity in Config Tool.

Before you begin

Wire your doors to access the control units.

To create a door:

1 From the Config Tool home page, open the *Area view* task.

2 Select the area where you want to add the door.

3 Click **Add an entity** (➕) > **Door**.

4 In the *Creating a door* wizard, enter the door name and description.

5 From the **Location** list, select the area in which the door belongs, and click **Next**.

6 In the *Door information* page, assign names to the door sides.
Example: In/Out, Secure/Non-secure, Entrance/Exit, East/West.

7 Associate the door with the access control unit it is wired to:
   a) From the **Access control unit** list, select a unit.
   b) From the **Interface module** list, select an interface module.
   c) (Optional) from the **Door template** list, select a template.
   NOTE: Security Center includes templates for most popular configurations; you can also create custom templates using the Security Center SDK.

8 Click **Next**.

9 Review the *Summary* page, and click **Create** > **Close**.
The new door appears in the area view's *entity tree*.

10 Select the door and click the **Properties** tab.

11 Configure the general access control behavior of the door.

12 Click **Apply**.

13 Describe the wiring between the access control unit and the door to Security Center.

14 Select who has access to the door.

After you finish

Link the door to the areas it secures.

Related Topics

About doors on page 776
About door templates on page 778

Mapping door entities to physical door wiring

For your door entity to be functional, you must match the hardware wiring you made to the door (reader connections, door locks, door sensors, REX's, buzzers, and so on) in Security Center, so the Access Manager knows how to control the door.

What you should know

The way you wire your door and assign the hardware interfaces affects how the door can be secured and monitored. For example, if the door has an entry sensor, you can monitor *Door forced open* and *Entry detected* events. If a door side is configured with an REX, access rules cannot be applied to that door side.

IMPORTANT: The door's hardware configuration must correspond to the I/O configuration you set for the access control unit controlling the door.

To map the physical wiring of a door to a door entity:

1. From the Config Tool home page, open the *Area view* task.
2. Select the door entity to configure, and click the **Hardware** tab.
3. From the **Preferred unit** list, select the access control unit that is connected to the door.
4. In the *Door side (In)* section, select the **Reader**, **Request to exit**, and **Entry sensor** from the drop-down lists, based on the door wiring.
5. To change the door reader settings, click **Reader settings** (✏), configure the following, and then click **Save**:
   - **PIN entry timeout:** This sets the entry timeout for the PIN after the card has been read. For example, by default, you have 5 seconds to enter all the PIN digits.
   - **Use card and PIN:** Turn on the option to change the reader mode to *Card and PIN* and use the **Schedule** list to select when this mode applies. When not in a scheduled time period, the reader behaves in either *Card only* or *Card or PIN* mode, depending on the unit-wide parameters configured in the portal of the Synergis unit.

   NOTE: Make sure your settings match the capabilities of your reader. The system cannot validate the capabilities of your hardware. You can configure this type of reader on the unit's *Peripherals* page.
6. Repeat the steps for the *Door side (Out)* section.
7. In the *Additional connections* section, assign the inputs and outputs for the buzzer, door lock, lock sensor, and so on.
8. Click **Apply**.
9. Assign cameras that display each side of the door to the door entity.

Example

If a physical door has the following installed, then the door entity must have a Card In/REX Out configuration in Config Tool:

- A reader wired on Door side In
- An REX wired on Door side Out
- A strike relay on the door lock
- A door sensor
- An auxiliary relay wired to a buzzer

Related Topics

Access control unit - HID - Peripherals tab on page 1234

Access control unit - Synergis - Peripherals tab on page 1241

Assigning cameras to local doors

To display camera feeds in the Security Desk *Monitoring* task, you can assign local and federated cameras to local door entities. This allows Security Desk operators to monitor door events, such as *Door forced* or *Access denied*.

Before you begin

To monitor doors with cameras, you must have one of the following Security Center configurations:

- An Archiver role with available cameras
- An Omnicast™ Federation™ role that can connect to an external Omnicast system
- A Security Center Federation™ role that can connect to an external Security Center system with cameras

What you should know

- If multiple cameras are associated with a door, it creates a *composite entity* where cameras linked to side (A) display in a Security Desk tile. You can cycle through or unpack a composite entity in Security Desk.
- If a video file is unavailable, a video request returns the video file that is closest to the requested time stamp.
- If the playback video associated with an access control event is no longer available, the next available video recorded closest to the time of the event is displayed instead.

To assign cameras to a local door:

1. From the Config Tool homepage, open the *Area view* task.
2. Select the door entity to configure, and click the **Hardware** tab.
3. In the *Door side (In)* section, click **Associate a camera** (➕).
4. From the **Camera** list, select a camera.

   If the camera has a PTZ motor, you can also include the PTZ preset number to ensure that the camera points towards the door.
5. To assign another camera to the door side, click **Associate a camera** (➕) again.
6. Repeat the steps for *Door side (Out)*.
7. Click **Apply**.

Assigning local cameras to federated doors

To display camera feeds in the Security Desk *Monitoring* task, you can assign local cameras to federated doors. This allows Security Desk operators to monitor door events, such as *Door forced* or *Access denied*.

Before you begin

To monitor federated doors with local cameras, you must have the following Security Center configurations:

- An Archiver role with available cameras
- A Security Center Federation™ role that can connect to an external Security Center system with doors

What you should know

- Assigning a local camera to a federated door creates a relationship between them in the local system. The camera is not shared with the federated system.
- The local camera is assigned to both sides of the federated door. You cannot assign the camera to a specific *door side*.

To assign local cameras to a federated door:

1. From the Config Tool homepage, open the *Area view* task.
2. Expand the Security Center Federation™ role (), and select the federated door.
3. Click and drag the local camera to the federated door.

   The local camera and federated door are now related.

   TIP: To select multiple cameras, hold Ctrl or Shift while clicking.

Configuring doors with lock sensors

To monitor whether or not your doors have locked correctly, you must configure additional connections for your door entities.

What you should know

If you have a door lock configured without a lock sensor, the door lock only indicates the intended lock state, not the physical lock state. To receive the *Door unsecured* and *Door secured* events, a door lock and door sensor must be configured alongside the lock sensor.

To configure a door with a lock sensor:

1. From the Config Tool home page, open the *Area view* task.
2. Select the door entity to configure, and click the **Hardware** tab.
3. Map the physical wiring of a door to a door entity.
4. In the *Additional connections* section, assign the output for the **Door lock**.
5. Assign the input for the **Door sensor**.
6. Click **Add connection** (+), and select **Lock sensor**.
7. Assign the input for the **Lock sensor**.
8. Click **Apply**.

Selecting who has access to doors

A door that is wired to an access control unit is locked by default. You can set schedules for when *free access* (unlocked) through the door is permitted, and when *controlled access* (credentials must be presented to unlock the door) is in effect, by applying access rules.

Before you begin

- Describe the wiring between the access control unit and the door to Security Center.
- Create the access rules.

What you should know

If the door is configured as an access point to a secured area, all access rules assigned to the area are applied to the door. If additional access restrictions are enforced on the area, they are applied to the door as well.

To select who has access to a door:

1. From the Config Tool home page, open the *Area view* task.
2. Select the door entity, and click the **Unlock schedules** tab.
3. Under the *Unlock schedules* section, click **Add an item** (➕).
4. Select the schedules that you want apply free access periods to, and click **Select**.

   Example: A typical use of an unlock schedule might be the following: The main door of the office should be unlocked from 9:00 am-12:00 pm, locked from 12:00 pm - 1:00 pm, and unlocked again from 1:00 pm - 6:00 pm.
5. Under the *Exceptions to unlock schedules* section, click **Add an item** (➕).
6. Select the schedules that you want to apply controlled access periods and access rules to, and click **Select**.
7. Click **Apply**, and then click the **Access rules** tab.

   BEST PRACTICE: If all the perimeter doors around the area share the same access rules, associate these access rules to the area instead of the doors.
8. In the **Door access applies to** option, select whether the access rules for the controlled access periods apply to **Both sides** or **Individual sides** of the door.

   NOTE: If the door is only configured with one reader, you can only configure access rules for the side where the reader is configured.
9. Under the *Access rules* section, click **Add an item** (➕), select access rules (and cardholders), and then click **OK**.

   If you assign cardholders or cardholder groups directly to the door, the cardholders are granted access at all times.
10. If the access rules are specific to each door side, then set access rules for the other door side.
11. Click **Apply**.

Related Topics

HID I/O linking considerations on page 1487

About double-badge activation on page 809

About elevators

An elevator is an entity that provides access control properties to elevators. For an elevator, each floor is considered an access point.

When a cardholder uses a credential, the floor buttons to access those floors for which that cardholder is authorized, are enabled. This is achieved by controlling an output relay to enable the floor button.

Floor tracking is achieved by monitoring inputs, which records the floor buttons that are pressed. This permits tracking reports for elevator usage in the Security Desk.

Hardware required for elevator control and floor tracking

To control access to an elevator, you require the following:

- An *access control unit*.

  NOTE: Only Synergis™ units are supported for new installations. For more information, see the *Synergis™ Softwire Integration Guide*.
- A reader in the elevator cab.
- Outputs that close relay contacts to enable the floor buttons.
- Inputs that record the floor buttons that have been selected (only necessary when floor tracking is required).
- *Interface modules* supplying or connecting the above hardware to the access control unit.

Reader modes

The following reader settings can be applied to the elevator cabin reader:

- Card only
- Card or PIN
- Card and PIN
- Card and PIN on a schedule

Elevator-wide settings

The following elevator-wide settings can be configured:

- **Grant time:** This value indicates for how long the elevator floor buttons stay enabled after the access has been granted.
- **Output relay state for free access:** There are two possible choices: (1) *Normal*, means floor access is enabled when the access control unit output relay is de-energized; (2) *Active*, means floor access is enabled when the access control unit output relay is energized.

Limitations

- An elevator (both the cabin reader and the I/Os) must be controlled by a single access control unit.
- *Antipassback*, *interlock*, and *people counting* do not work with elevators.
- Minimum *security clearance* cannot be enforced on elevators.

Creating elevators

To control access and monitor access control events related to elevators, you must create elevator entities in Security Center.

Before you begin

Make sure you have all the hardware required to control the elevator, installed the reader in the elevator cab, and wired the reader to the interface module connected to the access control unit.

To create an elevator:

1. From the Config Tool home page, open the *Area view* task.
2. Click **Add an entity** (➕) > **Elevator**.
3. In the elevator creation wizard, enter the elevator name and description.
4. From the **Location** list, select the area in which the elevator will be created, and click **Next**.

   NOTE: Unlike doors, elevators are not treated as *access points* to areas. Nevertheless, each elevator floor is an access point on its own.
5. Enter the number of elevator floors, and click **Create**.

   The default floor entities are created.
6. To change a floor name, select the floor, and enter a new name.
7. Make adjustments if necessary, and click **Next**.
8. Review the *Creation summary*, and click **Create** > **Close.**

   The new elevator appears in the area view with its floors. It initially appears in red until it is fully configured.
9. Select the output relay settings for the elevator floor.

   The output relay settings affect how you will wire the unit.
10. Describe the physical wiring between the access control unit and the elevator to Security Center.
11. Select who has access to the elevator floors.

Selecting output relay behavior for elevator floors

Before you can finish wiring your elevator, you must configure the unit output relay settings.

Before you begin

Create the elevator entity in Security Center.

What you should know

The output relay settings affect how you will wire the units. You must use the appropriate NO or NC relay contacts on the units, based on the settings you select in Security Center.

To select the output relay behavior for an elevator floor:

1 From the Config Tool home page, open the *Area view* task.

2 Select the elevator to configure, and click the **Advanced** tab.

3 In the **Grant time** option, select how long the elevator floor buttons stay enabled for after an access has been granted.

4 In the **Free access when the output relay is** option, select what the relay state must be for free access to be granted:

- **Normal:** Floor access is enabled when the access control unit output relay is de-energized. This means that a power loss results in free access to the floor.
- **Active:** Floor access is enabled when the access control unit output relay is energized. This mean that a power loss results in floor access being denied.

5 Click **Apply**.

After you finish

Finish wiring the elevator floors according to the relay settings you specified and map your wiring to the elevator entity.

Mapping elevator entities to physical elevator floor wiring

For your elevator entity to be functional, you must match the hardware wiring you made to the elevator in Security Center, so the Access Manager knows how to control the elevator.

To map the physical wiring of an elevator floor to an elevator entity:

1. From the Config Tool home page, open the *Area view* task.
2. Select the elevator entity to configure, and click the **Floors** tab.
3. From **Preferred unit** list, select an access control unit that is connected to the elevator cab reader.
4. From the **Elevator cabin reader** drop-down list, assign the reader input.
5. To change the elevator cab’s reader settings, click **Reader settings** (✎) and set the following options:

   NOTE: Make sure your settings match the capabilities of your reader. The system cannot validate the capabilities of your hardware. You can configure this type of reader on the unit's *Peripherals* page.

   - **PIN entry timeout:** This sets the entry timeout for the PIN after the card has been read. For example, by default, you have 5 seconds to enter all the PIN digits.
   - **Use card and PIN:** Turn on the option to change the reader mode to *Card and PIN* and use the **Schedule** list to select when this mode applies. When not in a scheduled time period, the reader behaves in either *Card only* or *Card or PIN* mode, depending on the unit-wide parameters configured in the portal of the Synergis unit.
6. Under the **Floors** section, use the following buttons to add elevator floors or change their configuration:

   - To add an elevator floor, click ➕.
   - To delete the selected elevator floor, click ✖.
   - To move the selected elevator floor up, click ▲.
   - To move the selected elevator floor down, click ▼.
   - To modify the selected elevator floor, click ✎.

   The *Floor properties* dialog box lets you do the following:

   - Change the floor name.
   - Assign an output relay to the push button corresponding to that floor.

     Use the appropriate NO or NC relay contacts on the unit, according to output relay settings configured in the **Advanced** tab.

     NOTE: The output relay state can be inverted according to your regulatory requirements.
   - (Optional) Assign an input for floor tracking.

   NOTE: On an access control unit dedicated to elevator control, all inputs can be used for floor tracking except for the door monitor inputs.
7. Assign cameras to the elevator cabin and to each elevator floor.
8. Click **Apply**.

Related Topics

Access control unit - HID - Peripherals tab on page 1234

Access control unit - Synergis - Peripherals tab on page 1241

Assigning cameras to elevators

To display a camera feed in a Security Desk monitoring tile when an elevator event occurs, such as *Floor accessed* or *Access denied*, you can assign cameras to elevator entities.

Before you begin

To monitor elevators with cameras, you must have one of the following Security Center configurations:

- An Archiver role with available cameras.
- An Omnicast™ Federation™ role to connect to an external Omnicast system.
- A Security Center Federation™ role to connect to an external Security Center system with cameras.

To assign cameras to an elevator:

1 From the Config Tool home page, open the *Area view* task.

2 Select the elevator entity to configure, and click the **Floors** tab.

3 In the *Cabin* section, click **Associate a camera** (✚).

4 From the **Camera** list, select a camera.

If the camera has a PTZ motor, you can also include the PTZ preset number to ensure that the camera points towards the elevator.

5 To add another camera to the elevator, click **Associate a camera** (✚) again.

6 To assign a camera to each elevator floor:

a) In the **Floors** section, select a floor and click **Edit the item** (✎).

b) In the *Floor properties* dialog box, click **Associate a camera** (✚).

c) From the **Camera** list, select a camera.

d) Click **OK**.

e) Repeat the steps for all elevator floors.

7 Click **Apply**.

Selecting who has access to elevators

You can set schedules for when access to an elevator is controlled, and who can access the elevator with their credentials when access is controlled by applying access rules.

Before you begin

Create the access rules.

What you should know

Just like a door, elevator control requires access rules to determine *who* will be granted access, *where* and *when*. You can also assign unlock schedules to allow *free access* (no credentials required) during certain periods.

To select who has access to an elevator floor:

1. From the Config Tool home page, open the *Area view* task.
2. Select the elevator entity, and click the **Access** tab.
3. Under the *Access rules* section, click **Add an item** (➕).
4. Select the access rules to apply to the elevator, and click **Select**.

   The access rules determine which cardholders can access the elevator and when.
5. For each access rule, click the **Floor** list, and select which floor the access rule applies to.
6. Under the *Exceptions* section, click **Add an item** (➕).
7. Select the schedules that you want apply exceptions to, and click **Select**.
8. From the **Floor** column drop-down list, select which floors the exception applies to.
9. From the **Mode** column drop-down list, select whether the elevator has free access or controlled access during the exception schedule.
   - **Free access:** Cardholders do not require a credential to access the elevator, and no access rules apply.
   - **Controlled access:** Cardholders require a credential to access the elevator, and access rules apply.
10. Click **Apply**.

Related Topics

HID I/O linking considerations on page 1487

Best practices for configuring exceptions to controlled access

Elevators are in controlled access mode by default. Therefore, the best practice is to start with an unlock schedule that tells when the elevator should be in free access mode (unlocked). Consequently, any non-selected time in the schedule sets the elevator in controlled access mode.

When schedules overlap, the controlled access schedules have priority over the unlock (free access) schedules. A controlled exception schedule is only useful if there is at least one unlock exception schedule.

About secured areas

A secured area is an area entity that represents a physical location where access is controlled. A secured area consists of perimeter doors (doors used to enter and exit the area) and access restrictions (rules governing the access to the area).

In the presence of a threat, access to secured areas can either be restricted to keep the danger out, or relaxed to allow people to get away from danger by activating *threat levels*.

You can configure the following access restrictions on a secured area:

- Access rules
- Antipassback
- Interlock
- First-person-in rule
- Visitor escort rule

Access rights

The basic access restrictions to an area are defined by granting access to specific cardholders (who can access this area and when). When nothing is configured, no one is allowed to enter or exit the area. Access rights can be granted through access rules (recommended approach) if it is constrained by a schedule, or directly to cardholders, if there is no schedule constraint. Access rights can be granted on the entire area, or individually to each access point of the area.

Antipassback

Antipassback is an access restriction placed on a secured area that prevents a cardholder from entering an area that they have not yet exited from, and vice versa. When access is denied due to an antipassback violation, the violation must be "*forgiven*" in Security Desk for the cardholder to unlock the door. The antipassback event might be forgiven automatically after a period of time if it is configured with a timeout value.

NOTE: HID units support antipassback *or* interlock, but not both simultaneously.

Interlock

An interlock (also known as sally port or airlock) is an access restriction placed on a secured area that permits only one perimeter door to be open at any given time. This is typically used in a passageway with at least two doors. The cardholder unlocks the first door, enters the passageway, but cannot unlock the second door until the first door is closed.

For interlock logic to work, the door sensors must be able to detect when the door is opened.

NOTE: HID units support antipassback *or* interlock, but not both simultaneously.

First-person-in rule

The first-person-in rule is the additional access restriction placed on a secured area that prevents anyone from entering the area until a supervisor is on site. The restriction can be enforced when there is free access (on door unlock schedules) and when there is controlled access (on access rules).

- When enforced on door unlock schedules, the doors remain locked until a supervisor enters the area. Cardholders who have access can still enter the area. Once an unlock schedule is enabled, it remains in effect till the end of the current time interval defined in the schedule.
- When enforced on access rules, no one can enter the area even though they have valid credentials, until a supervisor enters the area. A schedule defines when the first-person-in rule applies. You can configure

cardholders to be exempted from this constraint. An exempted cardholder can access the area without any supervisor being on site, but cannot clear the constraint for other cardholders.

NOTE: The first-person-in rule schedule must define discrete time intervals to allow the constraint to be reset. The *Always* schedule cannot be used.

- To clear the first-person-in rule constraint, the supervisor must arrive within the time frame defined by the unlock schedule or the first-person-in rule schedule, up to a few minutes earlier, defined by the **On-site time offset** value. After the constraint is cleared, normal access (free or controlled access) resumes until the end of the current time interval defined in the schedule.

  If the unlock schedule or the first-person-in rule schedule comprises several time intervals, then the supervisor must re-enter the area at the beginning of each time interval to clear the constraint.

NOTE: The *first-person-in rule* only works on areas controlled by a single Synergis™ unit. HID units do not support this feature. The *first-person-in rule* works best when the doors are equipped with entry sensors or door sensors. A Synergis unit is capable of differentiating between *No entry*, *Entry assumed*, and *Entry detected*. When no sensor is configured for a door, entry is assumed when access is granted.

Visitor escort rule

The visitor escort rule is the additional access restriction placed on a secured area that requires visitors to be escorted by a cardholder during their stay. Visitors who have a host are not granted access through access points until both they and their assigned host (cardholder) present their credentials within a certain delay. The host must present their credential after the visitors before access is granted to both. If multiple visitors are accompanied by the same escort, the escort only needs to present their credential once all visitors have presented their credentials.

Visitor escort for turnstiles in *delegation* mode requires the host to badge and enter before the visitors. For two-host visitor delegations, the tail host must present credentials and enter the area after the visitors. This mode requires Synergis™ Softwire 10.7 or later with dumb interfaces.

In contrast, visitor escort for turnstiles in *single passage enforcement* mode requires the host to badge after each visitor badges and enters. The host must badge and enter last. This mode is supported by dumb interfaces and Mercury controllers. For more information about this mode, see the *Synergis™ Softwire Single Passage Enforcement Technote*.

NOTE: HID controllers do not support the visitor escort rule.

Configuring secured areas

To set up an access control system with access rules and access control behavior, you must configure your areas as secured areas.

Before you begin

Create the areas that will represent your secured areas.

To configure a secured area:

1. From the Config Tool home page, open the *Area view* task.
2. Select the area entity (🏢) you want to configure and click the **Identity** tab.
3. Click **Access control** to turn on the option, and then click **Apply**.

   Two new tabs, **Properties** and **Advanced**, appear and the area icon is updated to show that it is now a secured area (🚪).
4. Click the **Properties** tab, and set the following:
   - **Access rules:** Define which cardholders are allowed to access (enter or exit) the area, and when by assigning access rules to the area. You can also assign cardholders or cardholder groups directly to the area, in which case, the cardholders are granted access all the time.
   - **Doors:** Link the doors that are used to enter and exit the area (perimeter doors) and the doors that are captive. Captive doors are necessary for the proper tracking of *people counting* and *antipassback*.

   NOTE: Access rules assigned to the area apply to all perimeter doors of the area, even though the access rules are not listed on the *Access rules* page of the perimeter doors. If each perimeter door must be governed by its own set of rules, configure the access rules on each door.
5. Click the **Advanced** tab, and set the following:
   - **Antipassback:** Access restriction placed on a secured area that prevents the same cardholder from entering an area they have not yet exited, and vice versa.
   - **Interlock:** Logic that only allows one perimeter door to be open at a time.
   - **First-person-in rule:** Unlock schedule is not triggered or regular access is disabled until a supervisor is present in the area.
   - **Visitor escort rule:** Visitors must be accompanied by their designated host (cardholder) to enter the area.
   - **Duress PIN:** A cardholder who is being coerced to open a door can enter their PIN with the last digit raised by 1 to trigger a Security Desk event. Only works on doors with readers set to Card and PIN.
6. Click **Apply**.

Related Topics

About secured areas on page 792

Adding doors to areas

To make sure an area is secure, add the doors to the area in Config Tool.

Before you begin

Create the areas that you want to link doors to.

What you should know

Doors that are members of an area can be configured as *Captive* or *Perimeter* doors. Perimeter doors are used to enter and exit an area, and help to control access. Captive doors are doors that are used within the area. Set the *door sides* correctly to ensure that *People counting* and *antipassback* are properly tracked. A door's *Entrance* and *Exit* sides are relative to the area being configured.

NOTE: Access rules configured for an area only apply to perimeter doors. All rules that deny access take precedence over the rules that grant access.

To add a door to an area:

1. From the Config Tool home page, open the *Area view* task.
2. Select an area and then click the **Properties** tab.
3. In the *Doors* section, click **Add an item** (➕) and select the doors that you want to link to your area.
4. For all doors in the *Doors* section, configure the door type:
   - If the door is used to enter or exit the area, set the slider to **Perimeter**.
   - If the door is located inside the area, set the slider to **Captive**.

     NOTE: If a smaller area is nested inside a larger area, you do not need to add the perimeter doors of the smaller area as captive doors of the larger area. The system automatically organizes nested areas when calculating people counts and applying antipassback rules.
   - To swap the door sides, select the door and click **Swap door side**.
5. Click **Apply**.

After you finish

To control access to your secured area, apply access rules to the area.

Applying antipassback to areas

After you created a secured area and configured at least one perimeter door, you can apply antipassback to prevent cardholders from entering areas they have not yet exited, and vice versa.

Before you begin

Create and configure a secured area to apply the antipassback restriction to.

What you should know

An area enabled with antipassback must be controlled by a single unit. If the area is not controlled by a single unit, the following criteria must be met in order to apply antipassback.

- All units controlling the doors within the area are Synergis™ units.
- All units controlling the area are managed by the same Access Manager role.
- Global antipassback is enabled on the Access Manager role.

Limitations: For areas controlled by HID units, the antipassback logic is only applied to perimeter doors, not to captive doors.

To configure antipassback for an area:

1 From the Config Tool home page, open the *Area view* task.

2 Select the secured area, and click the **Advanced** tab.

3 Turn on the **Antipassback** option.

4 If the doors are controlled by an HID unit, turn off the **Interlock** option.

5 Set the following:

- **Schedule:** Select *Always* if you want antipassback to be applied at all times.
- **Type:** Type of antipassback to apply.
  - **Soft:** Soft antipassback only logs the passback events in the database. It does not restrict the door from being unlocked due to the passback event.
  - **Hard:** Hard antipassback logs the passback event in the database and prevents the door from being unlocked due to the passback event.
- **Presence timeout:** Set how many minutes a cardholder’s presence in the area is remembered for the purpose of passback detection (not used for counting people). Past that period, a cardholder who never left the area can re-enter without triggering a passback event. The default value of zero (0) minutes means that a cardholder's presence never times out.

  NOTE: When global antipassback is enabled, the presence of a cardholder in an area is forgotten after seven days if no entry or exit from this area is reported for that cardholder during that period. This means that cardholders can re-enter an area that they never left, or leave an area they never entered, without triggering a passback event if no movement was registered for these cardholders on that area for seven days. This applies even if the **Presence timeout** is set to infinite (=0).
- **Strict:** Turn on this option to generate passback events for both types of access violations: when cardholders try to re-enter an area that they never left, and when cardholders try to exit an area that they never entered. Otherwise, the default is turn it off and antipassback logic is only verified on area entrances, and passback events are only generated when cardholders try to re-enter an area that they never left.

  BEST PRACTICE: If you choose to enable *strict* and *hard* antipassback on an area that is not controlled with turnstiles or similar devices that only allow one person through at a time, grant the *Forgive antipassback violation* privilege to the operators responsible for monitoring this area.

  NOTE: With strict antipassback turned off, you can have Card-In/REX-out perimeter doors, but the **Presence timeout** parameter must be configured (> 0). With strict antipassback turned on, all perimeter doors must be configured as Card-In/Card-Out, **Presence timeout** must be set to infinite (= 0), and no REX can be configured.

6 Click **Apply**.

Related Topics

About secured areas on page 792

About access control units on page 758

Enabling global antipassback on Access Manager roles

If the areas on which you want to apply the antipassback restrictions are controlled by multiple Synergis™ units, you must enable global antipassback on the Access Manager roles.

What you should know

When *strict* and *hard* antipassback is applied to an area without global antipassback, a cardholder who entered the area through one door cannot leave the area through another door if both doors are not controlled by the same unit. Also, the same cardholder who entered the area through one door, can re-enter the area through a different door if the two doors are not controlled by the same unit. With global antipassback enabled, these two violations can be prevented.

IMPORTANT: Global antipassback only works on areas that are entirely controlled by Synergis units. All units controlling the same area must be managed by the same Access Manager.

TIP: If you need to switch your units between Access Manager roles to meet the global antipassback requirements, use the Move unit tool.

To enable global antipassback on an Access Manager role:

1 From the Config Tool home page, open the *Access control* task, and click the **Roles and units** view.

2 Select the Access Manager role to configure, and click the **Properties** tab.

3 On the *Properties* page, select the following options: **Activate peer-to-peer** and **Activate global antipassback**.

NOTE: Up to 15 Synergis units can be connected as peers.

4 Click **Apply**.

Defining area occupancy limits

Setting a maximum occupancy limit is useful for controlling how many people are in a given area for safety or legal reasons. Going over the set limit triggers events that can be used to further trigger alarms and actions.

Before you begin

Do the following:

- Create and configure a secured area.
- Activate antipassback and set it to *Hard* and *Strict*, and set the schedule to *Always*, and the **Presence timeout** to **0**.
- Make sure that unlock schedules are not set for the area's perimeter doors.

What you should know

Max occupancy requires Synergis™ Softwire 10.7 or later.

To define an occupancy limit:

1. From the *Area view* task, select an area and click **Advanced**.
2. Under *Max occupancy*, set the following:
   - **Status:** Set it to **ON** to enable the max occupancy feature. Enabling a *Max occupancy* limit on an area generates the following events:
     - *Max occupancy reached* when the area reaches the configured limit. This event sends the area into a warning state.
     - *Max occupancy exceeded* when additional cardholders enter the area.
     - *Below max occupancy* when the number of occupants drops below the configured limit.
   - **Type:** Select from the following:
     - *Hard*: When the max occupancy limit is reached, it will deny the next access request on the area's perimeter door.
     - *Soft*: Will not deny subsequent access requests.
   - **Max occupancy limit:** Enter the number of people the area can hold before triggering the limit.

     NOTE: Cardholders with the **Bypass antipassback rules** option active are granted access even if the area's occupancy limit is reached or exceeded.
3. Click **Apply**.

   The area view in Security Desk's *People counting* task tracks how many cardholders are in the area, and displays the number next to the area in the *entity tree* (For example, an area with a six-person limit but only three occupants will show as "3/6"). When the area reaches capacity, its entity turns yellow. If additional cardholders enter the area, the number will turn red.

You can monitor maximum occupancy events in Security Desk's *Monitoring* or *Maps* tasks.

Interlocking doors within areas

After your area is created and it contains at least two perimeter doors, you can apply an interlock logic to it so that only one door can be open at a time.

Before you begin

- Create and configure a secured area to apply the interlocking logic to.
- Link at least two perimeter doors to your area.

What you should know

For interlock logic to work, the door sensors must be able to detect when the door is opened.

To interlock the perimeter doors of an area:

1. From the Config Tool home page, open the *Area view* task.
2. Select the secured area, and click the **Advanced** tab.
3. Turn on the **Interlock** option.

   When the option is on, only one perimeter door of the area can be open at any given time. To open a door, all others must be closed.
4. If the door is controlled by an HID unit, turn off the **Antipassback**.
5. If you need to override the normal behavior in case of an emergency, set the following:
   - **Override:** Select the input that is wired to the *override* key switch or flip switch. When the switch in on, the interlock feature is disabled.
   - **Lockdown:** Select the input that is wired to the *lockdown* key switch or flip switch. When the switch is on, all perimeter doors remain locked until the switch is back to its normal position.
   - **Priority:** When both the *override* and *lockdown* inputs are configured, select which one has priority when both inputs are active.
6. Click **Apply**.

Related Topics

About secured areas on page 792

Enforcing a supervisory presence on secured areas

You can keep a secured area locked until a supervisor shows up, by enforcing the *first-person-in* rule on the area.

Before you begin

Create and configure a secured area to enforce the first-person-in rule to.

What you should know

The *first-person-in rule* only works on areas controlled by a single Synergis™ unit. HID units do not support this feature.

To ensure a supervisor is on site before granting access to an area:

1. From the Config Tool home page, open the *Area view* task.
2. Select the secured area, and click the **Advanced** tab.
3. In the *First-person-in rule* section, do the following:
   - To ignore the door unlock schedules when no supervisor is present, set the **Enforce on doors unlock schedules** option to **ON.**
   - To ignore the access rules when no supervisor is present, set the **Enforce on access rules** option to **ON**, and then select the schedule to dictate when the first-person-in rule applies.
4. Click the **On-site time offset** to grant more freedom to the time the supervisor must show up to clear the first-person-in rule constraint.

   If the time offset is set to zero, the supervisor cannot show up earlier than the start of the access schedule, or else their arrival would be ignored.
5. Under the **Supervisors** list, click **Add an item** (+), and then select the cardholder groups and cardholders to designate them as supervisors of the area.

   You must configure at least one supervisor. Only one supervisor needs to be present in the area to satisfy the first-person-in rule constraint.
6. (Optional) Under the **Exemption list**, click **Add an item** (+), and then select the cardholder groups and cardholders to whom the first-person-in rule does not apply.

   Access is granted to those cardholders solely based on the access rules. A supervisor does not need to be present to grant them access to the area.
7. Click **Apply**.

Related Topics

About secured areas on page 792

Requiring visitors to be escorted to access secured areas

You can increase the security of certain areas by requiring visitors to be accompanied by a designated host. A host must present their credential after the visitor within a certain delay before access is granted to the entire party.

Before you begin

- Create and configure a secured area to enforce the visitor escort rule to.
- Link at least one perimeter door to your area.

To require a visitor to be escorted to access an area:

1. From the Config Tool home page, open the *Area view* task.
2. Select the secured area, and click the **Advanced** tab.
3. In the **Visitor escort rule** section, do one of the following:
   - Set the **Enforce visitor escort rule** option to **ON**.
   - Click **Revert to inherited value** (⬆) if the parent area has visitor escort rule enforced.
4. Click **Apply**.
5. Select the **Properties** tab.
6. (Optional) For all perimeter doors configured for this area:
   a) Select door and click **Jump to** (➡).
   b) Select the door’s **Properties** tab.
   c) Set the **Maximum delay between card presentations** in seconds.
      Access is denied if the escort does not present their credential within the specified delay after the visitor.
   d) Click **Apply**.

After you finish

When you check in visitors who need supervised access to this area, assign one or two hosts (cardholders who have access to this area) to the visitor, and select **Escort required**.

Related Topics

About secured areas on page 792

Configuring visitor escort for turnstiles in delegation mode

Requiring visitor escort increases security for turnstile-accessible areas. Using Config Tool, you can set restrictions on visitor host configuration and add visitor delegation size limits.

Before you begin

Create a secured area with at least one door.

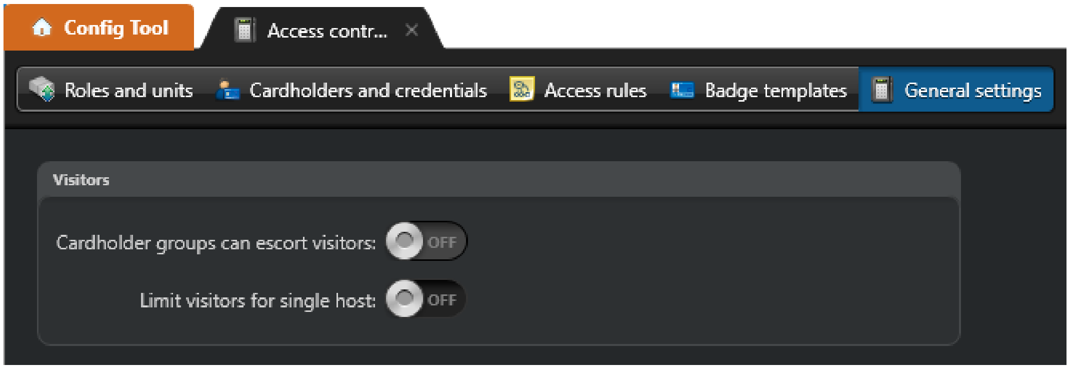
What you should know

Visitor escort for turnstiles in delegation mode requires Synergis™ Softwire 10.7 or later with dumb interfaces. This procedure does not apply to visitor escort for turnstiles in single passage enforcement mode.

NOTE: *Delegation* mode is not to be confused with *single passage enforcement* mode. The latter mode is supported by dumb interfaces and Mercury controllers. For more information about this mode, see the *Synergis™ Softwire Single Passage Enforcement Technote*.

To set up visitor escort for turnstiles in delegation mode:

1 Click **Access control** > **General settings** and set **Cardholder groups can escort visitors** to **OFF**.

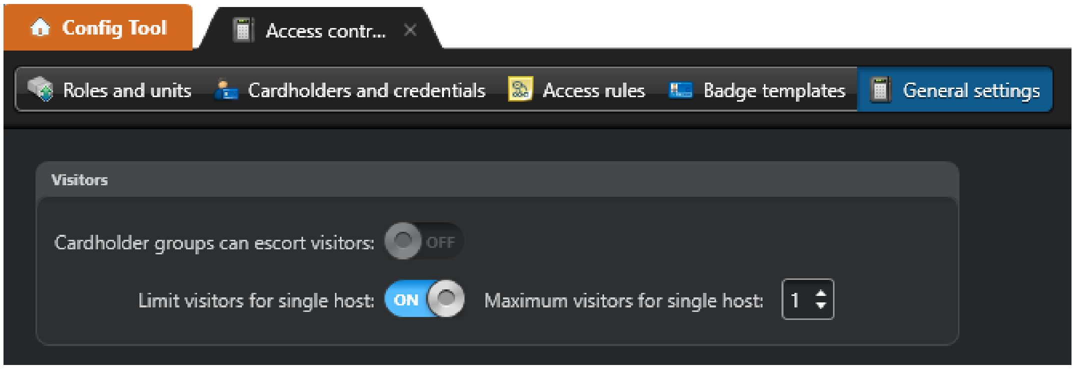


Cardholder groups can escort visitors: OFF

Limit visitors for single host: OFF

If the option is left **ON**, the *Visitor astray* and *Missing tail host* events are not triggered.

2 (Optional) Set **Limit visitors for single host** to **ON** and set a limit.



Cardholder groups can escort visitors: OFF

Limit visitors for single host: ON Maximum visitors for single host: 1

NOTE: The defined number is the threshold above which a second host must be added. There is no limit to the visitor number for two-host delegations.

3 Click **Apply**.

4 Click **System** > **General settings** > **Custom fields** and click **Add an item** (➕).

5 From the **Entity type** list, select **Door** (🚪).

6 From the **Data type** list, select **Boolean**.

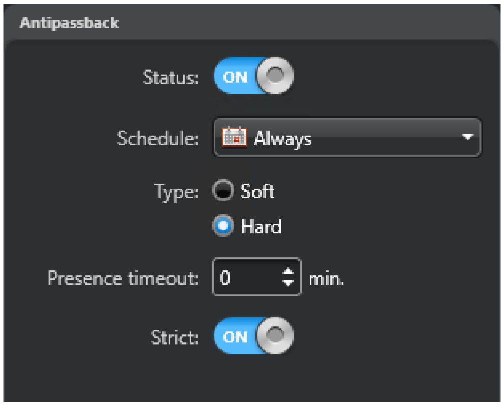
7 In the **Name** field, enter `TurnstileANSSI`.

8 Click **Save and close** > **Apply**.

9 In the *Area view* task, select the area in the entity tree.

10 On the *Advanced* page, set **Enforce visitor escort rule** to **ON**.

11 (Optional) Set Antipassback to **ON**.



Antipassback

Status: ON

Schedule: Always

Type: ○ Soft ● Hard

Presence timeout: 0 min.

Strict: ON

12 Select the area's door in the entity tree.

13 Click the **Custom fields** tab, select **TurnstileANSSI**, and click **Apply**.

14 (Optional) Click the **Identity** tab, and set the icon to a turnstile ().

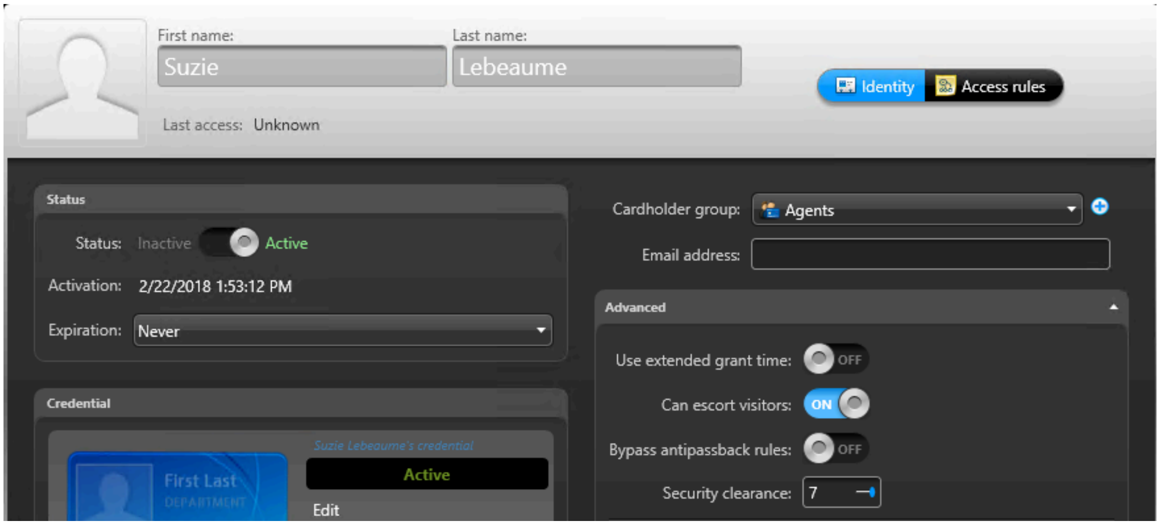
15 Click the **Properties** tab.

16 In the *Visitor escort and two-person rule* section, set **Maximum delay between card presentations** to a higher value than the default five seconds to give visitors enough time to badge and pass through the turnstile.

A visitor must present their credential and enter within the set delay, otherwise a *Visitor astray* event is triggered.

17 Click **Apply**.

18 In the *Cardholder management* task, ensure that the cardholders you want as designated hosts have the **Can escort visitors** option set to **ON**, and all other cardholders have **Can escort visitors** set to **OFF**.



First name: Suzie

Last name: Lebeaume

Last access: Unknown

Status

Status: Inactive Active

Activation: 2/22/2018 1:53:12 PM

Expiration: Never

Credential

Suzie Lebeaume's credential

Active

Cardholder group: Agents

Email address:

Advanced

Use extended grant time: OFF

Can escort visitors: ON

Bypass antipassback rules: OFF

Security clearance: 7

19 Click **Save and close**.

All cardholders created in Security Center versions before 5.7 SR2 have the **Can escort visitors** option enabled by default. You can use the **Options** check box in the Copy configuration tool to deactivate the

Can escort visitors option for multiple cardholders at the same time. The **Options** check box will copies the values of the following:

- Use extended grant time
- Can escort visitors
- Bypass antipassback rules
- Security clearance

Make sure to only use this feature on cardholders with matching option values.

Enabling Duress PIN

In cases where a cardholder is being forced to unlock a door, the ability to trigger an alarm in a non-obvious way can help ensure that employee's safety. *Duress PIN* will grant entry while generating a *Duress PIN entered* event, which can be used to trigger system actions.

What you should know

Duress PIN requires Synergis™ Softwire 10.7 or later, and readers set to Card and PIN.

To signal a duress, authorized cardholders must badge and enter their regular PIN + 1 to the last digit. For example, if the regular PIN is 1234, then the duress PIN is 1235. If the last digit is a 9, then it becomes a 0; for example, 9999 would become 9990.

To enable Duress PIN:

1. From the Config Tool home page, open the *Area view* task.
2. Select the area you want to modify and click **Advanced**.
3. Under *Duress PIN*, set the **Status** slider to **ON**.
4. Click **Apply**.
   Any changes made to the *Duress PIN* settings are traced in the *Audit trails* report.

About access rules

An access rule entity defines a list of cardholders to whom access is either granted or denied based on a schedule. Access rules can be applied to secured areas and doors for entries and exits, or to intrusion detection areas for arming and disarming.

Unlike other access control solutions, Synergis™ does not use *clearance codes* or *access levels* to grant or deny access. Instead, the basic logic used by Synergis to grant or deny access is defined by *access rules*.

The biggest difference between an *access rule* approach and an *access level* approach is that access rules are applied to the access points of the physical locations we want to protect, whereas access levels are applied to people. Access rules specify *who* can pass through a door and *when* they can do so. An access level defines *where* and *when* a person can gain access.

An access rule contains the three W's:

- Who? (Who can pass through - *cardholders* or *cardholder groups*)
- What? (Whether access is granted or denied)
- When? (The *schedule* when the access rule is applied)

Access rules that have been pushed to the door controllers, called *access control units* in Security Center, do not have to be modified. If you associate a new credential with a cardholder, the old rule is still valid.

Permanent vs. temporary access rules

Access rules are either permanent or temporary. A temporary access rule is an access rule that has an activation and an expiration time. Temporary access rules are suited for situations where permanent cardholders need to have temporary or seasonal access to restricted areas. These access rules are automatically deleted seven days after they expire to avoid cluttering the system.

Typical use case examples of temporary access rules include seasonal cardholders, such as students who need to access a lab during their semester, and permanent cardholders who need short term access to a restricted area, such as maintenance technicians who need to work on storage servers at a highly secured data center.

From the *Cardholder management* task, you can only assign a temporary access rule to one cardholder at a time. To assign a temporary access rule to multiple cardholders or cardholder groups, you must update the access rule properties from Config Tool.

Limitations

Temporary access rules work with both HID and Synergis units. However, only Synergis units can apply temporary access rules while operating offline (disconnected from the Access Manager). For HID units to work with temporary access rules, the controller must always be connected to the Access Manager, and the synchronization must be set to *Automatically*. The activation of temporary access rules is immediate because of the host lookup. However, the expiration of a temporary access rule only comes in effect after a synchronization with the Access Manager.

Related Topics

About Security Center Synergis on page 743

Creating access rules

To control access anywhere on your site, you must create access rules that will apply to the areas, doors, and elevators.

Before you begin

Create the schedules that will apply to this access rule.

What you should know

As a best practice, use a descriptive name when creating access rules so you can easily determine what each rule does. For example, *Lab Technicians Only* or *All Employees Regular Hours*.

To create an access rule:

1. From the Config Tool home page, open the *Access control* task, and click the **Access rules** view.
2. Click **Access rule** (+).
3. Assign a name and description to the access rule.
4. In the **Partition** list, select the partition in which you want the access rule to be created, and click **Next**.
5. Select the schedule for when you want your rule to be active. The default is *Always*.
6. Select the type of rule you want (*Permanent* or *Temporary*).

   Permanent access rule is the default. A temporary access rule is an access rule that has an activation and an expiration time. Temporary access rules are suited for situations where permanent cardholders need to have temporary or seasonal access to restricted areas. These access rules are automatically deleted seven days after they expire to avoid cluttering the system.
7. If you select **Temporary**, specify the following:
   - **Activation:** Activation date and time, or when the rule schedule starts to apply.
   - **Expiration:** Expiration date and time, or when the rule schedule stops to apply.
8. Click **Next.**
9. Review the *Creation summary*, and click **Create** > **Close.**
10. Select the access rule you created, and click **Properties**.
11. Select whether to **grant access** or **deny access** when the rule is active.

    BEST PRACTICE: Usually schedules are used to grant access. Access is denied when schedules are inactive. Use explicit **deny** schedules only for exceptions.
12. Under the *Cardholders affected by this rule* section, click **Add an item** (+), select the cardholders or cardholder groups the access rule applies to, and then click **Add**.

    BEST PRACTICE: Create cardholder groups instead of individual cardholders, as this becomes much more manageable in large systems as more people come and go.
13. Click **Apply**.

After you finish

Assign the access rule to secured areas, doors, and elevators so the access rule is operational. You can do this from the *Relationships* section of the access rule's *Identity* page or from the area, door, and elevator entities.

Related Topics

Configuring secured areas on page 794

Selecting who has access to doors on page 785

Selecting who has access to elevators on page 791

About double-badge activation

With double-badge activation, also known as double-swipe activation, an authorized cardholder can unlock a door and trigger actions by badging twice. The door remains unlocked and the action remains active until the next double-badge event.

A double badge or double swipe is defined as two badge reads from the same cardholder within the standard grant time configured for the door. The first read unlocks the door; the second read triggers the configured action.

How it works

Double-badge activation requires doors that are controlled by a Synergis™ unit, and a **DoubleSwipe** custom field configured for door entities in Security Center. This custom field identifies the cardholder group whose members are authorized to perform double-badge actions.

Cardholder information is logged with double-badge activation events. This information is shown in the credential column of the following reports:

- Cardholder activities
- Credential activities
- Door activities
- Area activities

Supported interface modules

You must operate interface modules in *dependent mode*, where the Synergis unit makes all access control decisions. The following table lists the interface modules that are supported, and any restrictions that apply.

Supported interface modules	Restrictions to the supported operation modes
HID VertX V100	The V100 must be online. Degraded mode is not supported.
Mercury MR panels	The MR panels must be online. Degraded mode is not supported.
Mercury controllers	The controller must be operating in dependent mode. Standalone mode is not supported.
Honeywell controllers	The Honeywell controller must be operating in dependent mode. Standalone mode is not supported.
DDS	The DDS controller must be operating in dependent mode. Standalone mode is not supported.
SALTO SALLIS	After the door is unlocked with a double-badge, press the *Privacy button* and double-badge again to return the lock to its normal state.
Aperio-enabled locks	Only Aperio v3 lock hardware is supported. See the *Synergis™ Softwire Integration Guide* for the certified models and firmware versions. You must set the lock access decision timeout to 8 seconds on Aperio hubs to get proper reader LED feedback on Aperio locks.
STid readers	None.

Limitations

- Double-badge activation does not work with turnstiles or elevators.
- Doors unlocked with double-badge activation remain unlocked if you delete the **DoubleSwipe** custom field while the door is unlocked.

Related Topics

Selecting who has access to doors on page 785

Changing the lock access decision timeout on Aperio hubs

To get proper reader LED feedback when using double-badge activation with an Aperio lock, it is recommended to change the lock access decision timeout of the communication hub to 8 seconds.

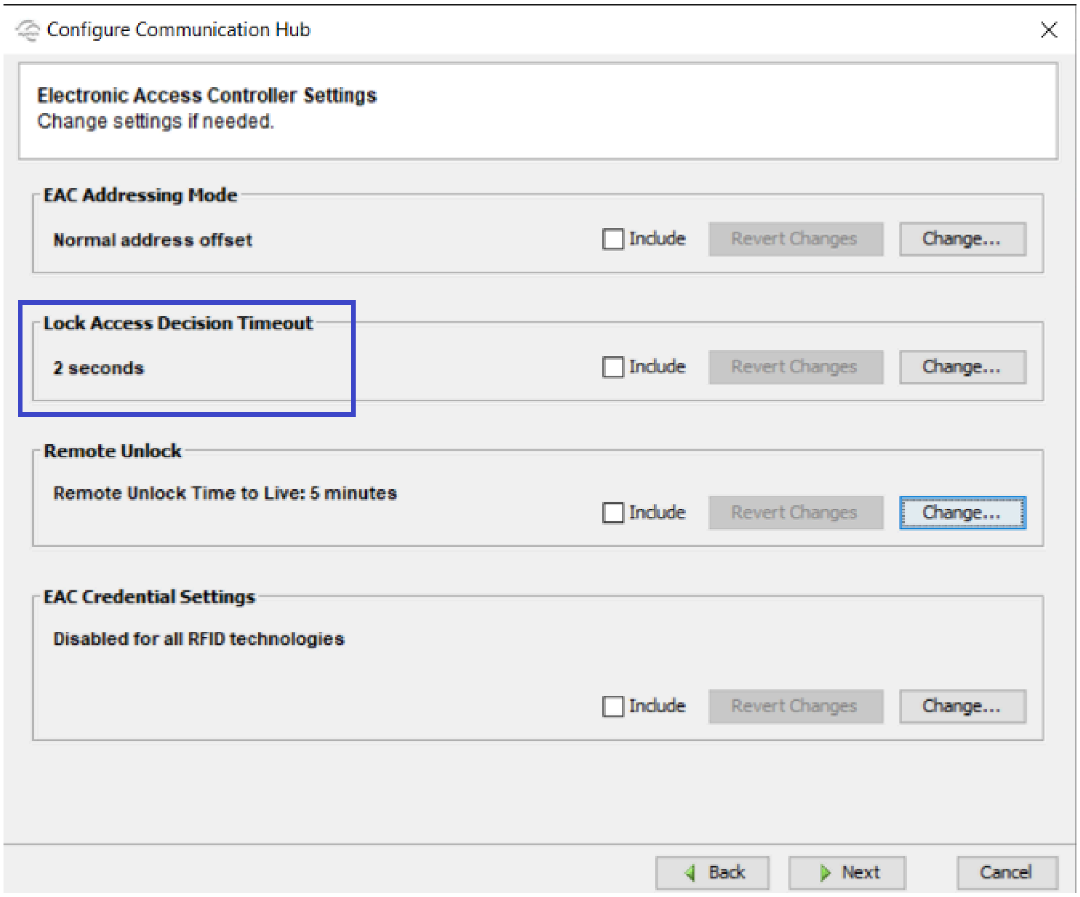
Before you begin

Pair the Aperio lock to its hub using *Aperio Programming Application* (APA). For more information, see the *Synergis™ Softwire Integration Guide*.

To change the lock access decision timeout on a hub:

1. Open APA (see the *Aperio Online Programming Application Manual* for instructions).
2. From APA, right-click the hub and select **Configure**.
   The *Configure Communication Hub* dialog box opens.

3 In the *Lock Access Decision Timeout* section, click **Change**, and set the **Lock Access Decision Timeout** to 8 seconds.



Configure Communication Hub

Electronic Access Controller Settings
Change settings if needed.

EAC Addressing Mode
Normal address offset

Lock Access Decision Timeout
2 seconds

Remote Unlock
Remote Unlock Time to Live: 5 minutes

EAC Credential Settings
Disabled for all RFID technologies

Enabling double-badge activation

To enable double-badge activation on a door controlled by a Synergis™ unit, create a custom field named **DoubleSwipe** for door entities so that you can set cardholder groups that are authorized to perform double-badge actions.

Before you begin

- Ensure that the door is controlled by a Synergis unit.
- Ensure that the interface modules are operating in dependent mode.
- Create a cardholder group for the cardholders who can use double-badge activation.

To enable double-badge activation:

1 From the Config Tool home page, open the *System* task, and click the **General settings** view.

2 Click the **Custom fields** tab, and then click **Add an item** (➕).

3 In the *Add custom field* dialog box, set the following values:

- **Entity type:** Select **Door**.
- **Data type:** Select **Entity**.
- **Name:** Enter `DoubleSwipe`.

4 (Optional) In the *Layout* section, enter a group name and a priority.

5 In the *Security* section, add the user groups and users who are authorized to edit this custom field.

6 Click **Save and close**.

7 Click **Apply**.

8 Configuring your doors for double-badge activation.

Configuring a door for double-badge activation

To configure a door for double-badge activation, you must apply a cardholder group to the door.

To configure a door for double-badge activation:

1 Open the *Area view* task.

2 In the entity tree, select the door on which you want to enable double-badge activation.

3 Click the **Custom fields** tab.

4 From the **DoubleSwipe** list, select the cardholder group that is authorized to use the feature.

5 Click **Apply**.

6 (Optional) Repeat the steps for any doors you want configured for double-badge activation.

After you finish

After all doors have been updated, manually synchronize all Synergis™ units that control them.

36

Cardholders

This section includes the following topics:

About cardholders

A cardholder entity represents a person who can enter and exit secured areas by virtue of their credentials (typically access cards) and whose activities can be tracked. They are the *Who* in an access rule.

Cardholder groups

The *cardholder group* entity is used to configure the common *access rights* and properties of a group of cardholders.

If you have a large access control system, cardholders and access rules are much easier to manage when cardholders are members of cardholder groups.

Creating cardholder groups

To configure the access rights and properties that are common to a group of cardholders, you can create cardholder groups.

What you should know

If you have a large access control system, cardholders and access rules are much easier to manage when cardholders are members of cardholder groups.

To create a cardholder group:

1. Open the *Access control* task, and click the **Cardholders and credentials** view.
2. Click **Cardholder group** (➕).

   A new cardholder group appears in the entity tree.
3. Type a name for the group, and press Enter.
4. Select the cardholder group, click the **Properties** tab.
5. At the bottom of the page, click ➕ to add individual cardholders or cardholder groups to your new group.
6. Click **Apply**.

Creating cardholders

To add new employees who must enter and exit secured areas using access cards, and to track their activities, you can create cardholders using the *Cardholder management* task.

Before you begin

- Define the maximum file size for cardholder pictures.
- To add custom information to cardholders, create custom fields.
- If you require different groups of cardholders with different access rights, create cardholder groups.
- To modify the security clearance of a cardholder, you must be granted the *Change cardholder options* and *Modify security clearance* privileges.

What you should know

Instead of creating cardholders manually, you can import them from a CSV file, or from your company's Active Directory.

To create a cardholder:

1. Open the *Cardholder management* task, and click **New** (✚).
2. At the top of the dialog box, enter the cardholder's first name and last name.
3. To assign a picture to the cardholder, click the silhouette and select one of the following options:
    - **Load from file:** Select a picture from disk. All standard image formats are supported.
    - **Load from webcam:** Take a snapshot with your webcam. This option appears only if you have a webcam attached to your workstation.
    - **Load from camera:** Take a snapshot from a camera managed by Security Center. When you click **Load from camera**, a separate capture dialog box opens. Select the video source, and click **Take snapshot** (▣).
    - **Load from clipboard:** Load the picture copied to the clipboard. This option appears only if you used the Windows copy command to save a picture onto your clipboard.
4. To edit the picture, click it to open the *Image editor* and use the editing options at the top of the editor's dialog box.
5. (Optional) To remove the current picture, right-click the picture and select **Clear the picture**.
6. In the *Status* section, set the following:
    - **Status:** Set their status to *Active* by clicking **Activate**, or *Inactive* by clicking **Deactivate**. For their credentials to work, and for them to have access to any area, their status must be *Active*.
    - **Activation:** Set an activation for their profile:
        - **Never:** The date and time that you clicked **New** (✚) to create the cardholder. This is only available after a cardholder is deactivated.
        - **Specific date:** Activates on a specific date and time.
    - **Expiration:** Set an expiration for their profile:
        - **Never:** Never expires.
          NOTE: You can remove this option. For more information, see Removing the option for cardholders and credentials to never expire on page 837.
        - **Specific date:** Expires on a specific date and time.
        - **Set expiration on first use:** Expires a specified number of days after the first use.
        - **When not used:** Expires when it has not been used for a specified number of days.

7 Assign a credential to the cardholder so they can access secured areas.

NOTE: You can assign a credential now or after all credentials have been enrolled in the system.

8 Assign the cardholder to a cardholder group.

NOTE: A cardholder can belong to more than one cardholder group.

a) Click **Add an item** (➕).

b) Select the cardholder groups from the dialog box.

c) Click **OK**.

9 Enter the cardholder’s email address.

A valid email address is necessary if you want to assign *mobile credentials* to the cardholder.

10 Enter the cardholder’s mobile phone number.

11 (Optional) If custom fields are defined for cardholders, such as department, phone numbers, and so on, enter the additional cardholder information.

12 (Optional) In the *Advanced* section, configure the following cardholder properties:

NOTE: Some of these properties can be inherited from the parent cardholder groups. When a specific value is configured for the cardholder, click **Revert to inherited value** (⬆) to inherit the property from the parent cardholder groups. If multiple parent groups exist, the most privileged value is inherited.

a) If the cardholder has been assigned a credential, grant access privileges to the cardholder:

- **Use extended grant time:** Grants them more time to pass through doors where the *Extended grant time* parameter is configured for a door. Use this option for those with reduced mobility.
- **Can escort visitors:** Indicates whether or not the cardholder can act as a visitor host.
- **Bypass antipassback rules:** Exempts them from all antipassback restrictions.

b) In the **Security clearance** field, enter the cardholder’s security clearance level. The security clearance level determines their access to areas when a threat level is set in Security Center. Level 0 is the highest clearance level, with the most privileges.

c) In the **Entity name** field, enter a name for the cardholder entity, if you do not want to use the cardholder’s name.

By default, the **Entity name** uses the **First name** and **Last name** fields.

d) In the **Description** field, enter a description for the cardholder.

e) Assign the cardholder to a partition.

Partitions determine which Security Center users have access to this entity. Only users who have been granted access to the partition can see the cardholder.

13 Click **Save**.

Related Topics

Cropping pictures on page 820

Applying transparent backgrounds to pictures on page 821

Creating doors on page 780

Configuring secured areas on page 794

Assigning access rules to cardholders

To grant or deny a cardholder access to areas, doors, and elevators, you must assign access rules to them.

Before you begin

Create access rules.

What you should know

You can assign access rules while you are creating cardholders, or after they are created. In this procedure, it is assumed you have already created a cardholder.

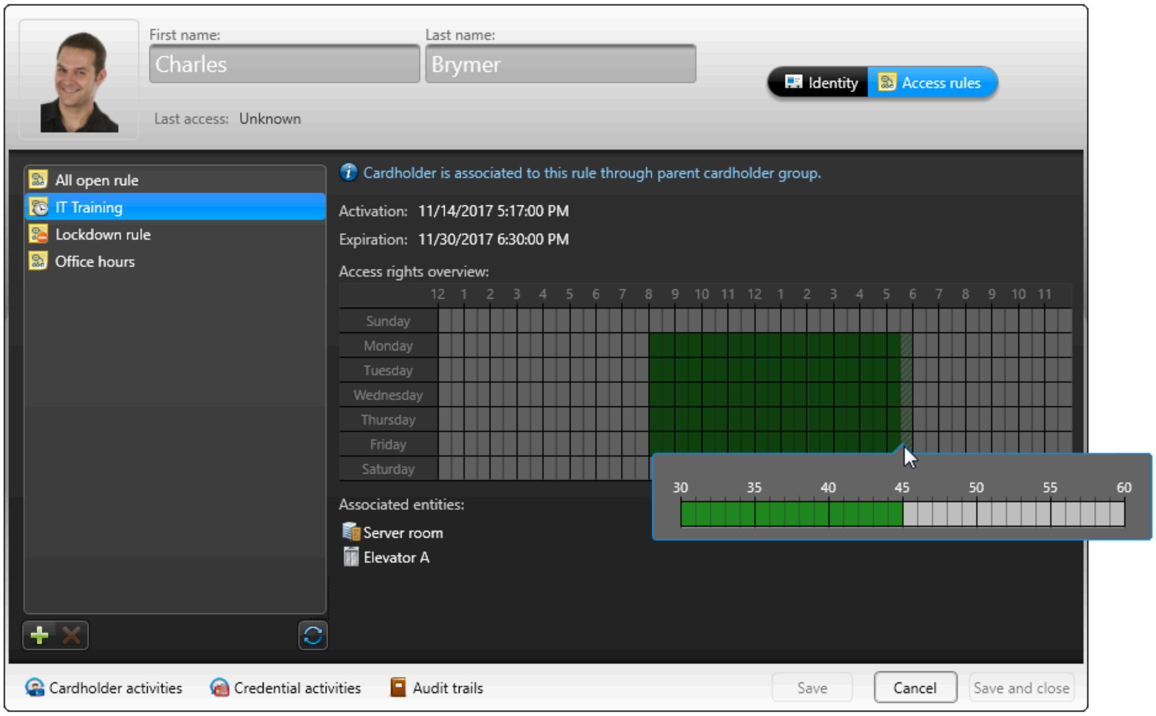
BEST PRACTICE: Assign access rules to cardholder groups, rather than to individual cardholders. Assign access rules to individual cardholders only as a temporary measure. When used too often, the access control system can quickly become unmanageable. If you need to grant temporary or short term access to a cardholder, create a temporary access rule.

To assign access rules to a cardholder:

1. In the *Cardholder management* task, select a cardholder, and then click **Modify** (✎).
2. Click the **Access rules** () tab and click **Add** (✚).

   A dialog box listing the access rules that are not yet assigned to this cardholder opens.
3. Do one of the following:
   - Select the rule you want to add, and click **Add**.
   - Create and assign a temporary access rule.
4. Select the access rule from the list.

   The schedule that applies to the access rule is shown in a grid on the right. Each time block represents 15 minutes. Green areas indicate periods when access is granted by the rule. Red areas indicate periods when access is denied by the rule. Grey areas are times not specified by the schedule; therefore, access is denied. If it is a temporary access rule (), the activation and expiration times are indicated. Areas, doors, and elevators that the rule is associated with are listed at the bottom.



First name: Charles

Last name: Brymer

Last access: Unknown

All open rule

IT Training

Lockdown rule

Office hours

Cardholder is associated to this rule through parent cardholder group.

Activation: 11/14/2017 5:17:00 PM

Expiration: 11/30/2017 6:30:00 PM

Access rights overview:

Associated entities:

Server room

Elevator A

5. To view a partial (hatched) time block in minutes, click and hold the left mouse button.
6. To assign another access rule to the cardholder, click ✚.
7. To remove an access rule directly assigned to the cardholder, click ✖.

   You cannot remove the *All open rule*, or the *Lockdown rule*.
8. Click **Save**.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

Assigning temporary access rules to cardholders

To accommodate seasonal cardholders, such as students who are enrolled during a semester, or permanent cardholders who need short term access to a restricted area, you can create and assign temporary access rules.

What you should know

A temporary access rule is an access rule that has an activation and an expiration time. Temporary access rules are suited for situations where permanent cardholders need to have temporary or seasonal access to restricted areas. These access rules are automatically deleted seven days after they expire to avoid cluttering the system.

NOTE: From the *Cardholder management* task, you can only assign a temporary access rule to one cardholder at a time. To assign a temporary access rule to multiple cardholders or cardholder groups, you must update the access rule properties from Config Tool. For Security Desk users to able to create temporary access rules, you need to grant them the *Add access rules* privilege.

To assign a temporary access rule to a cardholder:

1 In the *Cardholder management* task, select a cardholder, and then click **Modify** (✏).

2 Click the **Access rules** () tab and click **Add** (➕).

A dialog box listing the access rules that are not yet assigned to this cardholder opens.

3 Do one of the following:

- Select an existing temporary access rule (⏲) and click **Add**.
- Click **Temporary access rule** (➕).

  The temporary access rule creation wizard opens.

4 In the *Basic information* page, enter the rule name and description, then click **Next**.

5 In the *Access rule information* page, do one of the following:

- Click **Use an existing access rule as template** and select from the **Access rule** list, the access rule you want to use as template.

  The schedule and the associated entities will be copied to your temporary access rule.
- Click **Specify custom access parameters**, and specify the following:
  - **Access to:** Expand the area view and select the entities you want to grant access to.
  - **Activation:** Activation date and time, or when the rule schedule starts to apply.
  - **Expiration:** Expiration date and time, or when the rule schedule stops to apply.
  - **Schedule:** Choose when this access rule is active.

6 Click **Next** > **Create**.

A temporary access rule (⏲) is created and assigned to your cardholder.

7 Click **Save**.

After you finish

(Optional) Assign the temporary access rule you created to other cardholders.

Cropping pictures

To cut out an area of a cardholder or visitor’s picture and focus on the part of the image that you want to keep, you can crop the picture.

To crop a picture:

1 From the *Cardholder management* or *Visitor management* task, select a cardholder, and click **Modify** (✎).

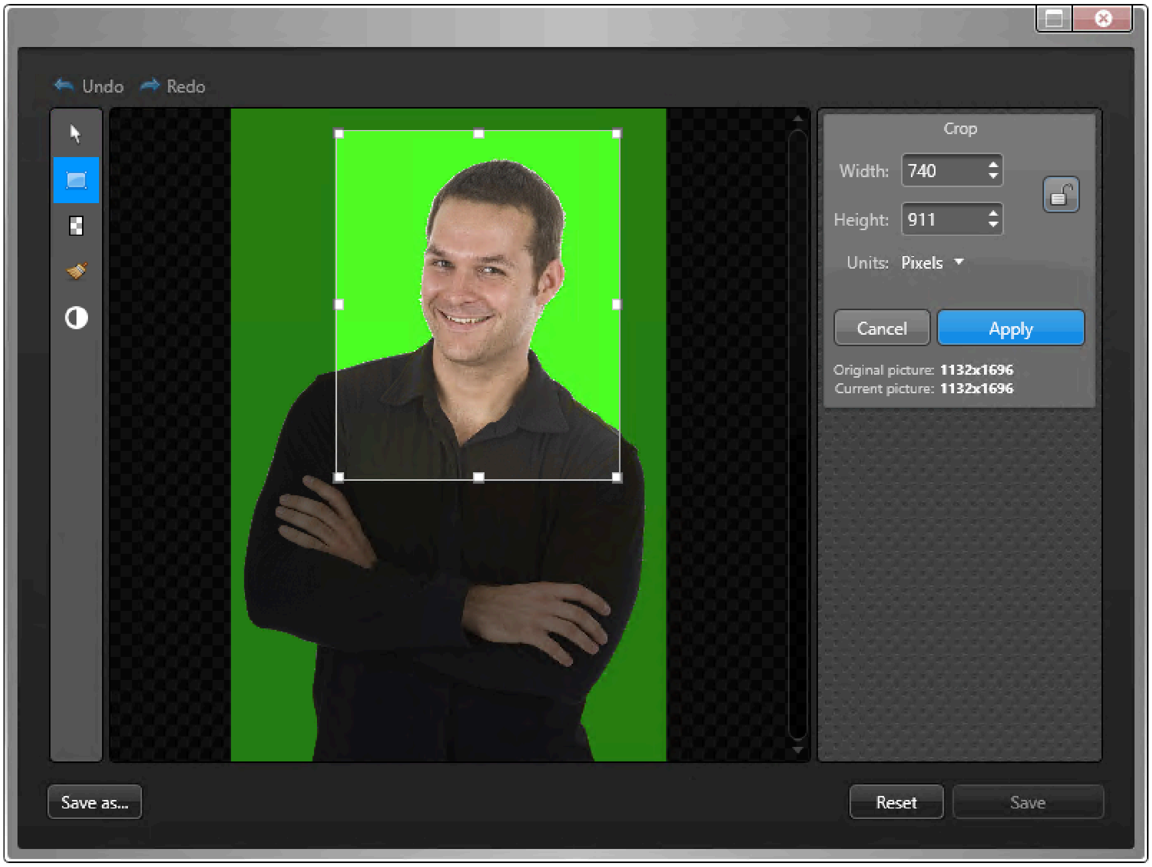
A dialog opens displaying the cardholder or visitor's information.

2 Click the picture.

3 In the image editor, click **Crop** (▭).

4 On the image, click and drag the ⊏ icon to crop the picture.

5 Change the crop area by resizing and moving the box on the image, or by changing the **Width** and **Height** values. The width and height values can be in pixels, inches, or millimeters.



6 To revert the picture to its original state, click **Reset**.

7 Click **Apply**, and then click **Save**.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

Applying transparent backgrounds to pictures

If a cardholder or visitor's picture was taken in front of a chroma key screen, you can make the picture background transparent. This is helpful if you create a badge template that has an image in the background.

What you should know

You can also set the transparency and color for backgrounds of cardholder pictures in the Import tool, so you can use the same settings while importing multiple cardholder pictures.

To apply a transparent background to a picture:

1 From the *Cardholder management* or *Visitor management* task, select a cardholder, and click **Modify** (✎).

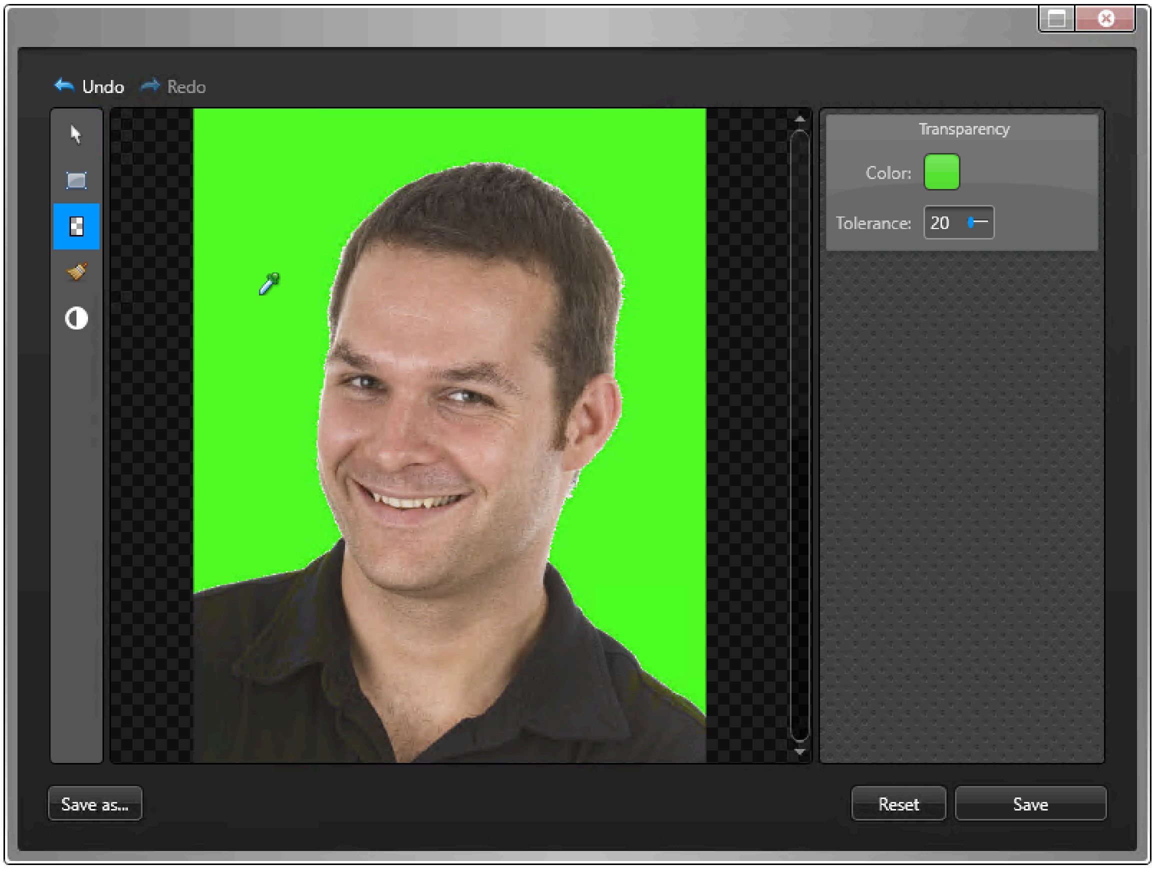
A dialog opens displaying the cardholder or visitor's information.

2 Click the picture.

3 In the image editor, click **Transparency** (▨).

The cursor changes to the eyedropper tool when you hover over the image.

4 Click the background where the chroma color is (usually green or blue).

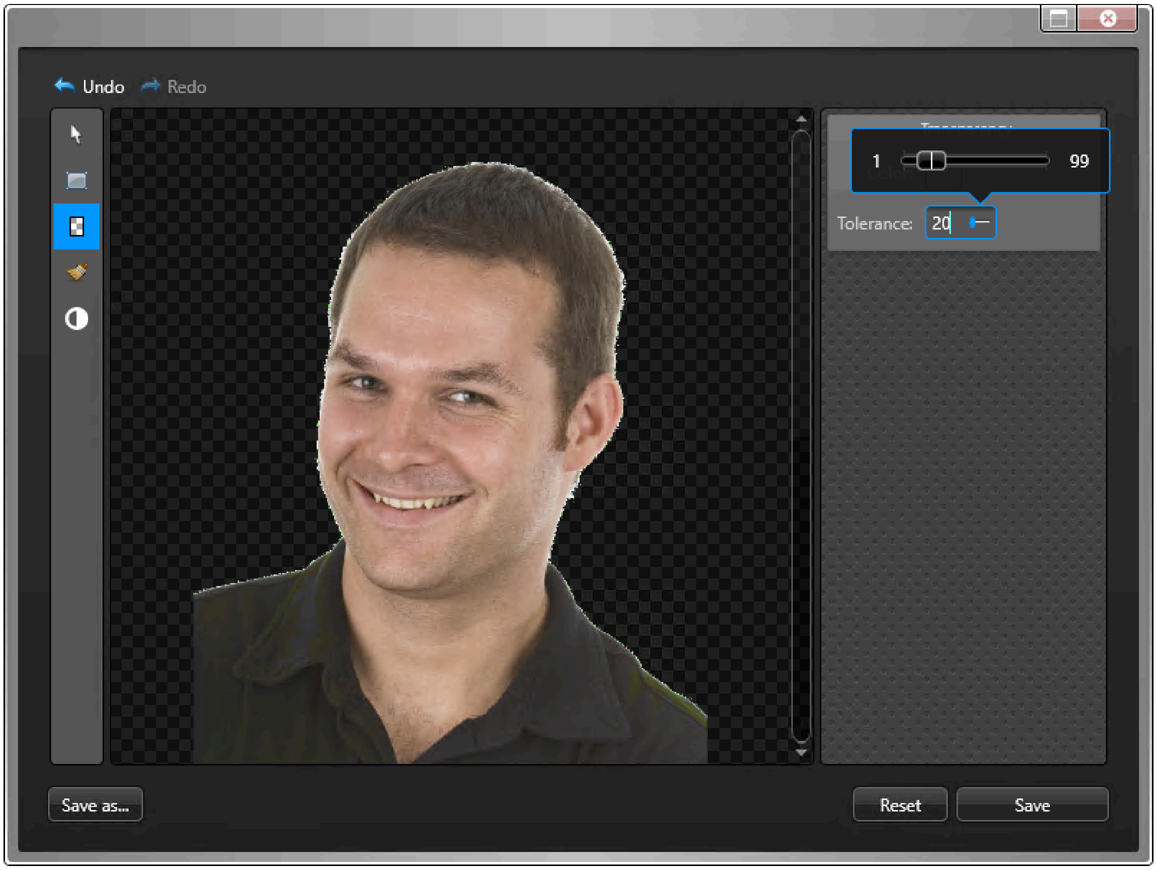


Transparency

Color: 🟩

Tolerance: 20

5 Using the **Tolerance** slider, adjust the transparency percentage.



Tolerance: 20

6 To revert the picture to its original state, click **Reset**.

7 Click **Save**.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

Defining the maximum file size of pictures

To improve the sharpness of the cardholder and visitor pictures, you can increase the maximum file size for pictures that are stored in the Directory database.

What you should know

The maximum file size applies to cardholder and visitor pictures and to all image data fields in Security Center. This setting also applies to the *Import tool*, and can be modified while running this tool. When loading image files, Security Center automatically reduces the image size so that their file size is under the limit you set.

The default value is 20 KB. You can set the limit anywhere between 20 and 5000 KB.

To define the maximum file size of pictures:

1 Open the *Access control* task and click the **General settings** view.

2 In the **Maximum picture file size** option, set the maximum number of kilobytes.

3 Click **Apply**.

The new limit will apply to all future image field updates.

Related Topics

Importing cardholders and credentials on page 912

Assigning credentials

To grant cardholders or visitors access to secured areas, you must assign them credentials.

What you should know

Cardholders and visitors can be assigned multiple *credentials*. You can assign credentials while you are creating a new cardholder or visitor (except for *mobile credentials*), or after they have been created. In this procedure, it is assumed you have already created the cardholders.

To assign credentials:

1 Do one of the following:

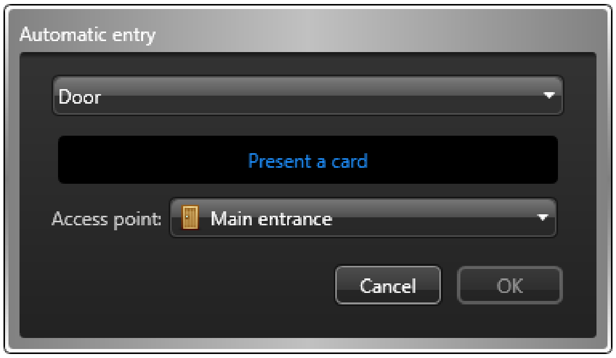
- For cardholders, open the *Cardholder management* task, select a cardholder, and then click **Modify** (✏).
- For visitors, open the *Visitor management* task, select a visitor, and then click **Modify** (✏).

2 In the *Credential* section, click **Add a credential** (➕).

3 Select one of the following options:

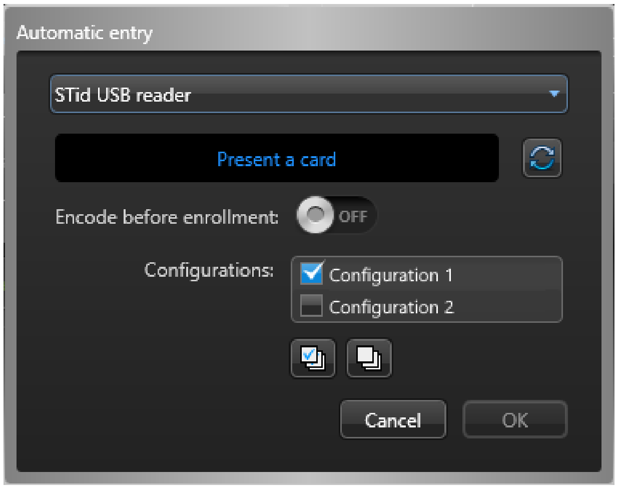
- **Automatic entry:** Present the card at a reader.
- **Manual entry:** Manually enter the card data. Use this method when you do not have a card reader near you.
- **Existing credential:** Select a pre-enrolled, unassigned credential.
- **PIN:** Create a PIN credential.
- **License plate:** Enter a cardholder's license plate number. Use this method if a Sharp camera is being used to trigger a vehicle access barrier. In this case, the cardholder's vehicle license plate can be used as a credential.
- **Request card:** Request a credential card for the cardholder or visitor. Use this method if you do not have a printer on site.
- **Mobile credential:** Request a mobile credential for the cardholder or visitor. You must have a mobile credential provider set up and mobile credential readers installed. The cardholder must have a valid email address configured.
- **Paper credential (print):** Print a badge (name tag or photo ID card) without assigning a credential. The paper credential cannot be used to open doors. It is only used to visually identify the cardholder or visitor.

4 If you select **Automatic entry**, select a reader (USB reader or a door) and present the card at the reader.



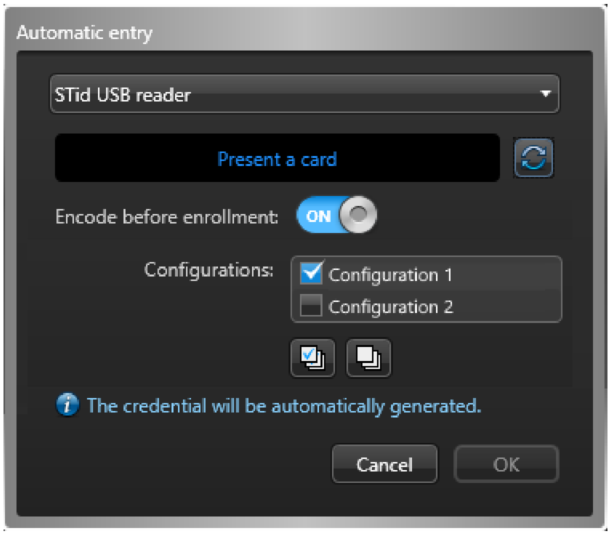
If you have a smart card encoding reader set up, do one of the following:

- To read a pre-encoded card, turn off the **Encode before enrollment** option. When the reader LED turns green (ready to read), place the smart card on the reader. The reader LED turns yellow and then green with a short beep before turning off.



- To generate and encode on your card a random 128-bit MIFARE DESFire credential before enrolling it, turn on the **Encode before enrollment** option and select at least one configuration with a credential. When the reader LED turns red (ready to encode), place the smart card on the reader for approximately 2 seconds. The reader LED turns yellow and then green with a short beep before turning off. If you hear a long beep and the LED stays red, try again.

NOTE: Your Security Center license must support smart card encoding.



Automatic entry

STid USB reader

Present a card

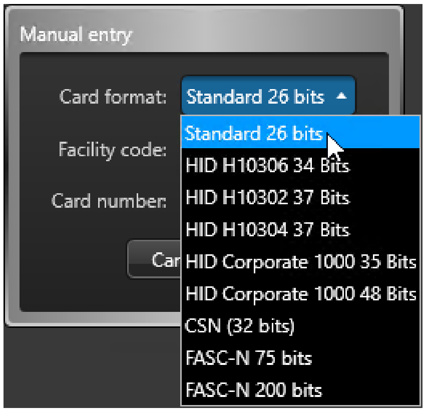
Encode before enrollment: ON

Configurations: ☑ Configuration 1 □ Configuration 2

The credential will be automatically generated.

The dialog box closes automatically after an eligible card is presented. If the card has not been enrolled, it is enrolled automatically. If the card was already assigned to someone, it is rejected.

5 If you select **Manual entry**, you must then select a card format, enter the required data fields, and click **OK**.



Manual entry

Card format: Standard 26 bits

Facility code:

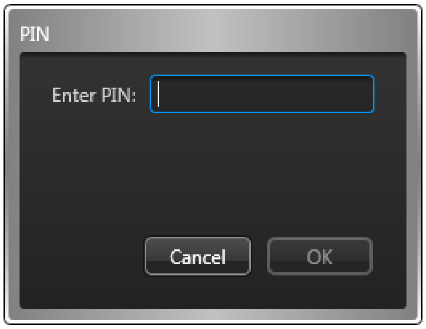
Card number:

CAUTION: Enter your card data carefully because the system cannot validate whether the data you entered correspond to a physical card or not.

If the card has not been enrolled, it is enrolled automatically. If the card was already assigned to someone, it is rejected.

6 If you select **Existing credential**, a dialog box listing all existing but unassigned credentials in the system appears. Select an unassigned credential from the list, and click **OK**.

7 If you select **PIN**, do the following:

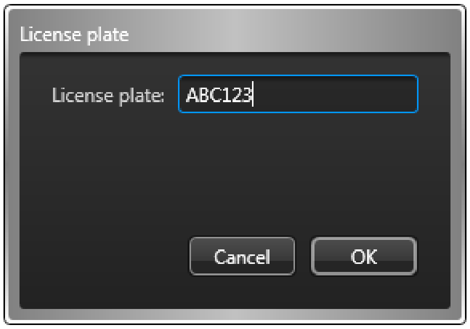


a) Enter the PIN as a numerical value.

NOTE: Do not exceed the number of digits accepted by your readers. A typical PIN length is five digits. But certain models accept up to 15 digits.

b) Click **OK**.

8 If you select **License plate**, you must then do the following:



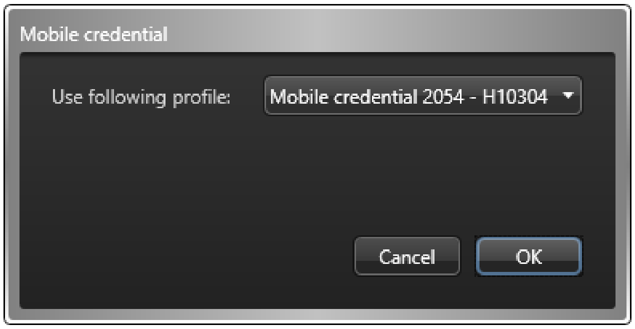
License plate: ABC123

a) Enter the license plate number.

NOTE: You do not need to enter spaces in the license plate number. The system treats "ABC123" and "ABC 123" as the same plate.

b) Click **OK**.

9 If you select **Mobile credential**, you must then do the following:



Use following profile: Mobile credential 2054 - H10304

a) Select the credential profile if there is more than one.

You can assign one mobile credential from each profile to the cardholder.

b) Click **OK**.

NOTE: An email invitation is sent to the cardholder with a link to download the mobile credential app. The cardholder must accept the invitation for the credential to be *activated* on their phone. If the cardholder declines the invitation or if the invitation times out, the credential remains *unused*, and the mobile credential provider can assign it to the next cardholder who needs one. Security Center does not know that the requested mobile credential has not been accepted by the cardholder until the same mobile credential is assigned to someone else, at which time, Security Center automatically removes it from the current cardholder.

IMPORTANT: A mobile credential that has been activated (paired to a phone) can never be reused on another phone. If a cardholder loses their phone or needs to change their phone, they must inform the Security Center operator who must delete the credential or flag it as *lost*. After that, the operator must log on to the credential provider's portal and *revoke* the mobile credential.

10. After the credential is assigned, it appears in the *Credential* section.

    The credential name and status are displayed. *Active* indicates the credential is assigned.

    NOTE: If the credential is a PIN, the keypad icon is displayed. If the credential is a license plate, a license plate icon is displayed. If the credential is a card, a default *badge template* is assigned, and a print preview of the badge is displayed instead of the credential icon.

11. (Optional) If the credential is a card, select a different badge template as follows.
    a) In the *Credential* section, click the badge image.
    b) Select a badge template, and then click **OK**.

       A print preview of the badge appears, with data corresponding to the current cardholder or visitor and their credential.

12. Click **Save**.

    You must save all your changes before you can print the badge.

13. To print the badge, click **Print badge** next to the badge preview.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

Related Topics

Designing badge templates on page 888

Setting up mobile credential profiles on page 876

ALPR access control on page 1048

Requesting credential cards

When you are not in possession of the credential cards, you can request the credential cards to be assigned to the cardholders and visitors you are managing by someone else.

What you should know

You can request a card while you are creating a new cardholder or visitor, or after they are created. In this procedure, it is assumed you have already created a cardholder or visitor.

NOTE: You can only manage visitors in Security Desk.

To request a credential card:

1. Do one of the following:
   - For cardholders, open the *Cardholder management* task, select a cardholder, and then click **Modify** (✏).
   - For visitors, open the *Visitor management* task, select a visitor, and then click **Modify** (✏).
2. In the *Credential* section, click **Add a credential** (➕).
3. From the drop-down menu, click **Request card**.

4. In the *Request card* dialog box, select the reason why you are requesting a card.

   NOTE: Card request reasons only appear if your administrator has created possible reasons in Config Tool.

5. From the **Badge template** list, select a badge template.

   You only need to select a badge template if you want a badge to be printed.

   A print preview of the badge appears.

6. In the **Activate** option, select when to activate the credential.

   - **Never:** The credential will never be activated.
   - **After enrollment:** After another user responded to the card request.
   - **On:** Select a specific date to activate the credential.

7. If you want to receive an email when the credential has been printed, select the **Email me when the card is ready** option.

   NOTE: For this option to work, your user must have a valid email address.

8. Click **OK**.

   The credential is shown as **Requested** in the *Credential* section of the cardholder or visitor details window.

9. Click **Save**.

The **Card requests** (💳) icon appears in the notification tray.

Related Topics

Designing badge templates on page 888

Adding reasons for credential card requests on page 872

Responding to credential card requests on page 873

Printing credential cards in batches

To save time when printing credential cards, you can print them in batches.

Before you begin

Create a badge template.

What you should know

All the credentials you select must be associated with a badge template.

To print credential cards in batches:

1. From the homepage, open the *Credential management* task.
2. Select the credentials you want to print:
   - Hold Ctrl and click specific credentials in the list.
   - Hold Shift and select a range of credentials in the list.
3. Click **Print**.

The selected credentials are printed in the order in which they are listed in the *Credential management* task.

Printing paper credentials

When you do not have credentials assigned to cardholders or visitors, you can print paper credentials (badges without credential data) as name tags or photo IDs for visual identification.

Before you begin

Create a badge template.

What you should know

To print a badge, you need a badge template. A badge template is usually associated with a card credential so that it can be used to unlock doors, but you can also print a badge without any credential data (called a paper credential) that can be used as a name tag or a photo ID for visual identification.

You can print a badge while creating a new cardholder or visitor, or after they are created.

NOTE: You can only manage visitors in Security Desk.

To print a badge:

1. Do one of the following:
   - For cardholders, open the *Cardholder management* task, select a cardholder, and then click **Modify** (✎).
   - For visitors, open the *Visitor management* task, select a visitor, and then click **Modify** (✎).
2. In the *Credential* section, click **Add a credential** (+).
3. In the menu that appears, click **Paper credential (print)**.
4. In the *Badge printing* dialog box, select a badge from the list.

   A print preview of the badge is shown. Cardholder or visitor information might be shown on the badge, depending on how the badge template is designed. No credential data is shown on the badge.
5. To print the paper credential, click **Print badge**.

Related Topics

Designing badge templates on page 888

Setting up smart card encoding stations

If you have a STid USB encoding reader, you can set up a smart card encoding station to generate, encode, and enroll MIFARE DESFire credentials, all from one place.

Before you begin

- Make sure your software license supports both *USB enrollment reader* and *Smart card encoding* options.
- Select a Security Desk workstation as your encoding station.
- Attach the USB encoding reader to your encoding station. See the *Synergis™ Softwire Integration Guide* for supported models.
- Have a MIFARE DESFire card at your disposal and a workstation equipped with the *SECard* software from STid to configure the MIFARE DESFire card as the Secure Key Bundle (SKB) card.

What you should know

The SKB card contains a set of indexed keys as a shared secret between the encoding reader and the readers at the doors. Three keys are needed for the smart card encoding solution to work: the *Card master key*, the *Application master key*, and the *Application read key*. The Security Center applications and the Synergis™ units only need to know where these three keys are stored (location index) on the smart cards, not the values of the keys. This information is saved to a configuration file called *SmartCardSites.xml*, which is found in the Security Center installation folder.

This configuration file comes with the following ready-for-use default settings:

- Application ID = 1
- Encryption method = AES
- File ID = 1
- File name = File 1
- Credential length = 16 bytes (128 bits)
- Credential offset = 0
- Key communication mode = Crypted (encrypted)
- Card master key location index = 1 (on the smart card)
- Application master key location index = 3 (on the smart card)
- Application read key location index = 2 (on the smart card)
- Application master keyhole number = 0
- Application read keyhole number = 1

To set up a smart card encoding station:

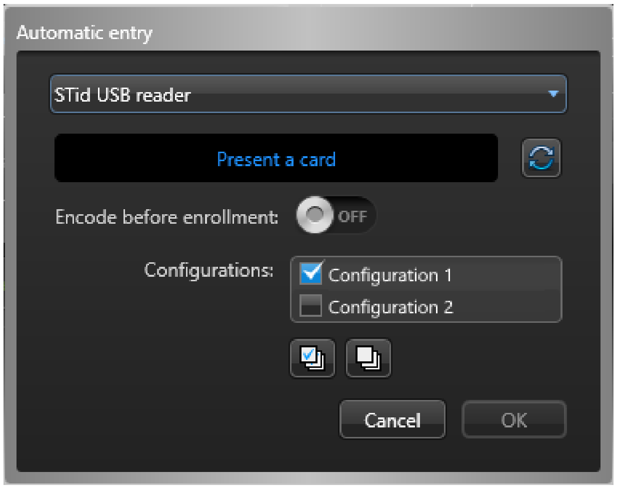
1. Configure your SKB card using the *SECard* software from STid.

   Do one of the following:

   - If it is a new installation, configure the blank MIFARE DESFire card as an SKB card. Use SECard to generate random keys, and the default key configuration settings found in the *SmartCardSites.xml* file.
   - If you have an existing SKB card that you want to use, contact your representative of Genetec Inc. to help you configure the *SmartCardSites.xml* file to match your existing SKB card.

2. Open Security Desk, and enable the STid USB reader.

3 Transfer the keys from the SKB card to the USB reader at your encoding station.
   a) Open the *Credential management* task and click **Create new credential** > **Automatic entry**.
   b) Select **STid USB reader** and turn off the **Encode before enrollment** option.



   The reader LED turns green (ready to read).
   c) Present the SKB card at the reader for approximately 3 seconds.
   The reader LED turns yellow and then green when the keys are transferred. If you hear a long beep, try again.
   d) Click **Cancel**.

4 If it is not a new installation, and if you are not using STid readers at your doors, end here.

5 Upload the *SmartCardsSites.xml* file found on your encoding station to the Synergis units that control the STid smart card readers.

6 Transfer the keys from the SKB card to the smart card readers at the doors.
   Go to each door in your facility, and present the SKB card at each door reader for approximately 3 seconds to enable the reader to read the MIFARE DESFire credentials generated by your encoding reader.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

After you finish

Generate, enroll, and assign MIFARE DESFire credentials to your cardholders.

Modifications to cardholders imported from an Active Directory

If you have cardholders that are imported from an Active Directory, there are a few cardholder properties that you can modify in Security Center.

You can make the following modifications:

- Assign pictures to imported cardholders.
- Assign temporary cards to imported cardholders.
- Modify the status of imported cardholders.

Temporary cards for imported cardholders

If an imported cardholder forgets or loses their card, you can assign them a temporary card in the *Cardholder management* task. When you assign them a temporary card, their credential becomes greyed out in Config Tool until the card is returned. For more information about assigning or returning temporary cards, see the *Security Center User Guide*.

Assigning pictures to imported cardholders

You can assign pictures to imported cardholders from Security Center, and then synchronize the pictures with the Active Directory.

Before you begin

The cardholder *Picture* field must be mapped to the AD attribute *thumbnailPhoto*.

To assign a picture to an imported cardholder:

1. From the *Cardholder management* task, assign a picture to the cardholder.
2. Open the *System* task and click the **Roles** view.
3. Select the Active Directory role, and then click the **Links** tab.
4. Select the **Upload pictures to Active Directory** option, and set the **Maximum uploaded picture file size** (default=20 KB).
5. Click **Apply**.
6. Click the **Properties** tab, and then click **Synchronize now**.

   NOTE: If Security Center synchronizes with the AD based on a scheduled task, then the next time the synchronization occurs, the new cardholder picture is synchronized with the AD.

Modifying the status of imported cardholders

You can modify the status and expiration date of an imported cardholder in Security Center. The cardholder becomes desynchronized from the AD.

To modify the status of an imported cardholder:

1. Open the **Access control** task.
2. Select an imported cardholder (👤), and click the **Properties** tab.
3. In the **Status** section, move the slider from **Keep synchronized** to **Override**.

4 Set the cardholder’s status and expiration date:

- **Status:** Set their status to *Active* by clicking **Activate**, or *Inactive* by clicking **Deactivate**. For their credentials to work, and for them to have access to any area, their status must be *Active*.
- **Activation:** Displays the current date.
- **Expiration:** Set an expiration for their profile:
  - **Never:** Never expires.
  - **Specific date:** Expires on a specific date and time.
  - **Set expiration on first use:** Expires a specified number of days after the first use.
  - **When not used:** Expires when it has not been used for a specified number of days.

5 Click **Apply**.

The cardholder is no longer synchronized with the AD. It will only become synchronized again once you set the cardholder’s status to **Keep synchronized**.

Using signature pads

If you have a signature pad attached to your computer, you can use it to capture cardholder and visitor signatures, and save them directly to a signature custom field that was created beforehand.

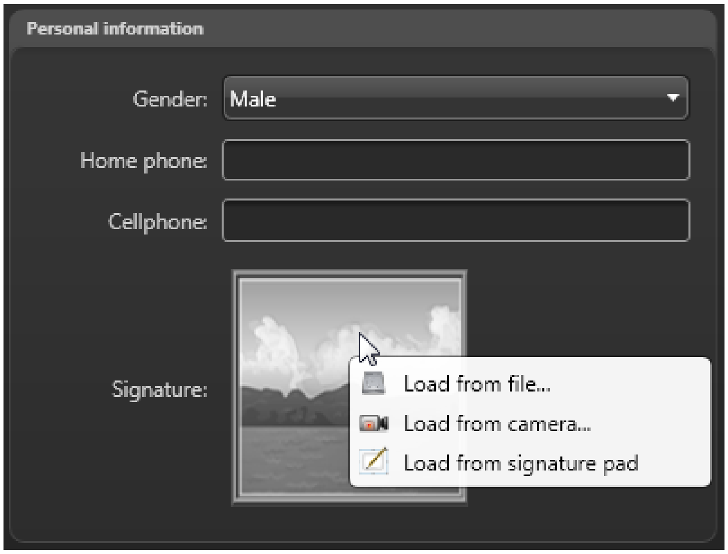
Before you begin

- Make sure cardholder and visitor signature custom fields have been created with the *Image data* type.
- Attach a Topaz signature pad to your computer, and enable it in Security Desk.

To use a signature pad:

1 Open the *Cardholder management* task or *Visitor management* task to create or modify the cardholder or visitor.

2 In the property dialog box, click the custom field reserved for the signature and select **Load from signature pad**.



Personal information

Gender: Male

Home phone:

Cellphone:

Signature:

3 Hand the signature pad to the cardholder or visitor and ask them to sign.

The captured signature appears in the signature field.

4 Click **Save**.

Time zones for cardholder and visitor activation and expiration

You can configure the activation and expiration of cardholders and visitors to follow a specific time zone by using a custom field. This can be configured in the *Cardholder management*, *Visitor management*, and *Access control* tasks, and viewed in the *Credential management* task.

Configured time zones are not taken into consideration for values imported through the Import tool, created through SDK macros, or synchronized from Active Directory roles because the activation and expiration times are saved in the database in UTC.

Requirements

The minimum required Security Center version to use cardholder and visitor time zones is 5.10.3.0. All your client workstations must meet this requirement.

About time zones for credentials

- Credentials inherit the time zone of the cardholder or visitor that the credentials are assigned to. The activation and expiration dates of unassigned credentials are based on the local time zone on the client workstation.
- When assigning and re-assigning credentials, their activation and expiration might not get updated to follow the time zone of the cardholder or visitor time zone. You must validate that the activation and expiration values are correct.

Limitation

In the report pane of tasks that can list cardholder and visitor activation and expiration, times are displayed in the local time zone of the client workstation, not the time zone that is specified for the cardholder or visitor.

Removing the option for cardholders and credentials to never expire

By default, the expiration of cardholders and credentials is set to **Never**. You can force cardholders and credentials to have an expiration by removing the **Never** option with a setting in Config Tool.

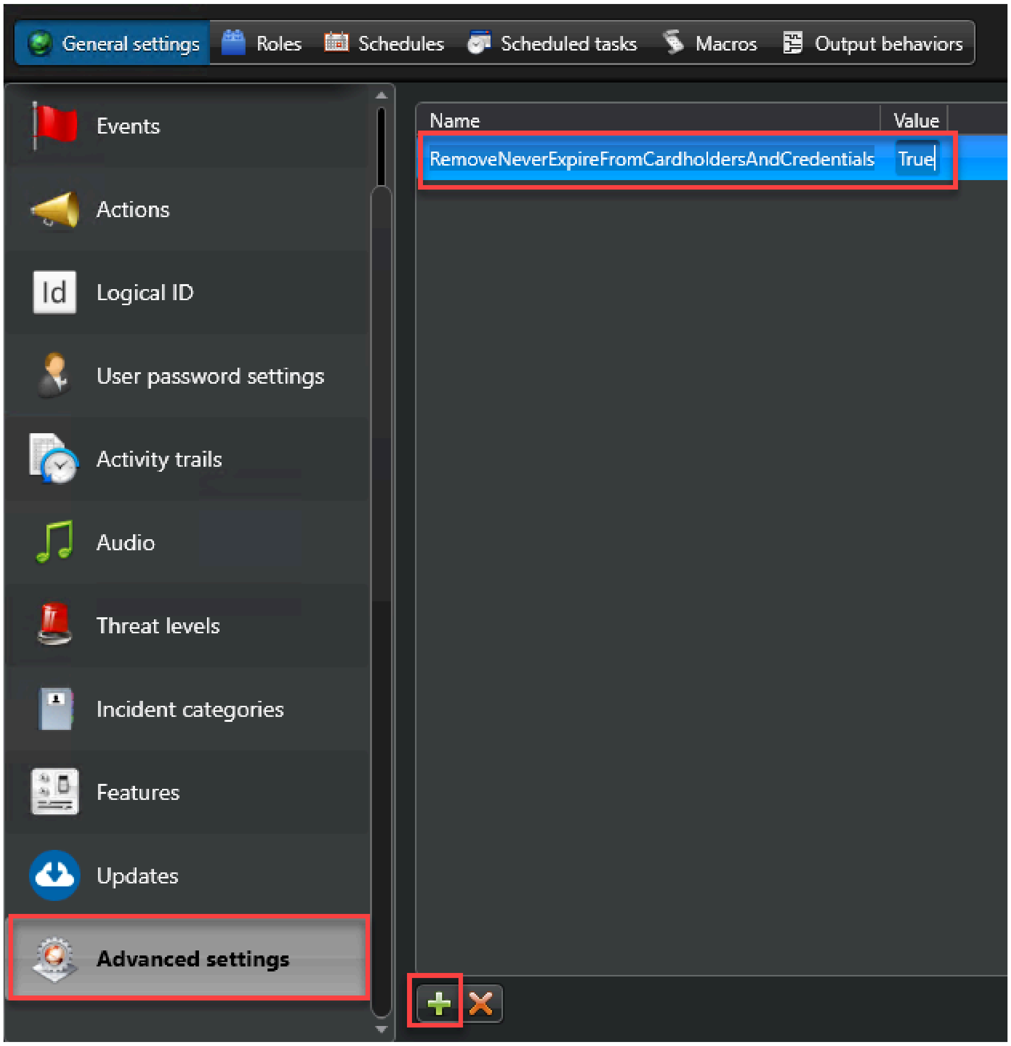
What you should know

- You can only remove the **Never** option from Config Tool and Security Desk. The SDK is unaffected by this change.
- Removing the **Never** option does not affect the expiration of existing cardholders and credentials that were set to never expire. An invalid status warning and an error in the expiration is displayed, but you must manually select a new expiration option for those cardholders and credentials.

To remove the option for cardholders and credentials to never expire:

1. From the Config Tool home page, open the *System* task, and click the **General settings** view.
2. Click the **Advanced settings** tab.
3. Click **Add an item** (➕).
4. In the **Name** field, enter `RemoveNeverExpireFromCardholdersAndCredentials`.

5 In the **Value** field, enter `True`.

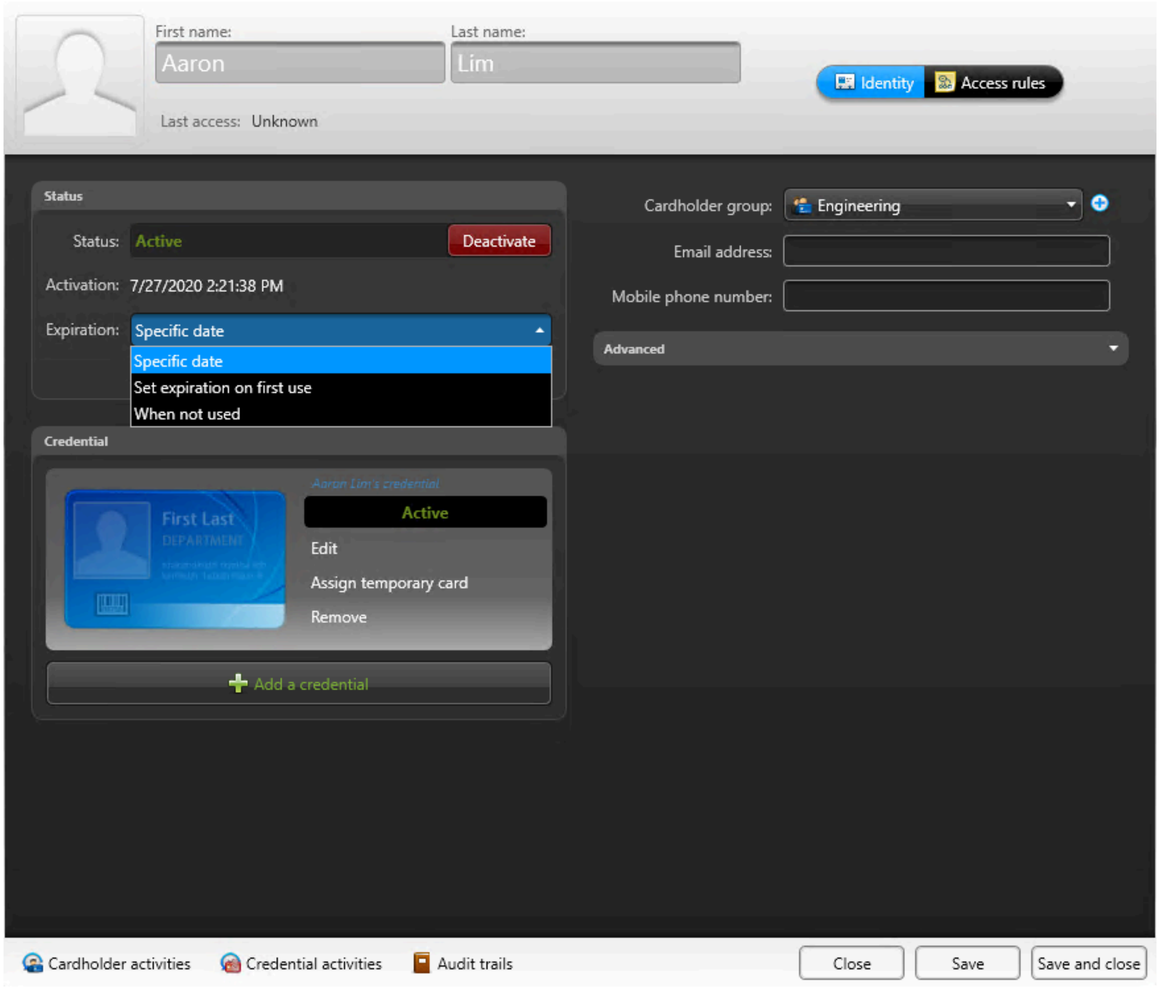


Name	Value
RemoveNeverExpireFromCardholdersAndCredentials	True

6 Click **Apply**.

7 Restart Config Tool and Security Desk.

The **Never** option is no longer visible.



First name: Aaron

Last name: Lim

Last access: Unknown

Status

Status: Active

Activation: 7/27/2020 2:21:38 PM

Expiration: Specific date

Credential

Aaron Lim's credential

Active

Cardholder group: Engineering

Email address:

Mobile phone number:

Creating a custom data type for time zones

To ensure that you enter valid time zone names when configuring time zones for cardholder and visitor activation and expiration, create a custom data type containing all the time zones you want to use.

What you should know

It is recommended to generate a list of time zones used by Windows to create the custom data type because time zones entered in the *Cardholder Time Zone* and *Visitor Time Zone* custom fields are not validated. If you enter an invalid value in the custom field, the local time of the client workstation is used, and you are not notified that the value is invalid.

To create a custom data type for time zones:

1. Generate a list of time zones from Windows, using a PowerShell command line.
   a) Open Windows PowerShell.
   b) Enter the following command line:
   ```
   get-timezone -ListAvailable | Format-Table -property ID -HideTableHeaders | Out-File C:\Genetec\TimzoneIDs.txt
   ```
   c) Press Enter to generate the list.

   Open the *TimeZoneId.txt* file that was generated in *C:\Genetec*. You can copy-paste the time zones you need from this file as values for the custom data type in Security Center.
2. From the Config Tool home page, open the *System* task, and click the **General settings** view.
3. Click the **Custom fields** tab, and then click the **Custom data types** tab.
4. Click **Add an item** (+) at the bottom of the custom data types list.
5. In the *Creating a custom data type* wizard, configure the following parameters on the *Basic information* page:
   - **Name:** Enter a name for the custom data type. For example, `Time zones`.
   - **Description:** Enter a description for the custom data type.
   - **Type:** Select **Text**.
6. Click **Next**.
7. On the *Data entry* page, click **Add an item** (+).
8. In the **Value** field of the dialog box, enter a time zone from the list you generated, and click **OK**.
   The value is added to the list.
9. Add more time zones as required.
10. When you are finished, click **Next**, **Next**, and **Close**.

After you finish

Create time zone custom fields for cardholder and visitor activation and expiration.

Creating time zone custom fields for cardholder and visitor activation and expiration

Before you can configure time zones for the activation and expiration of cardholders and visitors, you must create cardholder and visitor custom fields.

Before you begin

- Learn about time zones for cardholder and visitor activation and expiration.
- Create a custom data type for time zones.

What you should know

The minimum required version to use cardholder and visitor time zones is 5.10.3.0. Ensure that all your client workstations meet this requirement.

To create time zone custom fields for cardholder and visitor activation and expiration:

1 From the Config Tool home page, open the *System* task, and click the **General settings** view.

2 Click the **Custom fields** tab, and click **Add an item** (➕).

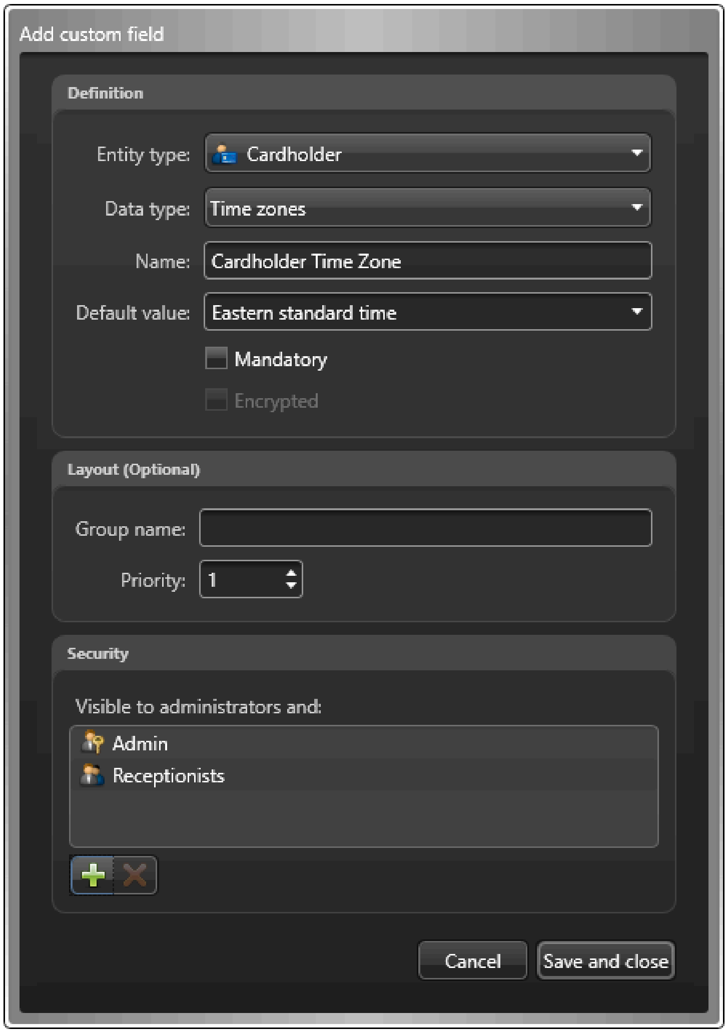
3 In the *Add custom field* dialog box, configure the following settings:

   - **Entity type:** Select **Cardholder** or **Visitor**, as required.
   - **Data type:** Select the custom *Time zones* data type you created.
   - **Name:** If you selected **Cardholder** as the entity type, enter `Cardholder Time Zone`. If you selected **Visitor** as the entity type, enter `Visitor Time Zone`.

NOTE: The system looks for these exact English values. The custom fields will not work if you name them differently.

- **Default value:** Select a time zone from the list to use as the default time zone.
- **Visible to administrators and:** Add the users or user groups that need to configure the activation and expiration of cardholders and visitors, otherwise, these users will only see the activation and expiration times in their local time.

Example:



Add custom field

Definition

Entity type: Cardholder

Data type: Time zones

Name: Cardholder Time Zone

Default value: Eastern standard time

□ Mandatory

□ Encrypted

Layout (Optional)

Group name:

Priority: 1

Security

Visible to administrators and:

Admin

Receptionists

4 Click **Save and close**.

After you finish

Configure the time zones for cardholders and visitors.

Configuring time zones for cardholder and visitor activation and expiration

You can change the time zone in which the activation and expiration of cardholders and visitors are displayed.

Before you begin

Create time zone custom fields for cardholders and visitors.

To configure the time zone for a cardholder in the Cardholder management task:

1 From the Security Desk or Config Tool home page, open the *Cardholder management* task.

2 Double-click a cardholder, and then select a time zone from the **Cardholder Time Zone** list.

3 If no other changes are required, click **Save and close**.

NOTE: If you want to edit a credential in the same window, make sure to click **Save** first.

To configure the time zone for a cardholder in the Access control task:

1 From the Config Tool home page, open the *Access control* task, and click the **Cardholders and credentials** view.

2 Select a cardholder, and click the **Custom fields** tab.

3 From the **Cardholder Time Zone** list, select a time zone.

4 Click **Apply**.

To configure the time zone for a visitor in the Visitor management task:

1 From the Security Desk home page, open the *Visitor management* task.

2 Double-click a visitor, and then select a time zone from the **Visitor Time Zone** list.

3 If no other changes are required, click **Save and close**.

NOTE: If you want to edit a credential in the same window, make sure to click **Save** first.

Receiving notifications when cardholders are expiring

You can configure Security Center to send you or another user an email before cardholders or their credentials expire.

Before you begin

If you want the user to be notified by email, make sure they have a valid email address.

What you should know

Users can be notified for every cardholder or credential that is expiring soon, or only for specific entities.

If a cardholder expires, their credential is no longer valid.

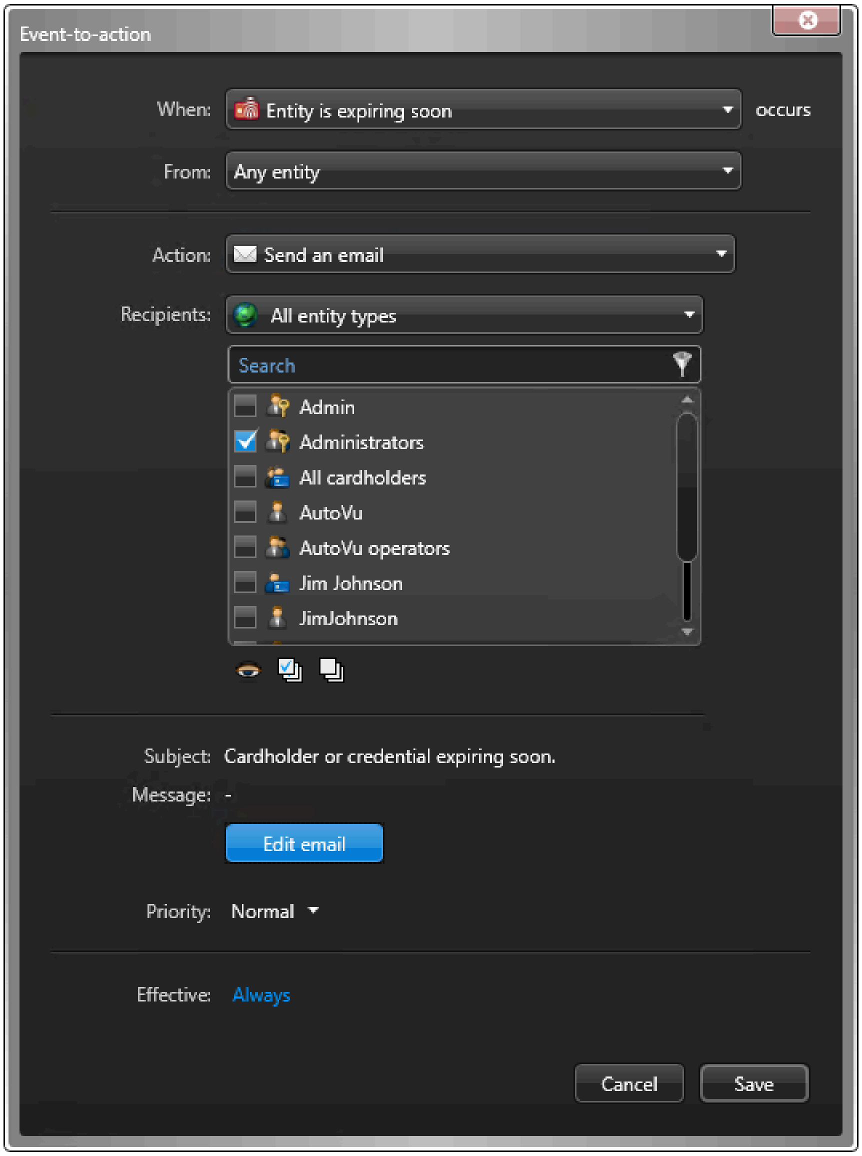
To receive a notification when a cardholder or their credential is expiring:

1. Open the *Access control* task, and click the **General settings** view.
2. Turn on the **Trigger event 'Entity is expiring soon'** option, and select how many days prior to the expiration to trigger the event.
3. Click **Apply**.
4. Open the *System* task, and click the **General settings** view.
5. Click **Actions** and then click **Add an item** (+).

   The *Event-to-action* dialog box opens.
6. In the **When** list, select **Entity is expiring soon**.
7. (Optional) Select an entity in the **From** list.

   CAUTION: Make sure that the entity you select is the one you want to monitor. If you select a cardholder, and it is the credential that is expiring soon, the event-to-action will not be executed.

8 In the **Action** list, select **Send an email**, then select the **Recipients**, edit the email, and set the **Priority**.



When: Entity is expiring soon occurs

From: Any entity

Action: Send an email

Recipients: All entity types

- □ Admin
- ☑ Administrators
- □ All cardholders
- □ AutoVu
- □ AutoVu operators
- □ Jim Johnson
- □ JimJohnson

Subject: Cardholder or credential expiring soon.

Message: -

Priority: Normal

Effective: Always

9 Click **Save**.

10 If necessary, change the time range when this event-to-action is in effect.

The recipient is sent an email the specified number of days before the entity expires.

Credentials

This section includes the following topics:

About credentials

A credential entity represents a proximity card, a biometrics template, or a PIN required to gain access to a secured area. A credential can only be assigned to one cardholder at a time.

The credential entity represents a proximity card, a biometrics template, or a PIN. Credentials are used by Security Center to identify who is requesting access through a secured access point. Credentials are *claims of identity*. A credential distinguishes one cardholder from another. For access control to be operational, every cardholder must have at least one credential. These are typically (but not exclusively) access control cards.

The required credential depends on the type of reader installed at the door.

Security Center native card formats

Security Center supports a few standard card formats.

For card formats, a card number is always required. Depending on the card format, the facility code might not be necessary. The following table describes the standard card formats supported by Security Center, and the valid ranges for the facility code (also known as *Company ID Code*) and card number (also known as *Card ID Number*).

Card format	Facility code range	Card number range
Standard 26 bits	0 to 255	0 to 65 535
HID H10306 34 bits	0 to 65 535	0 to 65 535
HID H10302 37 bits	Not required[1]	0 to 34 359 738 367
HID H10304 37 bits	0 to 65 535	0 to 524 287
HID Corporate 1000 35 bits	0 to 4095	0 to 1 048 575
HID Corporate 1000 48 bits	0 to 4 194 303	0 to 8 388 607
CSN 32 bits	Not required	0 to FFFFFFFF
FASC-N 75 bits[2]	-	-
FASC-N 200 bits[2]	-	-

[1] If HID H10302 37 Bits is the only card format referenced in your CSV file, it is preferable to bind the card number to the Security Center Card data field instead of the Card number field because the facility code is not required. Because a single value is stored in the Credential card data field, no separator character is needed.

Custom card formats can also be defined using the *Custom format editor* tool.

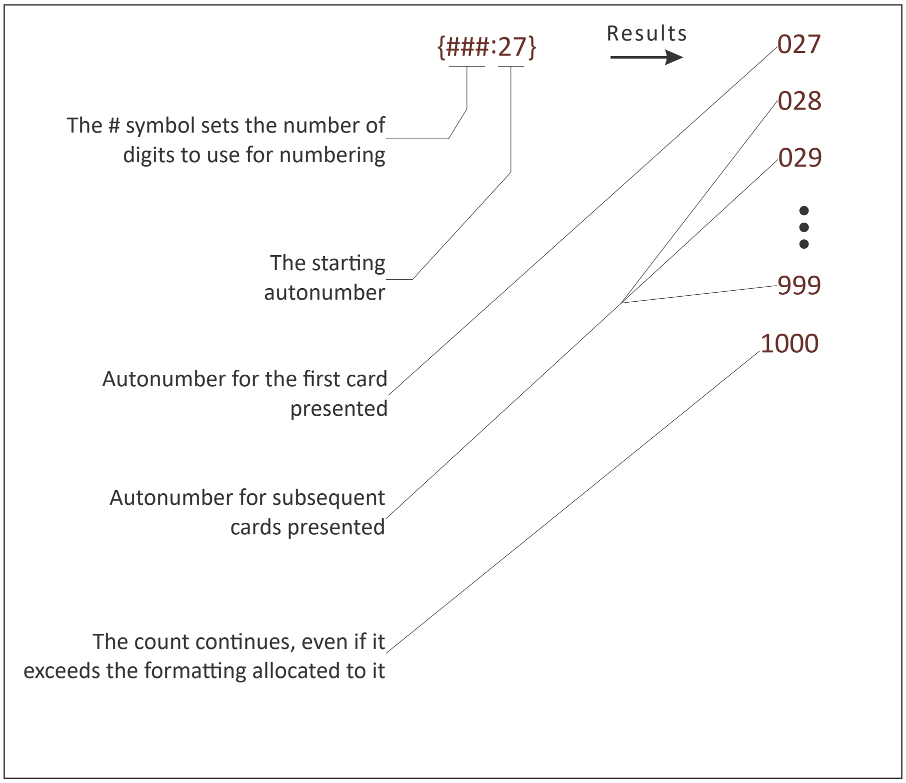
[2] See How credential card formats work with Active Directory in Security Center on page 880 for information on FASC-N 75 bits and FASC-N 200 bits formats.

The credential prefix and the counter

The **Credential prefix** sets the name of enrolled credentials. The *Credential management* task ensures that all enrolled credentials have a unique name by automatically adding a number to the name set in **Credential prefix**. You can also control the counter by adding an autonumber format (between curly brackets) to the credential prefix.

The credential autonumber format defines the counter style. The autonumber format can be placed anywhere in the credential prefix. Only one autonumber format can be used in the credential prefix at a time.

The autonumber format is explained in the following image:


{###:27}
Results
027
028
029
999
1000
The # symbol sets the number of digits to use for numbering
The starting autonumber
Autonumber for the first card presented
Autonumber for subsequent cards presented
The count continues, even if it exceeds the formatting allocated to it

The following are examples for the autonumber format:

Credential prefix	Credential sequence generated	Comments
Credential_	Credential_0 Crediential_1 Credential_2	When the autonumber format is omitted, the autonumber is appended at the end of the prefix and starts at 0.
Credential #{##:1}	Credential #01 Credential #02 Credential #03	A basic autonumber for the credential prefix.
1{####:46} 11203162-2	10046 11203162-2 10047 11203162-2 10048 11203162-2	Enrolled credentials can be autonumbered in Security Center so their names correspond to the serial number printed on the back of a series of cards.

PIN recommendation

When using PIN as a credential, you can use it either with a card (Card and PIN) or on its own (Card or PIN). Your reader capabilities and configuration determine how the PIN is required.

If you plan to use your readers in a Card or PIN mode, ensure that the PINs are unique for all cardholders and that there are no duplicates in the system. Duplicate PINs can lead to confusion as there is no way to determine which cardholder it belongs to when a user enters it in at the door.

License plate recommendation

If you plan to use hard antipassback, maximum occupancy, or people counting features, you should not have duplicate license plate credentials in your system. The license plate should be unique for each cardholder because when more than one cardholder uses the same license plate as a credential, there is no way to determine which cardholder the credential belongs to.

For example, if *Cardholder A* enters an area using a license plate credential, and *Cardholder B* exits the area using a credential with the same license plate, *Cardholder A* might be moved out of the area instead of *Cardholder B*.

Raw credentials

In Security Center 5.8 or later, any credential reads that do not match a native card format or a custom card format is recognized and displayed as **Raw [n] bits**, where *[n]* is the bit length of the card.

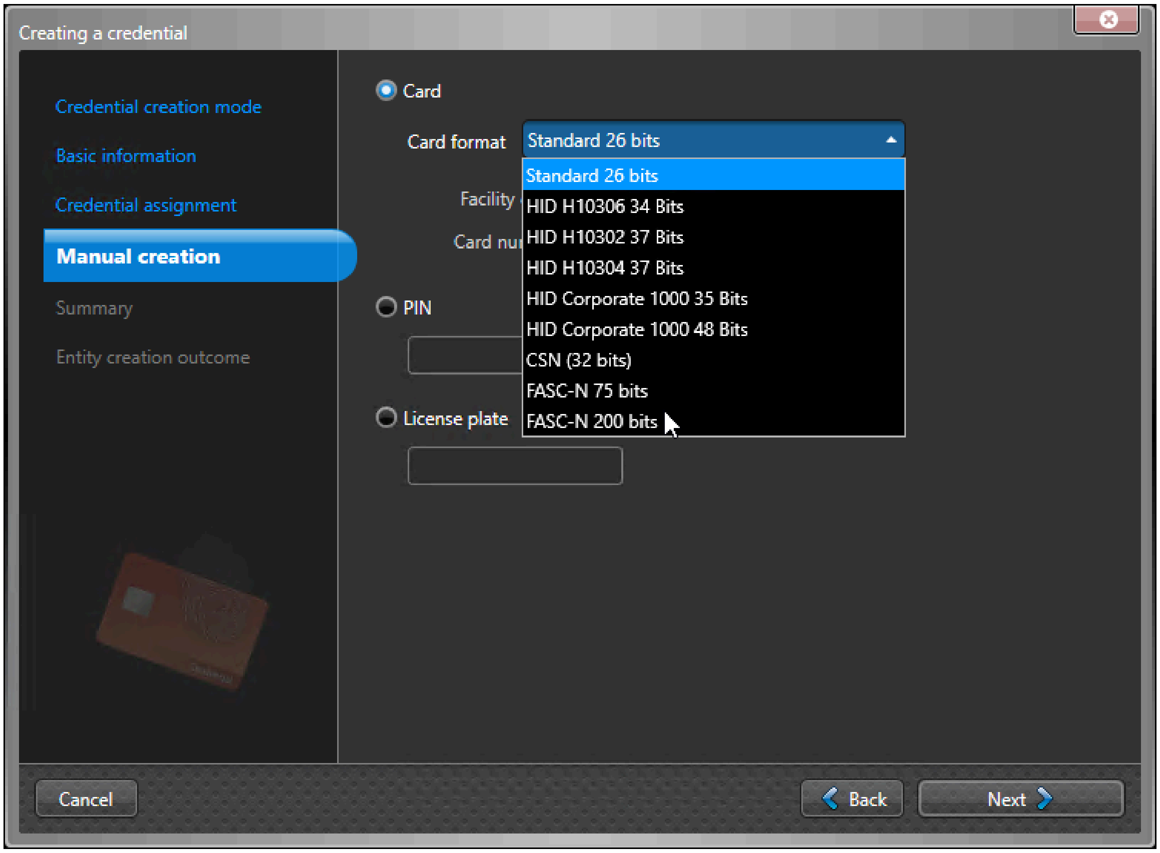
About FASC-N credentials

A Federal Agency Smart Credential Number (FASC-N) is an identifier used in the Personal Identity Verification (PIV) credentials issued by US Federal Agencies. FASC-N credential bit lengths vary based on reader configuration; Security Center natively recognizes 75-bit and 200-bit formats.

Creating credentials

For PIV credentials, you can select either the FASC-N 75 bits or FASC-N 200-bit format while manually generating a credential in Config Tool or Security Desk.

NOTE: 200-bit FASC-N is also called Full FASC-N.



● Card

Card format: Standard 26 bits

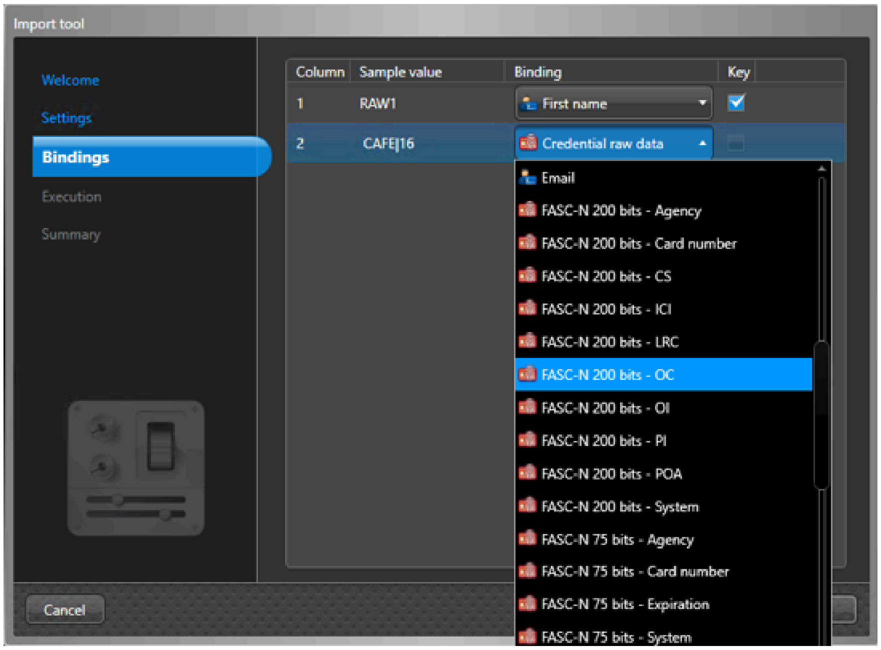
In Security Desk, you can use **Batch enrollment** in the *Credential management* task to create multiple FASC-N or GUID data. For more information, see "Enrolling multiple credentials automatically" in the *Security Center User Guide*.

Security Center recognizes CIV or PIV-I credentials as RAW 128-bit credentials, which can be mapped to a custom card format.

Import tool and SDK

The FASC-N formats are also available through the *Import tool* and the Security Center SDK.

When importing, select the **Credential raw data** binding.



Column	Sample value	Binding	Key
1	RAW1	First name	☑
2	CAFE|16	Credential raw data	□

NOTE: If you do not associate a card format while importing data, a credential will be generated with an empty Global Unique Identifier, or GUID.

Configuring MIFARE DESFire in Security Center

To encode MIFARE DESFire key cards or re-encode cards that were configured with a third-party production tool, you must create the configuration in Config Tool.

Before you begin

Ensure that your Security Center license supports MIFARE DESFire configuration.

What you should know

MIFARE DESFire EV1/EV2 is a 128-bit, Advanced Encryption Standard (AES)-based protocol for which you define the keys.

To configure MIFARE DESFire:

1. From the Config Tool homepage, open the *MIFARE DESFire configuration* task.
2. From the **MIFARE DESFire configuration** list, click **Add an item** (➕).

   Each MIFARE DESFire configuration corresponds to one application.
3. In the *Badge configuration* section, enter a name in the **Configuration name** field, and then do one of the following:
   - To enable Security Center to recognize a pre-encoded card, complete the fields to match the card.
   - To encode a new card or re-encode an existing card, select the **Card encoding** checkbox, and then set the values for your new configuration.

     For more information about how to encode cardholder information on the card, see Encoding cardholder information on MIFARE DESFire cards on page 855.

     NOTE: Enabling **Card encoding** opens three options for the kind of configuration file that you will create.
4. If you are encoding or re-encoding a card, select an option:
   - **Format card:** Delete all information on the card before creating an application.
   - **Free create:** Enable the creation of applications even when the card master key is unknown.
   - **Old application master key:** Change the master key of the application on the card.
5. Click **Save**.

   If you have multiple configurations in the **MIFARE DESFire configuration** list, selecting a configuration activates it.
6. Verify the configuration:

   a) Click the **Test USB reader** tab.

   b) Select a configuration from the **MIFARE DESFire configuration** list.

   c) Click **Read mode**.

   d) Badge a card.

   If the card matches the active configuration, it is read properly. If the card uses a different configuration than the one you selected, it returns a failed read.
7. To encode or re-encode a card:

   a) Click the **Test USB reader** tab.

   b) Select a configuration from the **MIFARE DESFire configuration** list.

   c) Click **Write mode**.

   d) Badge a card.

   The card is encoded or re-encoded to match the active configuration.

After you finish

Export the MIFARE DESFire configurations to a *SmartCardsSites.xml* file or directly to Synergis™ Cloud Link units.

Exporting MIFARE DESFire configurations

You can export MIFARE DESFire configurations to a *SmartCardsSites.xml* file or directly to Synergis™ Cloud Link units, using the *MIFARE DESFire configuration* task.

Before you begin

Ensure the following:

- Your Security Center license supports MIFARE DESFire configuration.
- You are granted the *Export configurations and keys* user privilege.

To export MIFARE DESFire configurations to a SmartCardsSites.xml file:

1. From the Config Tool home page, open the *MIFARE DESFire configuration* task.
2. On the *Configuration* page, under the **MIFARE DESFire configuration** list, click **Export to file** and save the *SmartCardsSites.xml* file to your local hard drive.
3. Log on to the Synergis™ Appliance Portal and upload the *SmartCardsSites.xml* file to your Synergis™ unit.

   For more information, see "Configuring MIFARE DESFire" in the *Synergis™ Appliance Configuration Guide* or the *Synergis™ Cloud Link Administrator Guide*.
4. Copy the *SmartCardsSites.xml* file to the Security Center installation folder of each workstation being used to configure MIFARE DESFire credentials.

To export MIFARE DESFire configurations directly to Synergis Cloud Link units:

1. From the Config Tool home page, open the *MIFARE DESFire configuration* task.
2. On the *Configuration* page, under the **MIFARE DESFire configuration** list, click **Export to units**.
3. In the *Unit selection* dialog box, select one or more Synergis Cloud Link units to export the configuration to.
4. Click **Export**.
5. In the Synergis™ Appliance Portal, verify the updated configuration by clicking **Configuration** > **MIFARE DESFire**.

   In the *Readers and associated MIFARE DESFire configurations* section, the configurations you exported are added to the **Available configurations** list for each reader.

Encoding cardholder information on MIFARE DESFire cards

To accelerate cardholder creation and prevent typos when copying a cardholder onto another system, you can encode cardholder information on a MIFARE DESFire card. When assigning the card to a new cardholder on the other system using a STid reader, the cardholder fields are automatically populated by the values encoded on the card.

Before you begin

Ensure the following:

- Your Security Center license supports MIFARE DESFire configuration.
- A smart card encoding station is set up.

What you should know

- Cardholder information is encoded on MIFARE DESFire cards by configuring custom string files in MIFARE DESFire configurations. The information defined in the custom strings is then retrieved from an existing cardholder. Each custom string file contains at least one custom string that defines information about the cardholder from fields such as first name, email address, cardholder custom fields, manually entered values, and so on.
- Each MIFARE DESFire configuration defines one application.
  - You can store up to 28 applications on a DESFire EV1 card, or as many applications as there is space on EV2 and EV3 cards.
  - An application can be empty (for future use) or contain up to 32 files.
  - A file can be empty (for future use) or contain a credential or a custom string.
- Security Center 5.11.3.0 or later is required to perform this task.

IMPORTANT: When you encode credentials on a MIFARE DESFire card in Security Center, you must always select at least one configuration with a credential.

To encode cardholder information on a MIFARE DESFire card:

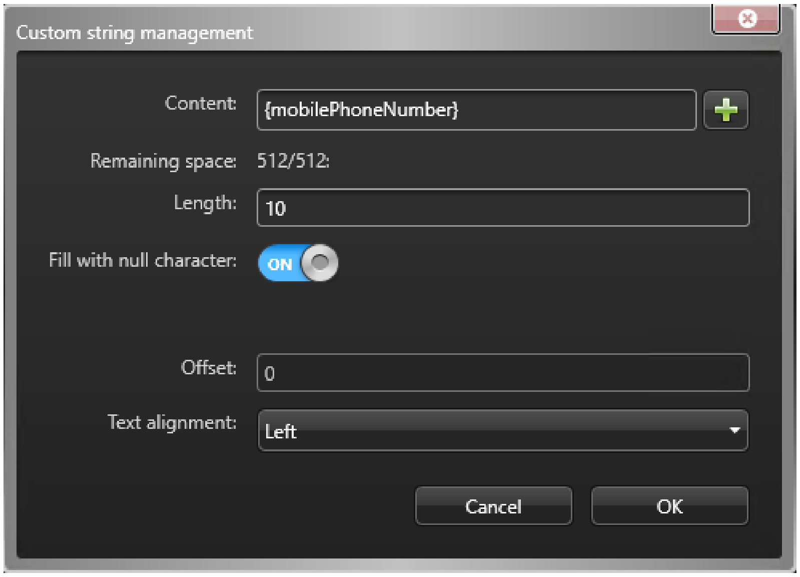
1. From the Config Tool home page, open the *MIFARE DESFire configuration* task.
2. From the **MIFARE DESFire configuration** list, and then click **Add an item** (➕).
3. In the *Badge configuration* section, enter a **Configuration name**.
4. Select the **Card encoding** check box.
5. Add a custom string file to the application:
   a) At the bottom of the *File selection* section, click **Add an item** (➕).
   b) (Optional) In the *File details* section, enter a **File ID** and **Name** for the custom string file.
   c) Select a value from the **Communication settings** list, and then configure a **Read key** and a **Write key**, or a **Read-write key**.
   d) From the **Type** list, select **Custom string**.
   e) In the *File details* section, select **Custom string** from the **Type** list.

6 Add at least one custom string to the custom string file to define what cardholder information to encode:

a) In the *Custom string* section, select **UTF-16** or **ASCII** from the **Encoding** list, and then click **Add an item** (➕).

b) In the *Custom string management* dialog box, configure the following:

Example:



Custom string management

Content: {mobilePhoneNumber}

Remaining space: 512/512:

Length: 10

Fill with null character: ON

Offset: 0

Text alignment: Left

- **Content:** Click **Add an item** (➕) and select the cardholder information that you want to store on the card.
- **Remaining space:** The number of characters remaining in the file over the total number of characters permitted.
- **Length:** Enter the maximum number of characters that you want the content to take up in the file.
- **Fill with null character:** When the option is on, if the value of the content does not use the maximum number of characters defined in the **Length**, the null character is used to fill the remaining space.

  When the option is off, the **Fill** field is displayed, and you can enter different characters to use instead of the null character.
- **Offset:** Where the custom string starts in the file.
- **Text alignment:** Whether to align the text to the left or to the right.

c) Click **OK**.

The custom string is added to the custom string file in the *File selection* section.

7 Add more custom strings to the custom string file, as required.

8 Click **Save**.

9 Encode the cardholder information and MIFARE DESFire credential on the card:

NOTE: Ensure that the *MIFARE DESFire configuration* task is not open on the *Test USB reader* page. This prevents you from using the STid reader in the *Cardholder management* task.

a) Open the *Cardholder management* task, and select the cardholder from which you want to retrieve the cardholder information.

b) Click **Add a credential** > **Automatic entry**.

c) In the *Automatic entry* dialog box, select **STid USB reader**, and ensure that the **Encode before enrollment** option is on.

d) From the **Configurations** list, select the MIFARE DESFire configuration that was configured with the custom string file.

e) Badge the card.

The cardholder information from the cardholder you selected is encoded on the card. The card can now be used to create a cardholder with the same values on a different system.

Using MIFARE DESFire cards to auto-fill cardholder information

If you want to create the same cardholder on multiple systems, and have encoded the cardholder information on a MIFARE DESFire card, you can use the card to auto-fill a new cardholder's information when assigning the card to it using a STid reader.

Before you begin

Ensure the following:

- Your Security Center license supports MIFARE DESFire configuration.
- A smart card encoding station is set up.
- The cardholder information of the cardholder you want to create on another system is encoded on the MIFARE DESFire card.

What you should know

- Security Center 5.11.1.0 or later is required to perform this task.
- Before opening the *Cardholder management* task, ensure that the *MIFARE DESFire configuration* task is not open on the *Test USB reader* page. This prevents you from using the STid reader in the *Cardholder management* task.

To use a MIFARE DESFire card to auto-fill cardholder information:

1. Create a MIFARE DESFire configuration with at least one Read key or Read-write key.
2. Open the *Cardholder management* task, and click **New** (+).
3. In the dialog box that opens, click **Add a credential** > **Automatic entry**.
4. In the *Automatic entry* dialog box, select **STid USB reader**, and turn off the **Encode before enrollment** option.
5. From the **Configurations** list, select the MIFARE DESFire configuration that was configured with the Read key.
6. Badge the card.

A credential is assigned to the cardholder and the cardholder fields are filled with the information encoded on the MIFARE DESFire card.

Importing MIFARE DESFire configurations in Security Center

You can import MIFARE DESFire configurations using an XML file in the *MIFARE DESFire configuration* task.

Before you begin

Ensure your Security Center license supports MIFARE DESFire configuration.

What you should know

Imported MIFARE DESFire configurations cannot be edited.

To import MIFARE DESFire configurations in Security Center:

1. From the Config Tool home page, open the *MIFARE DESFire configuration* task.
2. On the *Configuration* page, click **Import**.
3. From the file browser, select an XML file containing the MIFARE DESFire configurations, and then click **Open**.

The configurations from the file are added to the **MIFARE DESFire configuration** list.

Configuring MIFARE DESFire cryptographic keys in Security Center

You can use the *MIFARE DESFire configuration* task in Config Tool to configure and store cryptographic keys.

Before you begin

Ensure the following:

- Your Security Center license supports MIFARE DESFire configuration.
- You are granted the *Export configurations and keys* and *Modify keys* user privileges.

What you should know

MIFARE DESFire EV1/EV2 is a 128-bit, Advanced Encryption Standard (AES)-based protocol for which you define the keys.

To configure MIFARE DESFire cryptographic keys in Security Center:

1. From the Config Tool home page, open the *MIFARE DESFire configuration* task.
2. Click the **Key transfer** tab.
3. Create keys in the key store by doing one of the following:
   - Click **Retrieve application read keys**, select a key from the list, and then click **Edit the item** (✎). The keys are retrieved from the configurations you created on the *Configuration* page of the *MIFARE DESFire configuration* task.
   - Click **Add an item** (➕).
4. In the *Key configurations* dialog box, select a **Name** from the list.
5. Click **Add an item** (➕), and then enter the following:
   - **Version:** The number of times the key has been defined. Every time you create a new version of a key, you redefine the key by adding components to form it.
   - **Key:** The component that forms the key. Each component is a 32-character hexadecimal value. You can add multiple components per key version.
6. Click **Add component**, and then click **Create new version**.
7. (Optional) Enter a description for the key.
8. (Optional) Add up to two other versions of the key by clicking **Add an item** (➕), entering the version and the key components for the version, and then clicking **Create new version**.
9. Click **OK**, and then click **Save**.
   The new keys are listed.
10. (Optional) From the **Hash** list, select a different hash to verify the keys.

After you finish

Export one or more of the keys to your Synergis™ Cloud Link units.

Exporting MIFARE DESFire keys to Synergis Cloud Link units

You can export MIFARE DESFire cryptographic keys directly from the *MIFARE DESFire configuration* task in Config Tool to one or more Synergis™ Cloud Link units in your system.

Before you begin

Ensure the following:

- Your Security Center license supports MIFARE DESFire configuration.
- You are granted the *Export configurations and keys* user privilege.

What you should know

The Synergis Cloud Link units you can export to require Synergis™ Softwire 11.1 or later.

To export MIFARE DESFire keys to Synergis Cloud Link units:

1. From the Config Tool home page, open the *MIFARE DESFire configuration* task.
2. Click the **Key transfer** tab.
3. Select one or more keys from the list, and then click **Export to units**.
4. In the *Unit selection* dialog box, select one or more Synergis Cloud Link units to export the configuration to.
5. Click **Export**.

The keys are updated in the Synergis™ Appliance Portal. You can verify the changes in Synergis™ Appliance Portal by clicking **Configuration** > **Synergis™ key store**.

Credential enrollment methods

If you need many card credentials in your access control system, you can enroll multiple credentials at a time.

The following two enrollment methods are available in the *Credential enrollment* task:

- **Automatic entry:** This is the recommended method when the cards you want to enroll are at your disposal, and when the card data is not found within any known range of values. It is also appropriate to use this enrollment method when the cards come in many types of formats.
- **Manual entry:** This is the recommended method when all the cards you want to enroll are the same format, and one of the data fields (typically the *Card number*) contains a range of consecutive values. You do not require the actual cards, or a card reader to use this method, and it can be an effective way of pre-enrolling large quantities of cards.

You can also enroll credentials using the *Import tool*.

Enrolling multiple credentials automatically

If you need many card credentials in your access control system, you can enroll multiple card credentials automatically by presenting them to a reader.

Before you begin

You must have access to a card reader. The cards you present must be of a predefined format in your system.

Ensure that this is the correct enrollment method you require.

What you should know

All credentials you enroll must be new to your Security Center system. Any previously enrolled credential is discarded because the same credential cannot be enrolled twice in Security Center.

For information about how to encode a credential on your card before enrolling it, see Assigning credentials on page 824.

To enroll multiple credentials automatically:

1 In the *Credential management* task, click **Batch enrollment**.

2 Click the *Automatic entry* tab.

3 Select whether you want to present the card credentials to a local USB reader or nearby door:

- Select **rf IDEAS USB reader** or **Omnikey USB reader** from the list, connect a corresponding card reader to the local workstation, then click **Refresh** (🔄).
- Select **Door** from the list, and then select a door entity as the **Access point**.

4 In the *Credential prefix* section, enter the pattern for the enrolled credential names.

5 In the *Credential status* section, set the status, activation date, and expiration date for the credentials:

- **Status:** All possible values are accepted.
- **Activation:** Can be *Never*, or a specific date.
- **Expiration:** Set an expiration for the credential:
  - **Never:** The credential never expires.
    NOTE: You can remove this option. For more information, see Removing the option for cardholders and credentials to never expire on page 837.
  - **Specific date:** The credential expires on a specific date and time.
  - **Set expiration on first use:** The credential expires after a specified number of days after the first use.
  - **When not used:** The credential expires when it has not been used for a specified number of days.

6 In the *Advanced* section, select the partition the enrolled credentials belong to.
This field determines which users can view and modify the credentials.

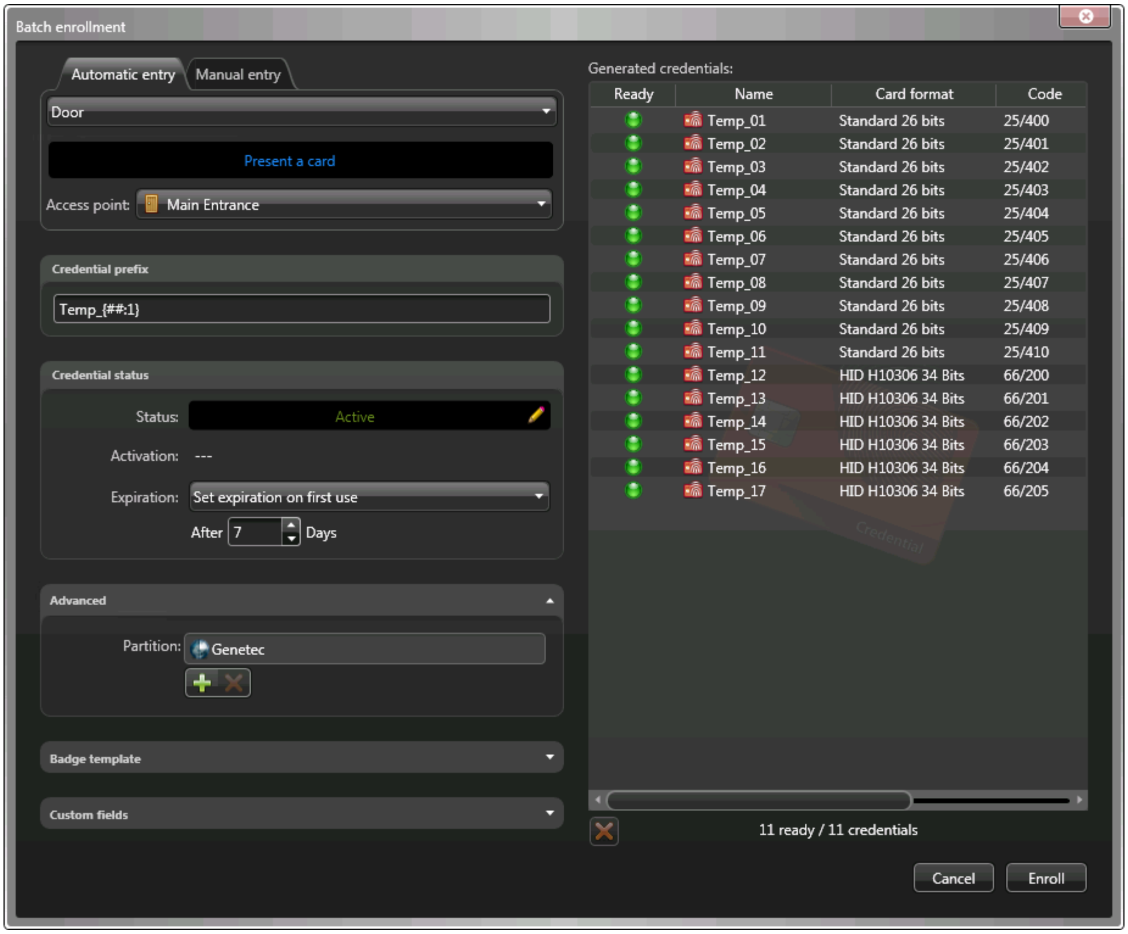
- To add a partition, click **Add** (➕).
- To remove a partition, select the partition, and then click **Remove** (✖).

7 From the **Badge template** list, select the default badge template used to represent the credential.

8 In the *Custom fields* section, set the default values for the custom fields.
This section is only available if custom fields have been created for credentials.

9 Present the cards to the selected reader.

All presented cards are listed in the *Generated credentials* section. Any already enrolled credentials are discarded and marked as rejected in the list with a red button.



Batch enrollment

Door

Access point: Main Entrance

Credential prefix

Temp_{##:1}

Credential status

Status: Active

Activation: ---

Expiration: Set expiration on first use

After 7 Days

Advanced

Partition: Genetec

Badge template

Custom fields

Generated credentials:

Ready	Name	Card format	Code
●	Temp_01	Standard 26 bits	25/400
●	Temp_02	Standard 26 bits	25/401
●	Temp_03	Standard 26 bits	25/402
●	Temp_04	Standard 26 bits	25/403
●	Temp_05	Standard 26 bits	25/404
●	Temp_06	Standard 26 bits	25/405
●	Temp_07	Standard 26 bits	25/406
●	Temp_08	Standard 26 bits	25/407
●	Temp_09	Standard 26 bits	25/408
●	Temp_10	Standard 26 bits	25/409
●	Temp_11	Standard 26 bits	25/410
●	Temp_12	HID H10306 34 Bits	66/200
●	Temp_13	HID H10306 34 Bits	66/201
●	Temp_14	HID H10306 34 Bits	66/202
●	Temp_15	HID H10306 34 Bits	66/203
●	Temp_16	HID H10306 34 Bits	66/204
●	Temp_17	HID H10306 34 Bits	66/205

11 ready / 11 credentials

10 To remove a discarded credential from the list, select it, and then click ✕.

11 Click **Enroll**.

After you finish

Assign the credentials to your cardholders.

Related Topics

Credential enrollment methods on page 862
How credential card formats work with Active Directory in Security Center on page 880
About credentials on page 847

Enrolling multiple credentials manually

If you need many card credentials in your access control system, you can enroll multiple credentials simultaneously by entering the card format and data manually.

Before you begin

You must know the exact range of values represented in the card data. Because the cards are not presented to a reader, the application cannot validate them.

Ensure that this is the correct enrollment method you require.

What you should know

All credentials you enroll must be new to your Security Center system. Any previously enrolled credential is discarded because the same credential cannot be enrolled twice in Security Center. Only a maximum of 5000 credentials can be created at once.

To enroll multiple credentials manually:

1. In the *Credential management* task, click **Batch enrollment**.
2. Click the **Manual entry** tab.
3. From the **Card format** list, select the card format used by the credentials you want to enroll.

   This option determines the data fields you must enter, and the range of values that they can have.
4. In the **Facility code** and **Card number** fields, enter the starting and ending values for the card numbers.

   The **Card number** field is used as a sequence generator.

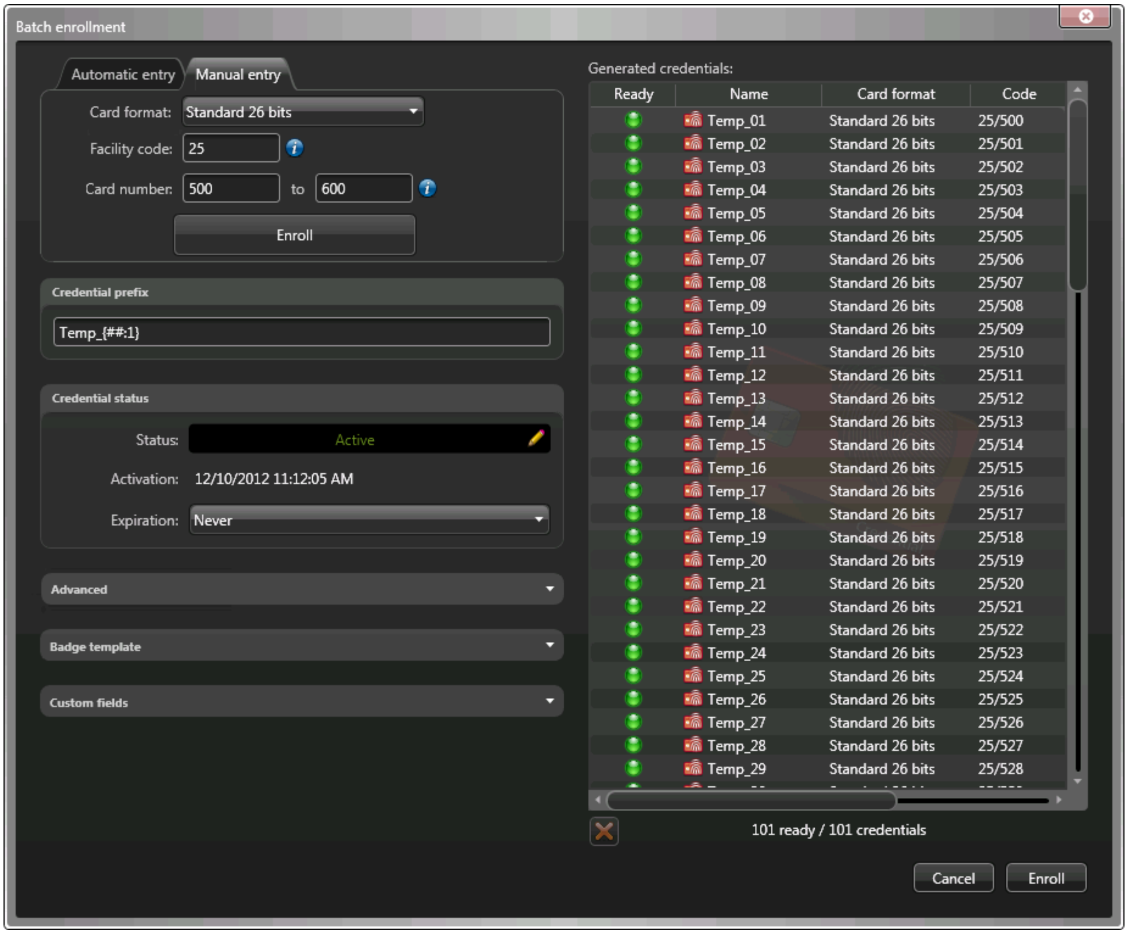
   NOTE: If the specified **Card number** range contains more than 5000 values, the end value is automatically adjusted to be the start value plus 5000.
5. In the *Credential prefix* section, enter the pattern for the enrolled credential names.
6. In the *Credential status* section, set the status, activation date, and expiration date for the credentials:
   - **Status:** All possible values are accepted.
   - **Activation:** Can be *Never*, or a specific date.
   - **Expiration:** Set an expiration for the credential:
     - **Never:** The credential never expires.
       NOTE: You can remove this option. For more information, see Removing the option for cardholders and credentials to never expire on page 837.
     - **Specific date:** The credential expires on a specific date and time.
     - **Set expiration on first use:** The credential expires after a specified number of days after the first use.
     - **When not used:** The credential expires when it has not been used for a specified number of days.
7. In the *Advanced* section, select the partition the enrolled credentials belong to.

   This field determines which users can view and modify the credentials.
   - To add a partition, click **Add** (✚).
   - To remove a partition, select the partition, and then click **Remove** (✖).
8. From the **Badge template** list, select the default badge template used to represent the credential.
9. In the *Custom fields* section, set the default values for the custom fields.

   This section is only available if custom fields have been created for credentials.

10 Click **Enroll**.

The credentials you are going to create are listed in the *Generated credentials* section. Any already enrolled credentials are discarded and marked as rejected in the list with a red button.



Card format: Standard 26 bits

Facility code: 25

Card number: 500 to 600

Credential prefix

Temp_{##:1}

Credential status

Status: Active

Activation: 12/10/2012 11:12:05 AM

Expiration: Never

Generated credentials:

Ready	Name	Card format	Code
●	Temp_01	Standard 26 bits	25/500
●	Temp_02	Standard 26 bits	25/501
●	Temp_03	Standard 26 bits	25/502
●	Temp_04	Standard 26 bits	25/503
●	Temp_05	Standard 26 bits	25/504
●	Temp_06	Standard 26 bits	25/505
●	Temp_07	Standard 26 bits	25/506
●	Temp_08	Standard 26 bits	25/507
●	Temp_09	Standard 26 bits	25/508
●	Temp_10	Standard 26 bits	25/509
●	Temp_11	Standard 26 bits	25/510
●	Temp_12	Standard 26 bits	25/511
●	Temp_13	Standard 26 bits	25/512
●	Temp_14	Standard 26 bits	25/513
●	Temp_15	Standard 26 bits	25/514
●	Temp_16	Standard 26 bits	25/515
●	Temp_17	Standard 26 bits	25/516
●	Temp_18	Standard 26 bits	25/517
●	Temp_19	Standard 26 bits	25/518
●	Temp_20	Standard 26 bits	25/519
●	Temp_21	Standard 26 bits	25/520
●	Temp_22	Standard 26 bits	25/521
●	Temp_23	Standard 26 bits	25/522
●	Temp_24	Standard 26 bits	25/523
●	Temp_25	Standard 26 bits	25/524
●	Temp_26	Standard 26 bits	25/525
●	Temp_27	Standard 26 bits	25/526
●	Temp_28	Standard 26 bits	25/527
●	Temp_29	Standard 26 bits	25/528

101 ready / 101 credentials

11 To remove a discarded credential from the list, select it, and then click ✖.

12 Click **Enroll**.

After you finish

Assign the credentials to your cardholders.

Related Topics

Credential enrollment methods on page 862
How credential card formats work with Active Directory in Security Center on page 880
About credentials on page 847

Creating credentials

You can create a credential, configure its properties, and assign it to a cardholder or visitor, using the *Credential management* task.

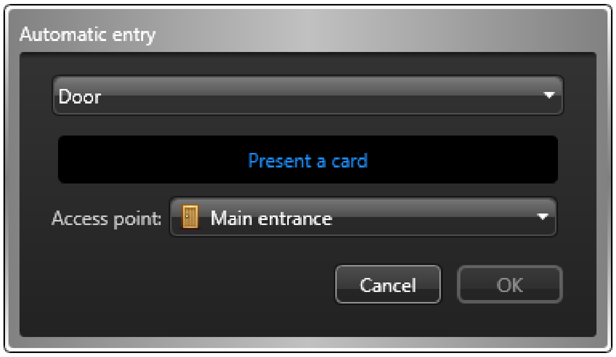
What you should know

- Instead of creating cardholders manually, you can import them from a CSV file, or from your company's Active Directory.
- To learn how to create mobile credentials, see Creating mobile credentials in the Mobile Credential Manager on page 879.

To create a credential:

1. In the *Credential management* task, click **Create new credential** (➕).
2. Select one of the following options:
   - **Automatic entry:** Present the card at a reader.
   - **Manual entry:** Manually enter the card data. Use this method when you do not have a card reader near you.
   - **PIN:** Create a PIN credential.
   - **License plate:** Enter a cardholder's license plate number. Use this method if a Sharp camera is being used to trigger a vehicle access barrier. In this case, the cardholder's vehicle license plate can be used as a credential.

3 If you select **Automatic entry**, you must then select a reader (USB reader or a door) and present the card at the reader.


Automatic entry

Door

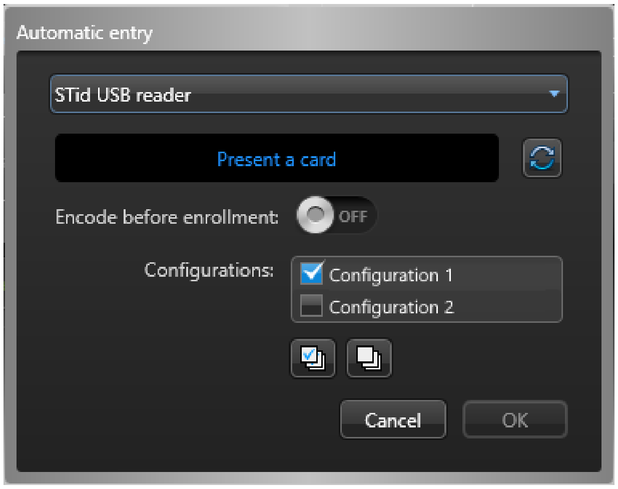
Present a card

Access point: Main entrance

Cancel OK

If you have a smart card encoding reader set up, do one of the following:

- To read a pre-encoded card, turn off the **Encode before enrollment** option. When the reader LED turns green (ready to read), place the smart card on the reader. The reader LED turns yellow and then green with a short beep before turning off.


Automatic entry

STid USB reader

Present a card

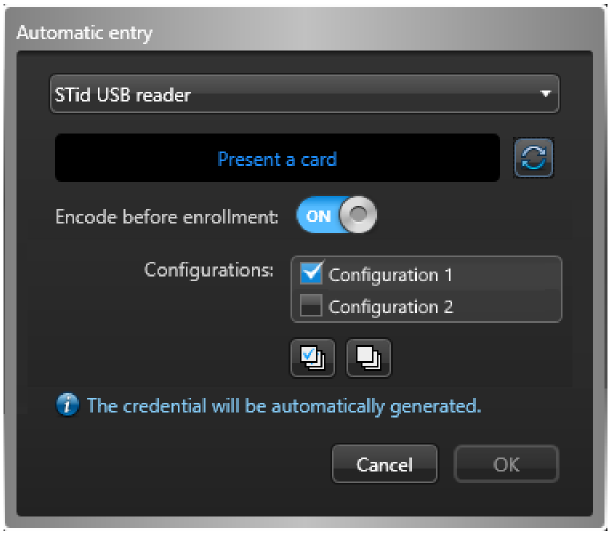
Encode before enrollment: OFF

Configurations:
☑ Configuration 1
□ Configuration 2

Cancel OK

- To generate and encode on your card a random 128-bit MIFARE DESFire credential before enrolling it, turn on the **Encode before enrollment** option and select at least one configuration with a credential. When the reader LED turns red (ready to encode), place the smart card on the reader for approximately 2 seconds. The reader LED turns yellow and then green with a short beep before turning off. If you hear a long beep and the LED stays red, try again.

NOTE: Your Security Center license must support smart card encoding.



Automatic entry

STid USB reader

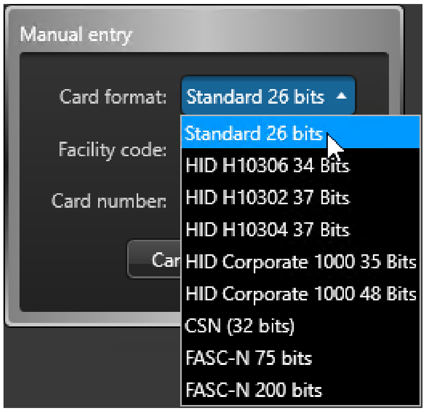
Present a card

Encode before enrollment: ON

Configurations: ☑ Configuration 1 □ Configuration 2

The credential will be automatically generated.

4 If you select **Manual entry**, you must then select a card format, enter the required data fields, and click **OK**.



Manual entry

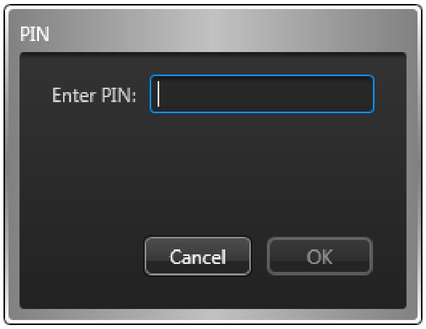
Card format: Standard 26 bits

Facility code:

Card number:

CAUTION: Enter your card data carefully because the system cannot validate whether the data you entered correspond to a physical card or not.

5 If you select **PIN**, you must then do the following:



PIN

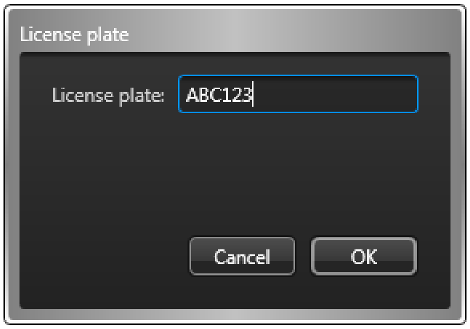
Enter PIN:

a) Enter the PIN as a numerical value.

NOTE: Be careful not to exceed the number of digits accepted by your readers. A typical PIN length is five digits. But certain models accept up to 15 digits.

b) Click **OK**.

6 If you select **License plate**, you must then do the following:



License plate

License plate: ABC123

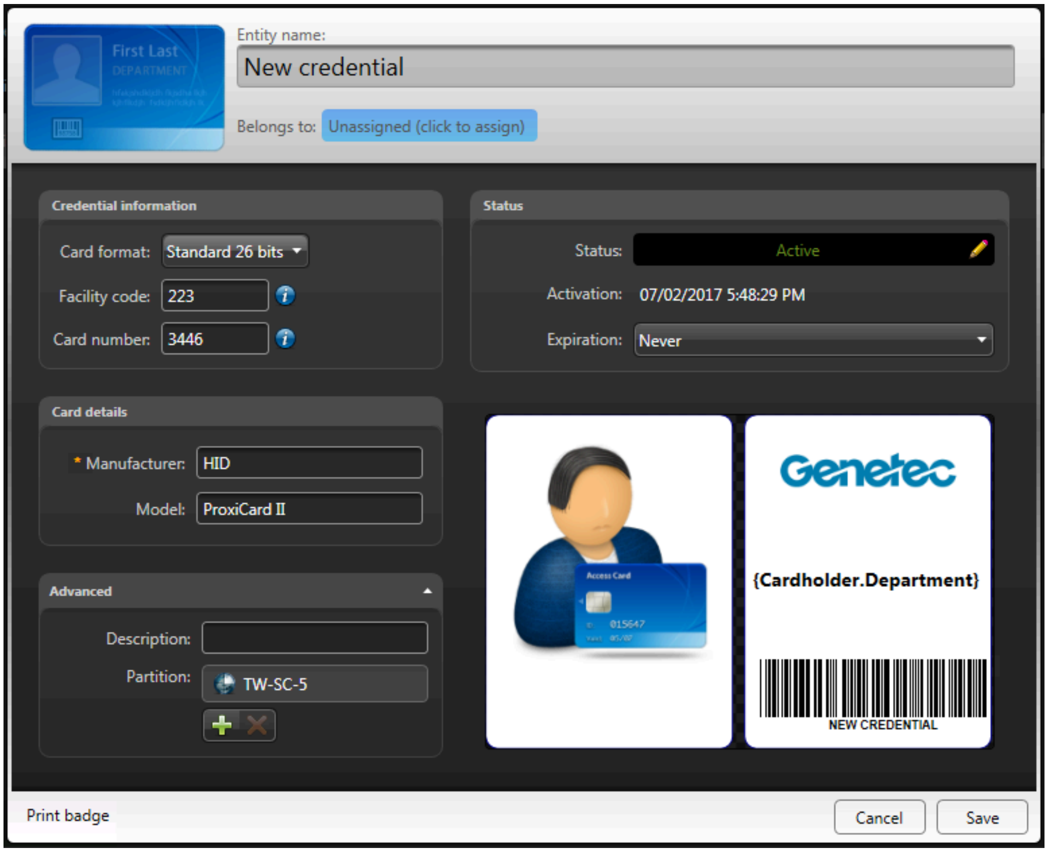
a) Enter the license plate number.

NOTE: You do not need to enter spaces in the license plate number. The system treats "ABC123" and "ABC 123" as the same plate.

b) Click **OK**.

7 In the **Entity name** field, enter a name for the credential entity.

The following screen capture is for card credentials. The dialog box looks different if you selected **PIN** or **License plate** credentials.



Entity name: New credential

Belongs to: Unassigned (click to assign)

Credential information

Card format: Standard 26 bits

Facility code: 223

Card number: 3446

Status

Status: Active

Activation: 07/02/2017 5:48:29 PM

Expiration: Never

Card details

* Manufacturer: HID

Model: ProxiCard II

Advanced

Description:

Partition: TW-SC-5

8 Click the **Belongs to** field, select a cardholder or visitor to assign the credential to, and then click **OK**.

Without assigning a credential, you cannot monitor the activities, or generate activity reports for that cardholder or visitor.

9 In the *Status* section, set the status and activation period for the credential.

If the credential is inactive, the cardholder or visitor does not have access to any area.

- **Status:** Set the credential status to **Active**.
- **Activation:** Displays the current date.
- **Expiration:** Set an expiration for the credential:

- **Never:** The credential never expires.
- **Specific date:** The credential expires on a specific date and time.
- **Set expiration on first use:** The credential expires after a specified number of days after the first use.
- **When not used:** The credential expires when it has not been used for a specified number of days.

10 If custom fields are defined for credentials, such as the manufacturer, the card model, and so on, enter the credential's custom information under the designated section.

11 (Optional) Expand the *Advanced* section, and configure the following credential properties:

   a) In the **Description** field, enter a description for the credential.

   b) Assign the credential to a partition.

   Partitions determine which Security Center users have access to this entity. Only users who have been granted access to the partition can see the credential.

12 (Optional) If the credential is a card credential (not a PIN), select a badge template.

   a) In the lower-right corner of the credential details dialog box, click the badge image.

   b) Select a badge template, and then click **OK**.

   Badge templates are created in Config Tool.

   A print preview of the badge appears, with data corresponding to the credential.

   NOTE: The badge template remains associated to the credential even if you unassign the credential from a cardholder or visitor.

13 To print the badge, in the lower-left corner of the credential details dialog box, click **Print badge**.

14 When you are finished editing the credential, click **Save**.

The new credential is added to the list in the *Credential management* task.

After you finish

To modify a credential, select the credential in the list, and then click **Modify** (✏).

Related Topics

Importing cardholders and credentials on page 912

Assigning credentials on page 824

Designing badge templates on page 888

Responding to credential card requests on page 873

ALPR access control on page 1048

Adding reasons for credential card requests

To allow users to specify why they are requesting a credential card, you can add a set of reasons that they can choose from.

What you should know

A common reason a user might request a credential card is: “no printer on site”.

To add a credential card request reason:

1 Open the **Access control** task, and click the **General settings** view.

2 Under the *Card request reasons* section, click **Add an item** (➕).

3 In the *Add a new card request reason* dialog box, type a reason, and click **Add** > **Apply**.

4 To modify a card request reason, select it in the list, and click **Edit the item** (✏).

5 To delete a card request reason, select it in the list, and click **Remove the item** (✖).

The new reason can now be selected when users request credential cards.

Responding to credential card requests

After a credential card request has been made, you can respond by assigning a credential to the applicant the request was made for, or by denying the request.

What you should know

The number of pending card requests is shown in the **Card requests** () icon in the notification tray, and at the top of the *Credential management* task.

Credential requests are sent when a user creates a cardholder, but cannot assign a credential or print a card for the cardholder (for example, because no printer is available). After you assign and print a credential card, it can be shipped to another site, if required.

To respond to a credential card request:

1. Do one of the following:
   - In the notification tray, click **Card requests** ().
   - At the top of the *Credential management* task, click **Card requests**.
2. In the *Card requests* dialog box, select the request you want to respond to.
   Hold `Shift` to select multiple requests.
3. To modify the request, click **Modify** (), edit the request, and then click **OK**.
4. To deny the request, click **Deny request** ().
5. To assign a card credential, click **Associate card** ().
   In the *Associate cards* dialog box that opens, do one of the following:
   - To assign a credential automatically, click **Automatic entry**, select a reader (USB reader or a door), and present the card at the reader.

     If an eligible card is presented, it is immediately assigned. If the card has not been enrolled, it is enrolled automatically. If the card was already assigned to someone, it is rejected.

     For information on how you can encode a credential on your card before enrolling it, see Assigning credentials on page 824.
   - To assign a credential manually, click **Manual entry**, select a card format, enter the required data fields, and click **Enroll**.
     CAUTION: Enter your card data carefully because the system cannot validate whether the data you entered correspond to a physical card or not.
   - To assign an existing credential, click **Existing credential** and double-click a credential from the list of eligible credentials.
6. To print the badge on the card, click **Print cards** () and follow the instructions.
7. Click **Close** to complete this request.

After the card request is completed or denied, an email is sent to the requester only if they selected the **Email me when the card is ready** option when they requested the card.

Related Topics

Requesting credential cards on page 828

Creating credentials on page 867

About the Mobile Credential Manager role

The Mobile Credential Manager role links Security Center to your third-party mobile credential provider so that you can view your subscription status, and manage your mobile credentials and profiles in Config Tool.

What you can do with the Mobile Credential Manager role

Use the Mobile Credential Manager role so that you can manage your mobile credentials without having to navigate to external mobile credential portals. You can use the role to do the following:

- Create mobile credential profiles
- Create mobile credentials
- Revoke mobile credentials
- Resend or cancel email invitations sent from the mobile credential provider
- View the status of your mobile credential subscription and license count

NOTE: Only one instance of this role can be created on the system.

Limitations of the Mobile Credential Manager role

When the role is created in your system, mobile credential profiles can no longer be created or configured from the *General settings* page of the *Access control* task.

Creating the Mobile Credential Manager role

You must create the Mobile Credential Manager role in Config Tool to manage the mobile credential profiles in Security Center.

What you should know

Only one Mobile Credential Manager role can be created per system.

To create the Mobile Credential Manager role:

1 Open the *System* task and click the **Roles** view.

2 Click **Add an entity** (➕), and then **Mobile Credential Manager**.

The *Creating a role: Mobile Credential Manager* wizard opens.

3 On the *Specific info* page, do the following:

a) From the **Server** list, select the server assigned to this role.

NOTE: If no expansion server is present, this option is not available.

b) In the **Database server** field, select or enter the name of the database server.

c) In the **Database** field, select or enter the name of the database.

d) In the **Authentication** field, select **Windows** or **SQL Server**.

e) Click **Next**.

4 On the *Basic information* page, do the following:

a) Enter the **Entity name**.

b) Enter an **Entity description** for the role.

c) Click **Next**.

5 On the *Creation summary* page, do the following:

a) Verify the information you entered.

b) If everything is correct, click **Create**, or click **Back** to modify your settings.

When the role is created, you see the following message: *The operation was successful.*

6 Click **Close**.

Setting up mobile credential profiles

Before you can assign mobile credentials to cardholders and visitors, you must purchase the service of a mobile credential provider and configure mobile credential profiles in your system in either the Mobile Credential Manager role or in the *Access control* task.

Before you begin

Purchase one or more services from a mobile credential provider.

What you should know

- A mobile credential profile links a part number from your mobile credential provider to your subscription so that you can create mobile credentials in Security Center.
- If HID Global is your mobile credential provider, you must purchase subscription user licenses and add credential types (identified by a *part number*) for each format you want to support. For each credential type in use, you must configure a *mobile credential profile* in Security Center.
- You cannot have more than one HID mobile credential from the same *mobile keyset*, even if the credentials use different part numbers. The keysets are configured on the HID side. For more information, contact your HID representative.
- Starting in Security Center 5.10, you can create mobile credential profiles using the Mobile Credential Manager role. If the role is created, you can no longer create the profiles in the *Access control* task.

  NOTE: It is recommended to use the Mobile Credential Manager role to create mobile credential profiles.

To set up a mobile credential profile:

1 To create a mobile credential profile in the Mobile Credential Manager role:

  a) Open the *System* task, and click the **Roles** view.

  b) Click the Mobile Credential Manager role, and then click the **Configuration** tab.

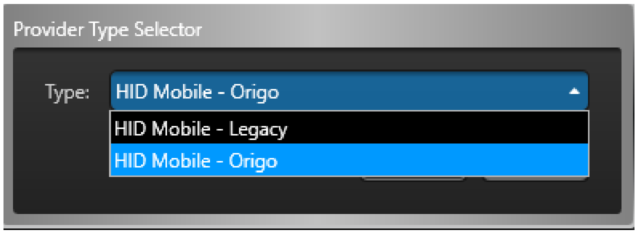
  c) In the *Mobile credential profiles* section, click **Add an item** (➕).

2 To create a mobile credential profile in the *Access control* task:

  a) Open the *Access control* task and click the **General settings** view.

  b) In the *Mobile credential profiles* section, click **Add an item** (➕).

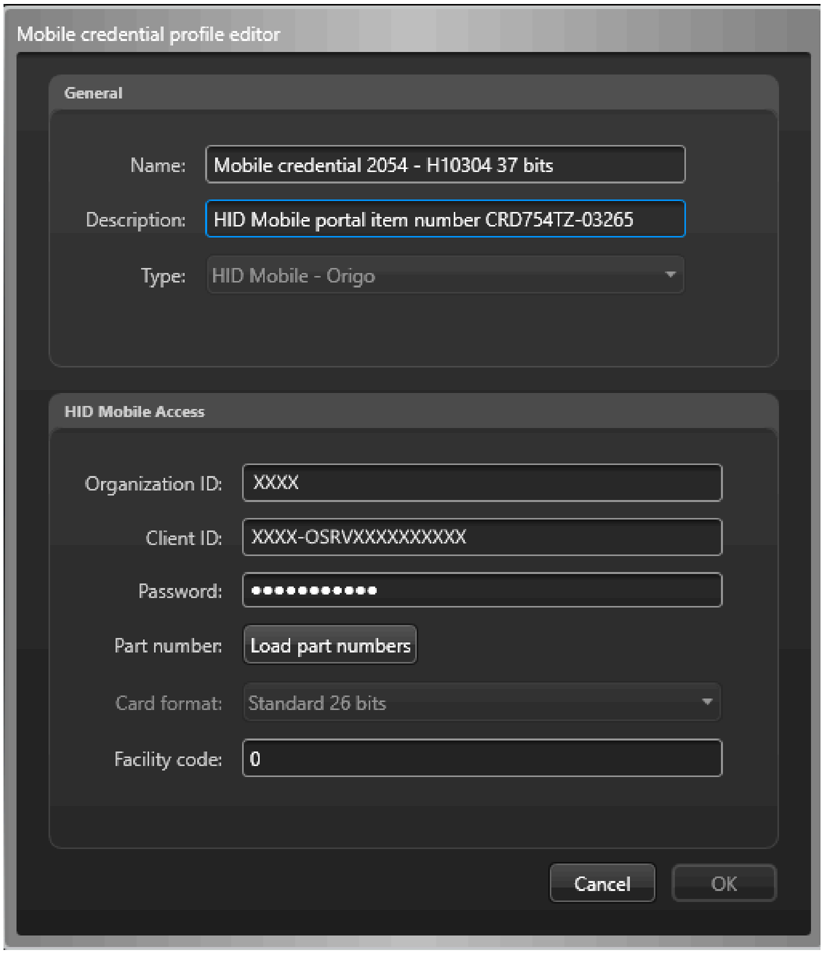
  c) In the *Provider Type Selector* dialog box, select a mobile credential provider and click **OK**.



Provider Type Selector

Type: HID Mobile - Origo

3 In the *Mobile credential profile editor* dialog box, enter the following information:


Mobile credential profile editor

General

Name: Mobile credential 2054 - H10304 37 bits

Description: HID Mobile portal item number CRD754TZ-03265

Type: HID Mobile - Origo

HID Mobile Access

Organization ID: XXXX

Client ID: XXXX-OSRVXXXXXXXXXX

Password: ●●●●●●●●●●●

Part number:

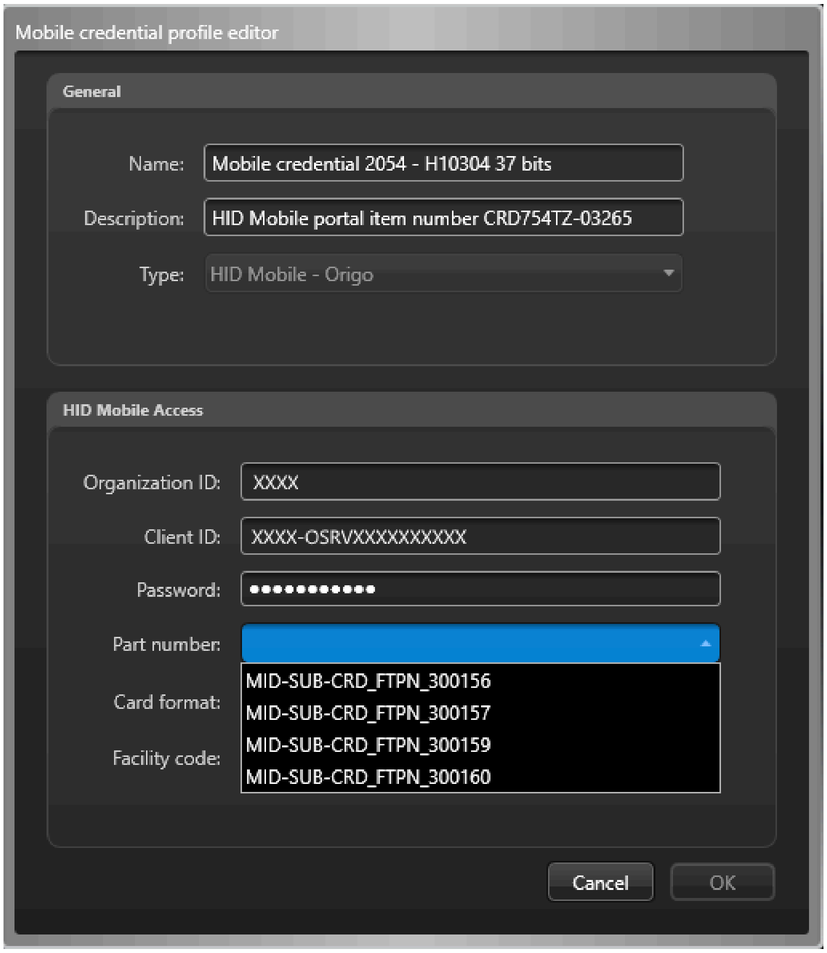
Card format: Standard 26 bits

Facility code: 0

- **Name:** The name used to identify this credential profile in Security Center. Include the facility code and the card format in the name to help the operator select the correct profile.
- **Description:** The description of this profile.
- **Type:** (Read-only) Your mobile credential provider.
- **Organization ID:** The numeric ID issued to your company by HID Global.
- **Client ID:** The client ID associated to the system account you created on the HID Origo Management Portal.
- **Password:** The password you created for your system account on the HID Origo Management Portal.

4 Click **Load part numbers**.
The part numbers from the mobile credential portal populate the **Part number** menu.

5 From the **Part number** list, select the part number corresponding to your credential profile.



Name: Mobile credential 2054 - H10304 37 bits

Description: HID Mobile portal item number CRD754TZ-03265

Type: HID Mobile - Origo

Organization ID: XXXX

Client ID: XXXX-OSRVXXXXXXXXXX

Password: ●●●●●●●●●●●

Part number:

- MID-SUB-CRD_FTPN_300156
- MID-SUB-CRD_FTPN_300157
- MID-SUB-CRD_FTPN_300159
- MID-SUB-CRD_FTPN_300160

Card format:

Facility code:

NOTE: The **Card format** and **Facility code** fields are automatically completed based on the part number you select. Not all part numbers have facility codes.

- **Part number:** The part number identifying the credential type you intend to use.
- **Card format:** The card format corresponding to the selected part number.
- **Facility code:** The facility code corresponding to the selected part number.

6 Click **OK**, and then click **Apply**.

Related Topics

Assigning credentials on page 824

Creating mobile credentials in the Mobile Credential Manager

You can create mobile credentials in the Mobile Credential Manager role.

Before you begin

Set up mobile credential profiles.

What you should know

- A mobile credential is a credential on a smartphone that uses Bluetooth or Near Field Communication (NFC) technology to access secured areas. Mobile credentials and card credentials are similar; they both follow standard credential formats such as *Standard 26 bits* and *HID H10304 37 Bits*.
- You can also create mobile credentials in the *Cardholder management* task.

To create a mobile credential in the Mobile Credential Manager:

1 Open the *System* task and click the **Roles** view.

2 Click the Mobile Credential Manager role, and then click the **Credentials** tab.

3 At the bottom of the *Credentials* section, click **Add an item** (➕).
The *Mobile credential creation wizard* opens.

4 Select the **Cardholder** to which you want to assign the credential, and a **Mobile credential profile**.

5 Click **OK**, and then click **Apply**.

How credential card formats work with Active Directory in Security Center

If you decide to map the credential *Card format* property to an Active Directory attribute, that attribute must contain either a numeric value (for standard card formats) or the exact card format name (text).

The following list describes the standard card formats supported by Security Center, their numeric values, and the valid ranges for the facility code (also known as *Company ID Code*), card number (also known as *Card ID Number*), or other codes associateds with specific card types.

- 0: **Standard 26 bits**
  - Facility code range: 0 to 255
  - Card number range: 0 to 65 535
- 1: **HID H10306 34 Bits**
  - Facility code range: 0 to 65 535
  - Card number range: 0 to 65 535
- 2: **HID H10302 37 Bits**
  - Facility code range: Not required[1]
  - Card number range: 0 to 0 to 34 359 738 367
- 3: **HID H10304 37 Bits**
  - Facility code range: 0 to 65 535
  - Card number range: 0 to 524 287
- 4: **HID Corporate 1000 (35 bits)**
  - Facility code range: 0 to 4095
  - Card number range: 0 to 1 048 575
- 5: **HID Corporate 1000 (48 bits)**
  - Facility code range: 0 to 4 194 303
  - Card number range: 0 to 0 to 8 388 607
- 6: **CSN (32 bits)**
  - Facility code range: Not required
  - Card number range: 0 to FFFFFFFF
- 7: **FASC-N 75 bits**
  - Agency code: 0 to 16 383
  - System code: 0 to 16 383
  - Credential number: 0 to 1 048 575
  - Exp date: 0 to 33554431

- 8: **FASC-N 200 bits**
  - Agency code: 0 to 9999
  - System code: 0 to 9999
  - Credential number: 0 to 999999
  - CS (Credential Series): 0 to 9
  - ICI (Individual Credential Issue): 0 to 9
  - PI (Person Identifier): 0 to 99999999999
  - OC (Organizational Category): 0 to 9
  - OI (Organizational Identifier): 0 to 9999
  - POA (Person/Organization Association): 0 to 9
  - LRC (Longitudinal Redundancy Character): 0 to 9

[1] If HID H10302 37 Bits is the only card format referenced in your CSV file, it is preferable to bind the card number to the Security Center Card data field instead of the Card number field since the facility code is not required. Because a single value is stored in the Credential card data field, no separator character is needed.

IMPORTANT: For custom card formats, you must use the exact spelling used to create the custom card format.

Related Topics

Integration with Windows Active Directory on page 473
Custom card formats on page 882
Custom card format editor tool on page 883
Creating custom card formats on page 884

Custom card formats

In addition to the standard card formats that are supported in Security Center, you can define custom card formats with unique data fields.

You can define custom card formats in Config Tool from the *General settings* view in the Access control task.

Benefits of custom card formats

Creating custom card formats has the following benefits:

- You can manually enroll a new card using a standard workstation keyboard, whereas a card with an unknown format can only be enrolled using a card reader.
- You can view the card number in the Config Tool and the Security Desk, whereas data for unknown card formats cannot be displayed.
- You can import cards using custom formats with the *Import tool*.
- You can enroll cards automatically, with a card reader, or manually in bulk, without a card reader, using the Credential management task.

Related Topics

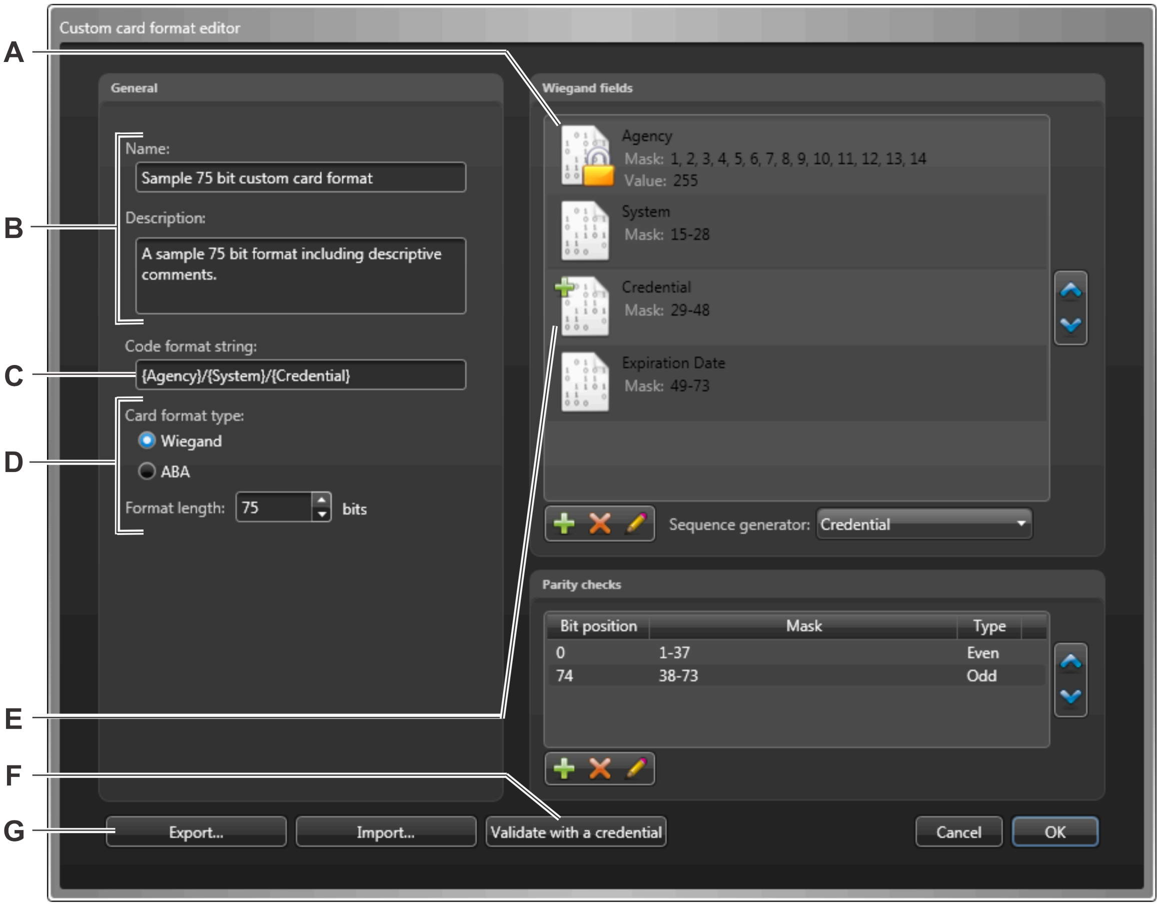
Importing security groups from an Active Directory on page 481

About federated entities on page 270

Custom card format editor tool

The *custom card format editor* is a Synergis™-specific tool that allows you to define your own card formats. It is available from the *General settings* view in the Access control task.

Only administrative users can use this tool.



Name: Sample 75 bit custom card format

Description: A sample 75 bit format including descriptive comments.

Code format string: {Agency}/{System}/{Credential}

Card format type:
● Wiegand
○ ABA

Format length: 75 bits

Agency
Mask: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
Value: 255

System
Mask: 15-28

Credential
Mask: 29-48

Expiration Date
Mask: 49-73

Sequence generator: Credential

Bit position	Mask	Type
0	1-37	Even
74	38-73	Odd

A	Fixed value field (indicated by the padlock 🔒 icon).
B	Card format name and description listed in the *Access control* task, view.
C	Format used to display the *Credential code* in reports.
D	Select the card format type and length before defining the fields.
E	Field designated as the sequence generator (indicated by the plus ✚ icon).
F	Validate the format with pre-enrolled credentials.
G	Import/export card format from XML file.

Related Topics

How credential card formats work with Active Directory in Security Center on page 880

Creating custom card formats on page 884

Creating custom card formats

To define custom card formats that have unique data fields, you can create custom formats manually, or import them from XML files, using the *Custom card format editor* tool.

What you should know

If you delete a custom card format that is being used in Security Center, all credentials using that format appear as *Unknown*, but the credentials are still granted access at the doors.

NOTE: You need to know the format of your card to enter it into the credential code field. If you do not know the format of your card, contact the card manufacturer or your sales representative of Genetec™ Inc. for help.

To create a custom card format:

1. Open the **Access control** task, and click the **General settings** view.
2. Under **Custom card formats**, click **Add an item** (➕).
3. In the **Custom card format editor**, enter the **Name** and **Description** of the custom card format.
4. Specify the **Card format type** and **Format length**.
   - **Wiegand** (8 to 512 bits)
   - **ABA** (2 to 128 characters)
5. Define the Wiegand fields or define the ABA fields that constitute the custom card format.
6. If you selected **Wiegand** format type, you might have to add parity check bits to the format.
7. (Optional) To enroll a range of credentials in bulk, you can designate one field as the **sequence generator**.

   The field designated as the sequence generator allows you to define a range of values for enrolling the credentials in bulk in the *Credential Management* task.
8. Enter the format string for printing the **credential code**.

   The credential code is the printed form of the credential data. It is an optional column that is available in most access control related reports.The **Code format string** tells the system how to print the credential data. To include a field in the credential code, the field name must be specified in the code format string as it is spelled in the card format field definition, between curly brackets “{ }”. The field names are case-sensitive. Any other characters in the format string that are not found between curly brackets are printed as is.For example, with the format string “{Facility}/{Card Number}”, a credential with the respective field values 230 and 7455 will be printed as “230/7455”.
9. To validate the new custom card format with a pre-enrolled credential, click **Validate with a credential**, select a pre-enrolled credential, and click **OK**.
10. (Optional) Click **Export** to save the custom card format to an XML file.

    Exporting the custom card format to an XML file allows you to import that same card format definition to other Synergis™ systems.
11. Click **OK** > **Apply**.

Related Topics

Custom card formats on page 882

Defining ABA fields

If you are adding a custom ABA card format, you must define the ABA data fields that constitute the card format.

What you should know

ABA field length is measured in characters (4 bits each). The maximum ABA card format length for HID units is 32 characters or 128 bits, though the maximum allowed by the Synergis™ unit is 128 characters or 512 bits.

The order of the ABA fields in the format is important for two reasons:

- It defines the card format.
- It corresponds to the order the field values are read from the Credential card data when using the Import tool.

To define an ABA field:

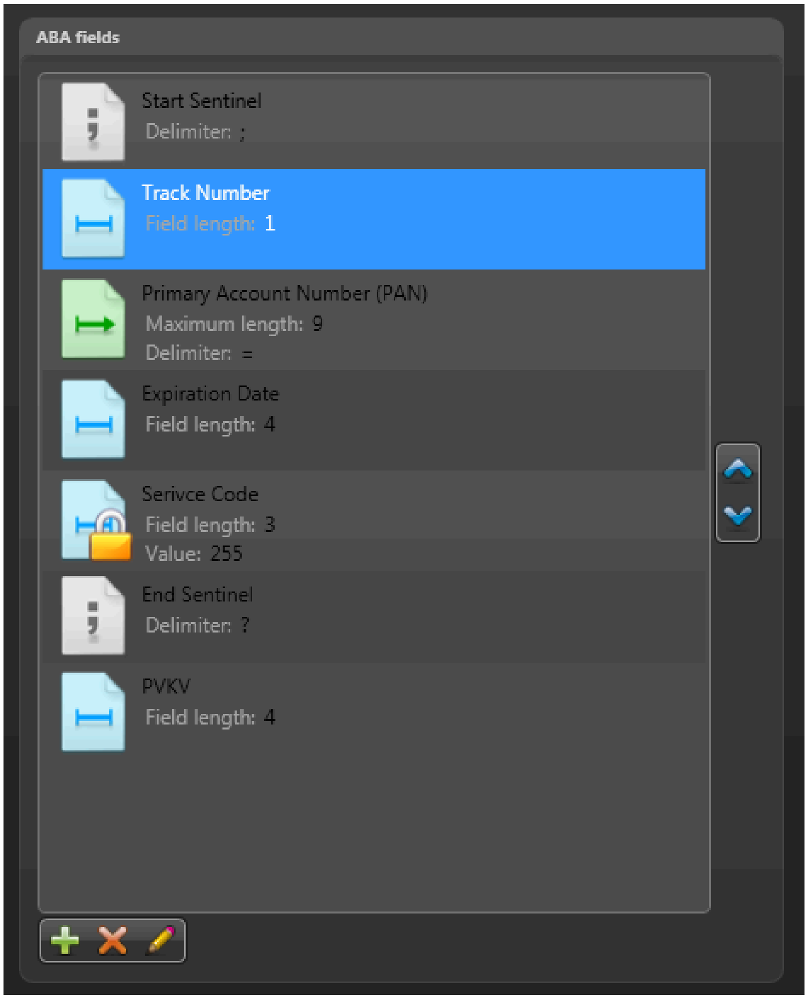
1 In the *Custom card format editor*, click **Add an item** (➕) under the **ABA fields** section.

2 Select one of the following ABA field types:

- **Delimiter:** Specifies a delimiter character, typically used at the beginning or the end of the card format.
- **Sized:** A fixed-length field. The length is specified in characters (4 bits each). The field can contain a fixed value. The field length must be long enough to hold the fixed value.
- **Delimited:** A variable length field. You must specify a maximum length (as 4-bit characters) and a delimiter character.

3 Click **OK**.

The field is added in the **ABA fields** section.



Defining Wiegand fields

If you are adding a custom Wiegand card format, you must define the Wiegand data fields that constitute the card format.

What you should know

A Wiegand field is composed of a series of bits. The maximum field length is 256 bits.

The order of the Wiegand fields for the card format is important. It corresponds to the order that field values are read from the Credential card data when using the *Import tool*.

To define a Wiegand field:

1 In the *Custom card format editor*, click **Add an item** (➕) under the **Wiegand fields** section.

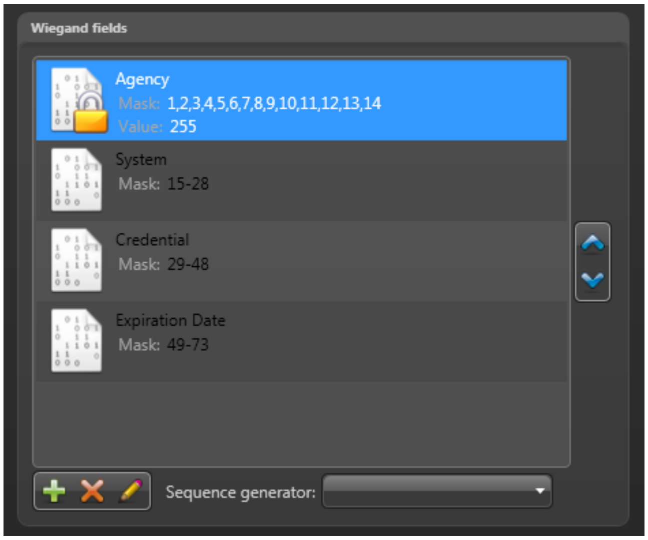
2 In the **Name** field, type a name for the Wiegand field.

3 In the **Mask** field, type the number of bits that are part of the Wiegand field.

The bits are named according to their position in the card format, starting from 0. You can enter the masks as a list of comma-separated bit positions, or as a range of bit position. For example, the mask "**1,2,3,4,5,6,7,8**" can also be written as "**1-8**" or "**1-4,5-8**". The order of the bits within the field is important ("**1,2,3,4**" is not the same as "**4,3,2,1**").

4 Click **OK**.

The field is added in the **Wiegand fields** section.



Wiegand fields

Agency
Mask: 1,2,3,4,5,6,7,8,9,10,11,12,13,14
Value: 255

System
Mask: 15-28

Credential
Mask: 29-48

Expiration Date
Mask: 49-73

Sequence generator:

Adding parity checks

If you are defining a custom Wiegand card format, you can add parity checks to strengthen the validation of your credentials.

What you should know

The order of the parity checks in the **Parity checks** list is important. It corresponds to the order in which the parity checks are evaluated. The mask of a subsequent parity check can include the parity bit of a previous parity check and their masks can overlap.

To add a parity check:

1 In the *Custom card format editor*, click **Add an item** (+) under the **Parity checks** section.

2 In the *Parity checks* dialog box, select the **Type** of parity check (**Even** or **Odd**).

3 In the **Parity bit** field, type the position of the parity bit in the card format (starts at 0)

4 In the **Mask** field, type the bits that should be evaluated.

The syntax must match the Wiegand data field mask values, but the order of the bits is not important.

5 Click **OK.**

The parity check is added in the **Parity checks** list.

Designing badge templates

To use customized printing templates for credential cards, you can design new badge templates that are tailored to your needs.

What you should know

A badge template is represented by a *badge template* entity in Security Center, and can include fields from the configuration database so that the correct name, cardholder photo, and so on, can be displayed on each card.

For example, you can add a company logo, a background image, employee photo, or a custom color to be printed on the access control cards.

To design a badge template:

1 Open the **Access control** task, and click the **Badge template** view.

2 Click **Badge template** (➕).

3 Type a name for the new badge template that appears in the entity list, and press **Enter**.

4 In the *Identity* page, type a description for the badge template.

5 In the *Relationships* section, select the partition where you want the badge template to be placed.

Partitions determine which Security Center users have access to this entity. Only users who have been granted access to the partition can see the badge template.

6 Click **Apply**.

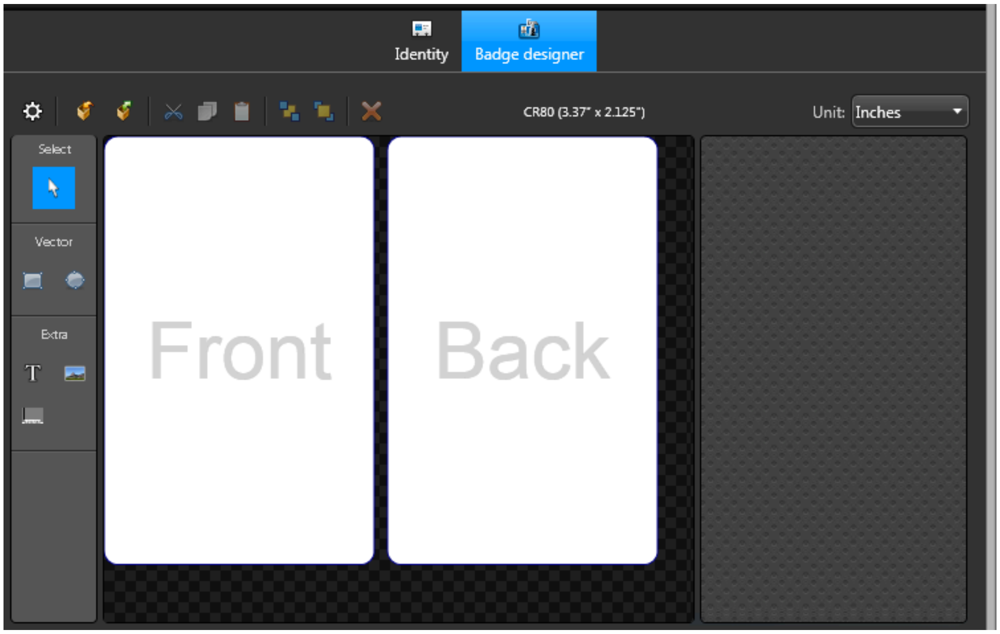
7 Click the **Badge designer** tab.

8 To select the size of the access control cards you want to print, click **Properties** (⚙).

9 In the *Format* dialog box, select a card size and orientation.

- To create custom card size, click ➕, enter the card name, width, and length, and then click **OK**.

10 Click **OK.**



Once the card size/format is chosen, you can design the actual printing template.

11 In the **Tools** section, select a tool, and then click the template to use it.

There are six graphical tools you can use to edit the template:

- **Select tool:** Use to click and select an object on the template.
- **Rectangle tool:** Use to draw a square/rectangle on the template.
- **Ellipsis tool:** Use to draw circles/ovals on the template.
- **Text tool:** Use to insert text on to the template. You can enter a static text or add dynamic cardholder and credential text fields, such as *First name*, *Last name*, and so on.
- **Image tool:** Use to insert a picture on to the template. You can insert cardholder pictures, a background image for the card, and so on.
- **Barcode tool:** Use to insert barcodes on to the template.

12 If you added an image to the template, select the image to edit it using the options in the **Image** and **Color and border** widgets.

In the **Image** widget, choose whether the **Source** of the image is a cardholder picture or an image from a file, and whether the image should be stretched or not.

- **Cardholder's picture:** Dynamic cardholder picture that changes, depending on which cardholder credential you are printing. This image field links to the value *Cardholder* picture in the configuration database.

  TIP: If a cardholder's picture was taken in front of a chroma key screen, you can make the picture background transparent. This is helpful if you are creating a badge template that has an image in the background.
- **File:** Static image selected from a file.

In the **Color and border** widget, you can use the following tools:

- **Fill:** Use to modify the fill color of an inserted object like a square or oval.
- **Border:** Use to modify the border color of an inserted object.
- **Opacity:** Use to modify the opacity of an inserted object.
- **Border thickness:** Use to modify the thickness of the inserted object's border

13 If you added text to the template, select the text to edit it using the options in the **Text** widget.

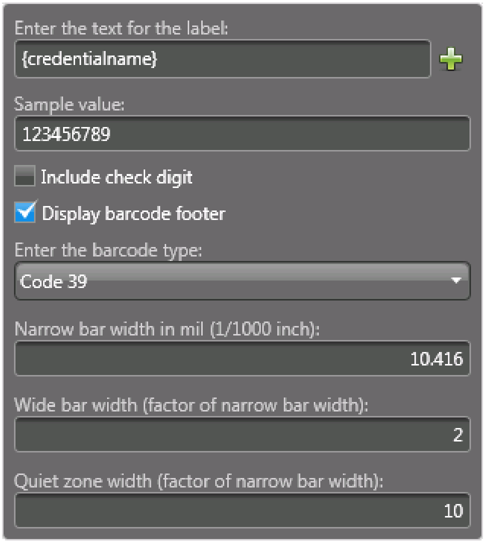
Right-click the text field to select the **Z order**, the text **Border**, **Font**, **Color**, and **Alignment**.

In the **Text** widget, you can use the following tools:

- Click **Add field** (➕) to add a dynamic cardholder or credential field. You can mix static text with the dynamic fields.
- Click **Fill** to set the text color.
- Click **Align left**, **center**, or **right** to set the text alignment.
- Click **Wrap text if too long** to turn on text wrapping.

  If text wrapping is turned on, the system wraps the text if it is too long to fit inside the text box, without changing the font size. If text wrapping is turned off, the system fits the text inside the text box by changing the font size.

14 If you added a barcode to the template, right-click the barcode, and then click **Properties** to edit it. The data on the barcode can be static or use dynamic credential properties.



Enter the text for the label:
{credentialname}

Sample value:
123456789

□ Include check digit

☑ Display barcode footer

Enter the barcode type:
Code 39

Narrow bar width in mil (1/1000 inch):
10.416

Wide bar width (factor of narrow bar width):
2

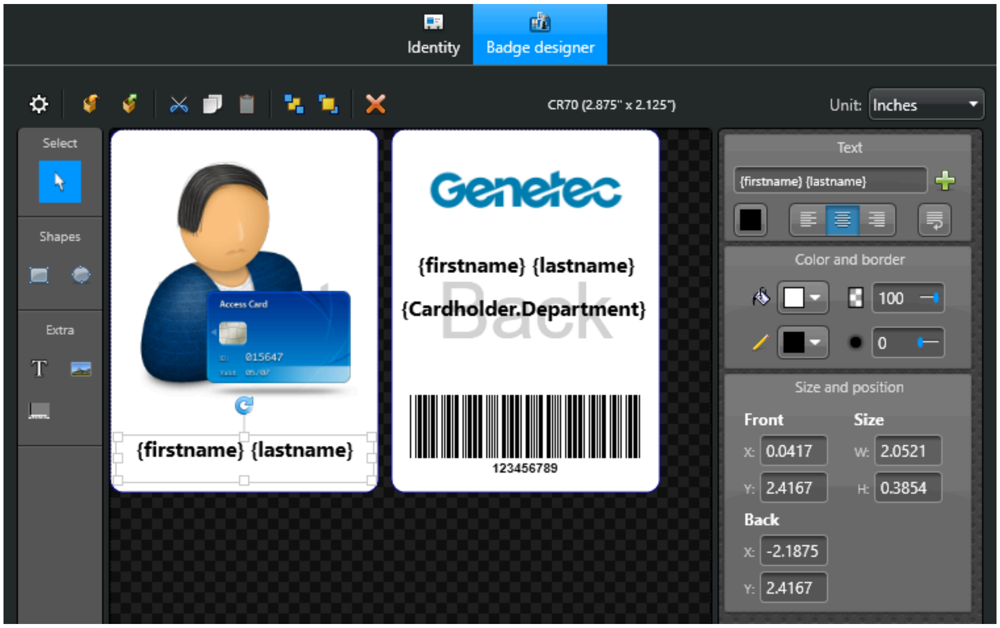
Quiet zone width (factor of narrow bar width):
10

15 In the *Size and position* section, select where the text, image, or barcode is located on the badge, and its width and height.

16 Click **Apply**.

Example

Here is a sample badge template with objects already inserted:



CR70 (2.875" x 2.125")

Unit: Inches

Text: {firstname} {lastname}

100

0

Front
X: 0.0417
Y: 2.4167

Size
W: 2.0521
H: 0.3854

Back
X: -2.1875
Y: 2.4167

- Two different images have been inserted. One is dynamic, and the other is static:
  - The dynamic cardholder picture is displayed on the front of the card.
  - The static image is displayed on the back of the card. It is the company logo that is displayed on every card.

- Three dynamic text fields have been inserted:
  - **{Firstname} {lastname}** appears on the front of the card. The text printed will be taken from the configuration database and we will see *first name, (space), last name*. The text is centered and text wrapping is turned on.
  - **{Firstname} {lastname}** appears on the back of the card. This is the same as the name field on the front except with a smaller font size, and text wrapping is turned off.
  - **{Cardholder.Department}** *Custom field* that was created for the cardholder entity.
- A barcode has been inserted, containing dynamic data. It displays the credential name, using the barcode type Code 39.

Viewing print previews of badge templates

After you design a new badge template, you can see what it is going to look like on a credential card.

To view a print preview of a badge template:

1. Open the *Access control* task and click the **Credentials** view.
2. Select the credential that you want to preview badge template with, and then click the **Badge templates** tab.

38

Global cardholder management

This section includes the following topics:

Global cardholder management

Global cardholder management (GCM) is used to synchronize cardholders between independent Security Center installations.

With GCM, you can have a central repository of cardholder information for your entire organization, whether this information is managed from a central office or by individual regional offices. The different locations can have their independent installations share information with a centralized human resource management system.

Each local office continues to manage the employees working at their local office, such as maintaining the employee profiles, photo ID’s, credentials, and so on. For employees that need to travel from site to site, that same information can be shared among all sites within the organization.

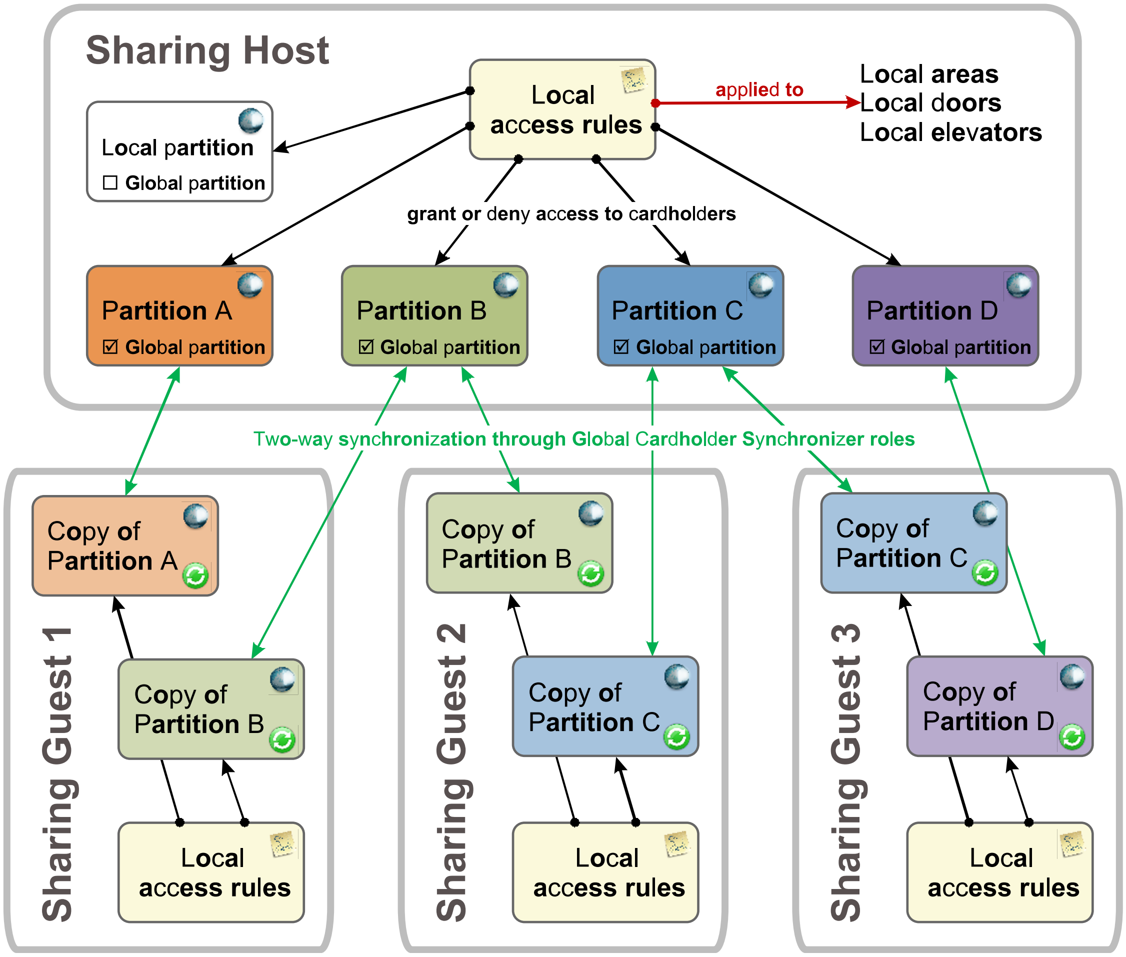
With GCM, you can do the following:

- Create global cardholders from a central location (for example, your head office) and synchronize them at remote Security Center systems that operate independently of the central system and of each other.

  NOTE: Unlike cardholders and cardholder groups, visitors and visitor groups are not synchronized between independent Security Center installations.
- Allow local system administrators to decide which areas global cardholders can or cannot access at their local facilities.
- Allow local system administrators to make changes to global cardholders and their related entities, and synchronize those changes with other sharing systems.
- Allow local system administrators to keep exclusive ownership of their local cardholders and related entities, while sharing global cardholders with other systems.

Architecture of Global cardholder management

To share cardholders across multiple independent Security Center systems, one of the systems must act as the *sharing host*, while the others act as *sharing guests*.



Sharing host system

The sharing host is the Security Center system that you choose to *initiate* the sharing process. This is done by creating a *global partition* on that system. All cardholders, cardholder groups, credentials, and badge templates that are members of the global partition automatically become available for sharing. Other types of entities can be part of the global partition, but they are not visible to the sharing guests.

The sharing host owns the *master copy* of the global partition and the entities that are in it. The sharing host validates all changes made by a sharing guest to the content of the global partition before propagating the change to other sharing parties.

The global partition is like a central database. The sharing host is like the database server and the sharing guests are like the database clients. There is no limit to the number of global partitions that a host system can share.

Sharing guest systems

The sharing guest is a Security Center system that *participates* in the sharing process. Participation is achieved by creating a Global Cardholder Synchronizer (GCS) role on that system, and using it to connect the sharing guest to the sharing host.

As the sharing guest administrator, you can decide which partitions shared by the host are of interest to your system. The GCS role then creates a copy of the selected global partitions and entities on your local system. Only cardholders, cardholder groups, credentials, and badge templates are eligible for sharing. The shared entities are visually identified with a green icon (🔄) superimposed over the regular entity icon.

You can assign local access rules and credentials to global cardholders to grant them access to your local areas, doors, and elevators. You can create, modify, and delete entities from the global partition. The actions you can perform depend on the access rights and privileges of the user account representing the GCS role on the sharing host. All changes made to global entities on the guest system must be validated by the host system. All modifications rejected by the host system are also rejected on your local system.

Differences between Federation™ and GCM

Global cardholder management (GCM) and Federation™ are both used for sharing information in Security Center, but cardholders and other information are shared differently.

The following table highlights the differences between GCM and Federation™.

BEST PRACTICE: Use GCM and Federation™ together on the same system to complement each other.

Federation™ (applied to access control)	Global cardholder management (GCM)
Purpose: Central activity and event monitoring	Purpose: Sharing of a central configuration
Allows an organization to *monitor* from a central location (Federation™ host), the access control events and activities at independent remote locations (federated sites).	Allows an organization to *share* the common configuration of access control entities, hosted at a central location (sharing host), with independent remote locations (sharing guests).
The Federation™ host uses the Security Center Federation™ role to connect to the remote sites.	The remote sites use the Global Cardholder Synchronizer role to connect to the sharing host.
Entities created at remote sites are federated at the central system.	Entities created at the central system are shared at the remote sites.
The Federation™ host can observe, but cannot change anything on the remote sites. Remote entities can be created, modified, or deleted using the *Remote configuration* task.	The remote site can create, modify, and delete the entities that are shared by the host with all other remote sites (two-way synchronization).
A federated site has no visibility on what is going on at the Federation™ host or other federated sites.	All sharing guests have the same read/write access to all shared (global) entities, while maintaining full ownership of the local entities.
Almost all entities that generate events can be federated (monitored).	Only cardholders, cardholder groups, credentials, and badge templates can be shared.
Custom fields are not federated.	All custom fields and data types are shared.
A federated cardholder can be granted access to the facility managed by the Federation™ host, but not the reverse.	A global cardholder can be granted access to all facilities participating in the sharing.

Related Topics

Rules and restrictions for Global cardholder management on page 898

About the Federation™ feature on page 268

Differences between Active Directory integration and GCM

Global cardholder management (GCM) and Active Directory integration are both used to centralize the management of cardholder information in Security Center, but their approach is different.

The following table highlights the differences between GCM and Active Directory integration.

BEST PRACTICE: Use Active Directory integration and GCM in tandem. The sharing host should be the only system that integrates with the Active Directory. This solution keeps the Active Directory protected on the corporate LAN, while the sharing host only pushes the employee information that need to be shared to the satellite systems.

Active Directory integration	Global cardholder management (GCM)
Purpose: Centralized employee (users and cardholders) security management	Purpose: Centralized employee (cardholders) security management
Allows an organization to *manage* the employee information from a central location, and share it with a single Security Center system (users and cardholders).	Allows an organization to *manage* the cardholder information from a central location, and share it with all Security Center systems within the organization.
The corporate directory service is the information source. Security Center gets the employee information from the corporate directory service.	One Security Center system acts as the information source (sharing host), and shares it with all other Security Center systems within the organization (sharing guests).
The Security Center system connects to the information source (directory service) through the Active Directory role.	The sharing guests connect to the information source (sharing host) through the Global Cardholder Synchronizer role.
Custom fields defined on the Active Directory can be linked to Security Center custom fields.	All custom fields and data types are shared.
The shared employee information can only be modified on the Active Directory. Only the cardholder picture can be loaded in Security Center and updated on the Active Directory.	The shared information can be modified by all sharing parties. The sharing host validates and propagates the changes to all sharing parties.
The source information can only be shared with one Security Center system. If multiple Security Center systems need to share the same information, they need to connect individually to the corporate directory service.	The central Security Center system can share the cardholder information with as many satellite Security Center systems as needed.

About Global Cardholder Synchronizer roles

The Global Cardholder Synchronizer role ensures the two-way synchronization of shared cardholders and their related entities between the local system (sharing guest) where it resides and the central system (sharing host).

Only a single instance of this role is permitted on each system.

The Global Cardholder Synchronizer can synchronize the host and the guest using the following three ways:

- **On demand:** The guest system is synchronized only when it is requested by a user.
- **On schedule:** The guest system is synchronized on schedule using a scheduled task.
- **Automatically:** The guest system is synchronized automatically.

The guest-to-host synchronization is always performed immediately by the GCS role, because all changes to the global partitions must be validated by the host system before they can be accepted by the guest system. The host system processes the change requests on a first come, first served basis. The Global Cardholder Synchronizer (GCS) role must stay connected to the sharing host to keep the local copies of the *global entities* synchronized with the host.

NOTE: The Global Cardholder Synchronizer can sync up to a maximum of 250,000 credentials.

Rules and restrictions for Global cardholder management

Before you start globally managing your cardholders, read the rules and restrictions that apply when using Global cardholder management.

Rules concerning local and global partitions

- A sharing guest cannot have more than one host. Only one instance of the GCS role is allowed per system.
- A global partition cannot be modified on a sharing guest, but its members can. What the sharing guest is actually allowed to modify is subject to the privileges of user assigned to the GCS role.
- No system is allowed to share what it does not own. Two-tier sharing is not permitted. An effect of this rule is that a local partition cannot be converted into a global partition if it contains global entities, unless it is performed on the host system.
- Adding a local entity to a global partition transfers the ownership of that entity from its local owner (sharing guest) to the partition owner (sharing host).
- Deleting a global entity on a sharing guest also deletes it on the sharing host, unless that entity also belongs to another global partition, in which case, only its membership is removed from the first partition.

Rules concerning local and global entities

- An entity is global by virtue of its membership to a global partition. This means that a cardholder does not automatically become global simply because its parent cardholder group is global.
- Local access rules can apply to local and global cardholders alike. Access rules are never shared. This ensures that local administrators always have full control over the security of their local facilities.
- Global cardholders and groups can become members of local cardholder groups.
- Local cardholders and groups cannot become members of global cardholder groups. An exception to this rule is when both entities belong to the same system. In this case, the local cardholder cannot be shared, although the cardholder group can.
- Both global and local credentials can be assigned to global cardholders.
- Global credentials cannot be assigned to local cardholders.
- Global credentials using custom card formats can be used and edited on the sharing guest. However, the credential data would only be visible if the corresponding custom card format (XML file) is also defined on the sharing guest using the *Custom card format editor* tool.

BEST PRACTICE: It is always recommended to apply access rules to cardholder groups rather than individual cardholders. For this reason, it is recommended to share the cardholders along with their parent cardholder groups. If this is not feasible for any reason, then we recommend that you create a local cardholder group for the global cardholders.

Rules concerning global custom fields and data types

- Custom fields and data types defined for global entities are automatically shared when the global entities are shared.
- Global custom field and data type definitions cannot be modified on the sharing guest.
- Global and local custom fields remain separate. They are differentiated by their owner, which is the system that defines them.
- Global and local custom field and data type definitions cannot have the same names. Using the same names for custom fields or data types causes the synchronization of cardholders and credentials to fail.
- Global data types cannot be used to define local custom fields.
- Custom field values of global entities can be modified on sharing guests.
- Global custom fields also apply to local entities, but their values stay local.
- Local custom fields also apply to global entities, but their values stay local.

- When a guest system stops sharing a global partition, all local copies of the shared global entities, and the custom field values of the local entities are deleted.

BEST PRACTICE: If you are to implement GCM within your organization, we recommended that you define all custom fields and data types for global entities on the sharing host.

Rules concerning Federation™ and global entities

- If a sharing host also federates its sharing guest, only the local entities belonging to the sharing guest are federated. The entities that are shared are not federated on the sharing host.
- The sharing host that also happens to be a Federation™ host should not share the entities that it federates by adding them to a global partition because it does not own the federated entities. An entity can only be shared by its rightful owner. For the federated entities to become shared, the federated system needs to be a sharing guest of the Federation™ host. This gives the Federation™ host the rights to share any of the federated entities.
- A sharing guest which happens to federate a third system cannot share its federated entities with the sharing host, because it is not the owner of the federated entities.
- If a sharing guest is federated by another system, both its local and global entities appear as federated entities on the Federation™ host.

Rules concerning Active Directory and global entities

- Cardholders and cardholder groups imported from an Active Directory can be added to a global partition on the sharing host.
- Cardholders and cardholder groups imported from an Active Directory that is local to the sharing guest cannot be added to a global partition because the Active Directory and the sharing host cannot both be owners of the shared cardholders.
- Global cardholders and cardholder groups imported from an Active Directory must only be modified through the directory service that owns them.

CAUTION: Although it is possible to modify global cardholders and cardholder groups imported from an Active Directory on the sharing guest, these changes are temporary. You lose the changes you made when the sharing host synchronizes with the Active Directory.

BEST PRACTICE: If all cardholder data entry must be centralized, the system that imports cardholders from your corporate Active Directory should act as the sharing host, and all modifications must be made using the directory service.

Related Topics

Importing security groups from an Active Directory on page 481

About federated entities on page 270

Custom card formats on page 882

Preparing to synchronize entities across sites

Before you can share and synchronize cardholders, cardholder groups, credentials, and badge templates with other sites, there are some steps you must take.

Before you begin

IMPORTANT: You should not attempt to deploy the Global cardholder management solution on your own if you intend to bring together systems that have data to share on both ends, meaning that both the sharing host and the sharing guest have existing data to share. If this is your situation, we strongly recommend that you book a technical consultation with a GTAP specialist.

To prepare synchronizing entities across sites:

1. Decide which Security Center system is going to be the sharing host.

   The sharing host is typically the system running at your head office or the system that is synchronized with your corporate Active Directory.
2. If the sharing host is protected behind a firewall, open a port to allow the Global Cardholder Synchronizer role to connect to the sharing host.
3. Decide what types of updates the users on the guest systems are allowed to perform on the shared global partitions.

   You can limit their range of actions by restricting the privileges of the user representing the GCS roles on the host system.
4. Make sure you follow the recommended best practice:
   - Avoid assigning cardholders directly to access rules. Assign cardholder groups instead.
   - Avoid assigning cardholders or cardholder groups directly to doors. Use access rules instead.
5. Back up the Directory database on all the systems you intend to synchronize and enable scheduled backups.

After you finish

Share entities across sites.

Related Topics

Ports used by core applications in Security Center on page 1452

Differences between Active Directory integration and GCM on page 896

Synchronizing entities across sites

To share information with other sites in your system, you can synchronize cardholders, cardholder groups, credentials, and badge templates.

Before you begin

Prepare the synchronization.

To synchronize entities across sites:

1 On the sharing host, create global partitions or change the status of local partitions to global.

2 Create a user with the proper level of administrative privileges over the shared entities so it can be used to connect the GCS roles to the sharing host.

You might have to create more than one user accounts if the sharing guests have different update requirements.

3 On each sharing guest system, create a GSC role and synchronize the sharing guest with the sharing host.

4 Assign local users to global partitions (🌐).

5 Apply local access rules to global cardholders (👤) and cardholder groups (👥).

NOTE: Custom card formats are not shared. If you have shared credentials that use custom card formats, the credentials will work on your local system, but you will not be able to view the card data fields unless the custom card format in use is also defined on your local system.

6 Create a scheduled task to periodically synchronize your local system to the host.

Related Topics

Custom card format editor tool on page 883

Setting up partitions for synchronizing

The entity synchronization is initiated on the sharing host by setting a partition as *a global* partition.

What you should know

You cannot share the *Public partition*.

To set up a partition for synchronizing:

1 Open the *Access control* task, and select the **Cardholders and credentials** view.

2 If the partitions are hidden, click **Show partitions** (🌐)

3 Select the partition you want to share.

4 Click the **Properties** tab, and switch the **Global partition** option to **ON**.

The partition is now visible to all GCS roles connected to this system. Only cardholders, cardholder groups, credentials, and badge templates are shared.

Synchronizing your system with the sharing host

You must create and configure the Global Cardholder Synchronizer (GCS) role to connect your local system to the sharing host.

To synchronize your system with the sharing host:

1 Open the *System* task and click the **Roles** view.

2 Click **Add an entity** (➕) > **Global Cardholder Synchronizer**.

3 On the *Specific info* page, enter the following parameters, and then click **Next**.

- **Server:** Server where this role will be hosted.
- **Directory:** Sharing host's main server name. If anything else than the default connection port (5500) is used, you must explicitly indicate the port number after the Directory name, separated by a colon. For example: HostServer:5888.
- **Username and Password:** Credentials used to connect to the sharing host. The extent of what the sharing guest can do on the global partition will be limited by what this user can see and do on the sharing host.

  The user must have the *Global Cardholder Synchronizer* privilege on the sharing host in order to connect.

4 On the *Basic information* page, enter the name, description, and partition where the GCS role should be created.

Partitions determine which Security Center users have access to this entity. Only users who have been granted access to the partition can see the GCS role.

5 Click **Next**, **Create**, and **Close**.

A new Global Cardholder Synchronizer () role is created. Wait a few seconds for the role to connect to the sharing host.

6 Click the **Properties** tab, and click **Refresh** () .

The partitions shared by the host are listed under **Global partitions**.

7 Select the partitions you want your local system to share and click **Apply**.

8 Click **Synchronize** (⇅).

The GCS role creates a local copy of all shared entities on your system. This might take a while depending on how many entities you are sharing.

After you finish

Configure the global entities you shared so they can be used on your local system.

Sharing entities with other sites

You share an entity by adding it to a global partition. This can be done from both the sharing host or the sharing guest. You can also create a new entity directly in a global partition.

What you should know

A *global entity* is an entity that is shared across multiple independent Security Center systems by virtue of its membership to a global partition. Only cardholders, cardholder groups, credentials, and badge templates are eligible for sharing.

To share an entity with another site:

1. Open the *Access control* task, and select the **Cardholders and credentials** view.
2. If the partitions are hidden, click **Show partitions** (🌐)
3. Select the global partition you want to share it from, and click the **Properties** tab.
4. Under the *Members* section, click **Add** (➕).
5. In the *Search* dialog box that appears, pick the entity you want to share, and click **Select**.

   On the sharing guest, only cardholders, cardholder groups, credentials, and badge templates can be added to a global partition.

On the sharing host, the effect of this action is immediately visible. On a sharing guest, the newly shared entity does not appear until after a synchronization is performed on their GSC role.

Related Topics

Global Cardholder Synchronizer configuration tabs on page 1360

Stopping entity sharing with other sites

You stop sharing an entity by removing it from its global partition. This can be done from both the sharing host or the sharing guest.

What you should know

If you remove a shared entity from the sharing guest system, the entity is converted from a global entity to a local entity.

CAUTION: Removing a shared entity from a global partition deletes it from all other systems that might be sharing it, even from the sharing host.

To stop sharing an entity with another site:

1. Open the *Access control* task, and select the **Cardholders and credentials** view.
2. If the partitions are hidden, click **Show partitions** (🌐)
3. In the *Members* section, select the entity you want to stop sharing, and click **Remove** (✖).
4. To confirm the action, click **Remove**.

After you finish

Any entity removed from a partition ends up in the root partition. If the root partition is not where you want it to be, move it to another local partition.

Overriding synchronized cardholder statuses

If the GCS role is disconnected from the sharing host, and you need to change a cardholder status, you can override the entity synchronization.

What you should know

If the GCS role is disconnected from the sharing host, all global entities at the sharing guest become inactive (red), and you can no longer make any changes to them because they cannot be validated by the sharing host. However, if you urgently need to deactivate a cardholder (for example, if an employee has just been fired) you can temporarily *override* the synchronization.

To override the status of a synchronized cardholder:

1. Open the *Access control* task, and click the **Cardholders and Credentials** view.
2. Select the global cardholder you need to activate or deactivate.
3. Click the **Properties** tab, and switch the **Status** option to **Override**.

   The cardholder icon changes to . You can now change the cardholder’s status.
4. Make the necessary changes and click **Apply**.

After you finish

When the connection with the sharing host is re-established, turn the synchronization on again.

Upgrading Security Center with Global Cardholder Synchronizer roles

To upgrade a composite Security Center system involving Global Cardholder Synchronizer (GCS) roles, you must upgrade the sharing host system first, then upgrade the sharing guest systems.

Before you begin

Back up the Directory databases of your *sharing host* and *sharing guest* systems.

To upgrade a composite Security Center system involving GCS roles:

1. Disconnect the sharing guests from the sharing host.

   Do one of the following:

   - Deactivate the GCS roles on the sharing guest systems.
   - Temporarily change the passwords of the GCS role user accounts.

2. Upgrade the sharing host system first.
3. Upgrade the sharing guest systems next.
4. Confirm that the upgrades were successful.
5. Reconnect the sharing guests to the sharing host.

   Do one of the following:

   - If you deactivated the GCS roles on the sharing guest systems, reactivate them.
   - If you changed the passwords of the GCS role user accounts, change them back.

6. Give the sharing guests some time to sync with the sharing host.

Related Topics

Overview of the System status task on page 382

Architecture of Global cardholder management on page 894

39

Import tool

This section includes the following topics:

About the Import tool

The Import tool is the tool that you can use to import cardholders, cardholder groups, and credentials from a comma-separated values (CSV) file.

The CSV file must be plain text with delimiters (commas, spaces, periods, and so on) to separate the fields. The delimited fields in the text files would represent values such as first name, last name, cardholder group, path and filename of employee photo, and so on.

The Import tool Security Center license must be enabled in your system for this tool to be available. The *Import tool* privilege is also required to launch this tool.

You can use the Import tool on a schedule, using the *Import from file* action.

How you can use the Import tool

You can use the Import tool to do the following:

- Import credentials alone:
  - Card format
  - Card number
  - Credential activation date
  - Credential code
  - Credential expiry date
  - Credential name
  - Facility code
  - License plate
  - Number of inactive days to expire credential
  - Number of days after first use to expire credential
  - Partition
  - PIN
  - Status
- Import cardholders alone:
  - Cardholder activation date
  - Cardholder expiry date
  - Cardholder group
  - Cardholder name
  - Custom field
  - Description
  - Email
  - Mobile phone number
  - Number of inactive days to expire cardholder
  - Number of days after first use to expire cardholder
  - Partition
  - Picture
  - Status
  - Whether cardholder escort visitors

- Import cardholders and credentials together (in this case, the cardholder and the credential are specified on the same line and automatically linked together).
- Replace old credentials with new ones.

Limitations of the Import tool

If you are importing multiple cardholders who are members of different partitions, and there is either no cardholder group or only one cardholder group specified in the CSV file, the imported cardholders are added to all the partitions.

Related Topics

Replacing credentials on page 916
Scheduled tasks on page 220

CSV files and the Import tool

To import comma-separated values (CSV) files using the Import tool, the CSV file must follow a format and include information for each type of entity. These files can be imported from an Excel spreadsheet.

Minimum information required in CSV files

The information in the CSV file must be coherent to be accepted by the Import tool. When required information is missing, the **Next** button in the *Bindings* page is disabled. Each type of imported entity has a minimum information requirement, as described in the following table:

Entity type	Minimum information required
Credential: Card	You have the choice of two credential keys: • Complete all fields required by a given card format. • Supply the Credential card data. If you choose a custom card format, all fields required by your card format must be bound to a column in the CSV file. Otherwise, the CSV file is rejected. When credentials are being imported, one of these two keys must be present. If both keys are missing values, the line is discarded. If both keys are present, only the card data is imported.
Credential: License plate	Enter a cardholder's license plate number. Use this method if a Sharp camera is being used to trigger a vehicle access barrier. In this case, the cardholder's vehicle license plate can be used as a credential.
Credential: PIN	PIN credentials can be used with cards or as standalone credentials. Make sure that each cardholder's PIN is unique if you plan to use your readers in Card or PIN mode.
Cardholder	The default cardholder key is the combination of the cardholder’s first and last name. One of these two fields must be bound to a CSV column if cardholders are to be imported. When cardholders are being imported, all CSV lines must have a value in at least one of these two fields. If not, the line would be discarded.
Cardholder group	Only the cardholder group name is required. Missing the cardholder group does not cause a line to be discarded.
Partition	Only the partition name is required. Missing the partition name does not cause a line to be discarded.

Format of the CSV file

Here is an example file called *EmployeeData.csv*, containing three new cardholders to import. It can be created from a spreadsheet by saving it as a *.csv* file in Excel.

The sample file contains the following four lines of text:

```
#First name,Last name,Picture,Cardholder description,Cardholder email,
Cardholder group,Cardholder status,Credential name,Facility code,Card
 number,Credential status,Cardholder_activation,Cardholder_expiration,
 Credential_activation,Credential_expiration
Abdoulai,Koffi,D:\Tools\Import\WithPics\Koffi.jpg,Market
 Analyst,akoffi@genetec.com,Marketing,Yes,82968378,102,8,active,10-10-2018
 7:00:00,10-20-2018 17:00:00,10-10-2018 7:00:00,10-20-2018 17:00:00
Andrew,Smith,D:\Tools\Import\WithPics\Smith.jpg,Sales
 Representative,asmith@genetec.com,Sales,Yes,82748590,101,12,active,10-12-2018
 8:00:00,10-14-2018 17:00:00,10-12-2018 8:00:00,10-14-2018 17:00:00
Audrey,Williams,D:\Tools\Import\WithPics\Williams.jpg,Technical
 Writer,awilliams@genetec.com,TechWriters,Yes,83748952,104,18,active,10-13-2018
 7:00:00,10-20-2018 18:00:00,10-13-2018 7:00:00,10-20-2018 18:00:00
```

The first row is a comment line, listing the cardholder and credential fields that are included in the CSV file as a reference. The following three rows contain the fields to be imported. You can add additional custom fields if they have been created for cardholders or credentials in Security Center.

IMPORTANT: If you add columns for activation and expiration dates without defining the time of day, activation and expiration are set to midnight by default. If you set specific hours, use 24-hour time.

TIP: Instead of the cardholder or credential expiry date, you can provide the number of days after first use or the number of inactive days after which the cardholder or credential will expire.

Notes and limitations about custom fields

Note the following about importing cardholder and credential custom field values from CSV files:

- When you import a blank field for a custom field using the *Text* data type, the default value is set. If the default value is not defined, the imported custom field is blank.
- When you import a blank field for a mandatory and unique custom field using the *Text* data type, the existing value is not changed.

You can import cardholder and credential custom field values from CSV files with the following limitations:

- You cannot import custom fields using the *Entity* data type.
- Custom fields using the *Date* data type must be imported with the YYYY-MM-DD format.
- The Import tool performance decreases as the number of custom fields per imported record increases.
- When you have a large number of custom fields per record, the number of records you can import at the same time might also be limited. For example, if your records contain 100 custom fields each, including a 25 KB image data field, you can only import 1000 records at a time.
- If you are importing pictures, the CSV file must include the full path to the image file.

Related Topics

Database fields supported by the Import tool on page 919

About custom fields on page 91

Notes about imported entity names

Security Center supports multiple entities with the same name. If a cardholder already exists in Security Center with the same first and last name combination as one being imported, only the first matching cardholder found in the Security Center will be updated (for example, with a new description from the imported CSV file).

If there are two cardholder groups with the same name (for example, created in two different partitions) and an imported cardholder is assigned to one of these cardholder groups, the cardholder will be assigned to the first cardholder group found. The same logic also applies to partitions.

If the same cardholder is imported twice, each time with a different cardholder group, in the end, the cardholder will belong to both cardholder groups. Again, the same logic applies to partitions.

However, the association between cardholders and credentials might be treated differently, depending on whether the credential is part of the cardholder key or not.

Example

If the cardholder key is only composed of the cardholder's first and last names. The result of importing the following CSV file is the creation of a new cardholder: First name = Joe, Last name = Dalton, Email = JDalton@genetec.com, and with two card credentials (12/555 and 12/556).

First name	Last name	Facility code	Card number	Email
Joe	Dalton	12	555	jdalton@acme.com
Joe	Dalton	12	556	jdalton@acme.com

However, if the credential is also part of the cardholder key, the same CSV file will generate two separate cardholders with the same first name, last name and email address.

Importing cardholders and credentials

To accelerate the setup of your system, you can import cardholders and credentials from a CSV file instead of creating them manually in Security Center.

Before you begin

If you want to receive an email report after importing cardholders and credentials using a scheduled task, ensure that the user selected as the recipient of the schedule task is configured with an email address. This is configured in the *User management* task, on the *Properties* page of the user.

What you should know

Importing cardholders and credentials manually differs from doing so using a scheduled task. When configuring an *Import from file* scheduled task, note the following:

- If you are using a network path, you must enter it manually and include the full file name of the CSV file, including the suffix.
- By default, the CSV source file is automatically deleted after a successful scheduled import, and an email is sent to the recipient configured in the scheduled task; you must generate a new source file for the next scheduled import.
- If the import fails, the source CSV file is renamed to include the word "Errors" in the file name, and an email is sent to the recipient configured in the scheduled task. You can use the Windows Event Viewer to see why the import failed.

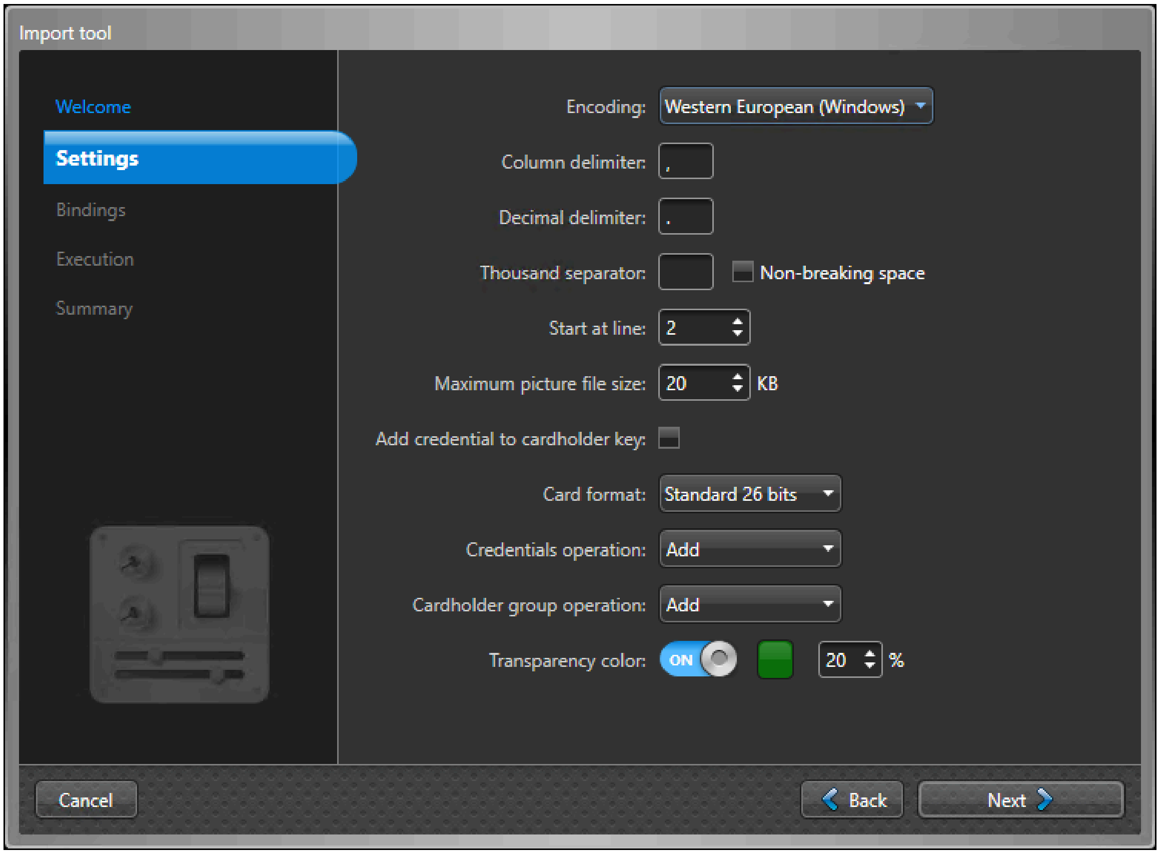
To import cardholders or credentials:

1 Do one of the following:

   - To import cardholders or credentials manually, from the Config Tool home page, click **Tools** > **Import tool**.
   - To import cardholders or credentials using a scheduled task, from the Config Tool home page, open the *System* task, click the **Scheduled tasks** view, and then configure a new scheduled task as follows:
     - **Status:** Set to **Active**.
     - **Recurrence:** Select how often you want the task to run.
     - **Action:** Select **Import from file**.
     - **Recipient:** Select a user.
     - **File name:** Click ✏ to open the Import tool.

2 On the *Welcome* page of the Import tool, enter the file path to the CSV file you want to import, and click **Next**.

The *Settings* page opens.



Encoding: Western European (Windows)

Column delimiter: ,

Decimal delimiter: .

Thousand separator: □ Non-breaking space

Start at line: 2

Maximum picture file size: 20 KB

Add credential to cardholder key: □

Card format: Standard 26 bits

Credentials operation: Add

Cardholder group operation: Add

Transparency color: ON 🟩 20 %

3 On the *Settings* page, configure the import settings:

- **Encoding:** Select the character encoding type.
- **Column delimiter:** Set the CSV field delimiter for columns.
- **Decimal delimiter:** Set the CSV field delimiter for decimals.
- **Thousand separator:** Set the CSV field delimiter for thousand separators.
- **Start at line:** (Optional) Enter a value of 2 or greater to reserve lines for column headings or comment lines.
- **Maximum picture file size:** (Optional) Set the maximum picture file size to minimize storage usage. The default value is taken from your access control system settings. Changing its value in the Import tool also changes your system settings.
- **Add credential to cardholder key:** Select this option if the CSV file contains both cardholder and credential information.

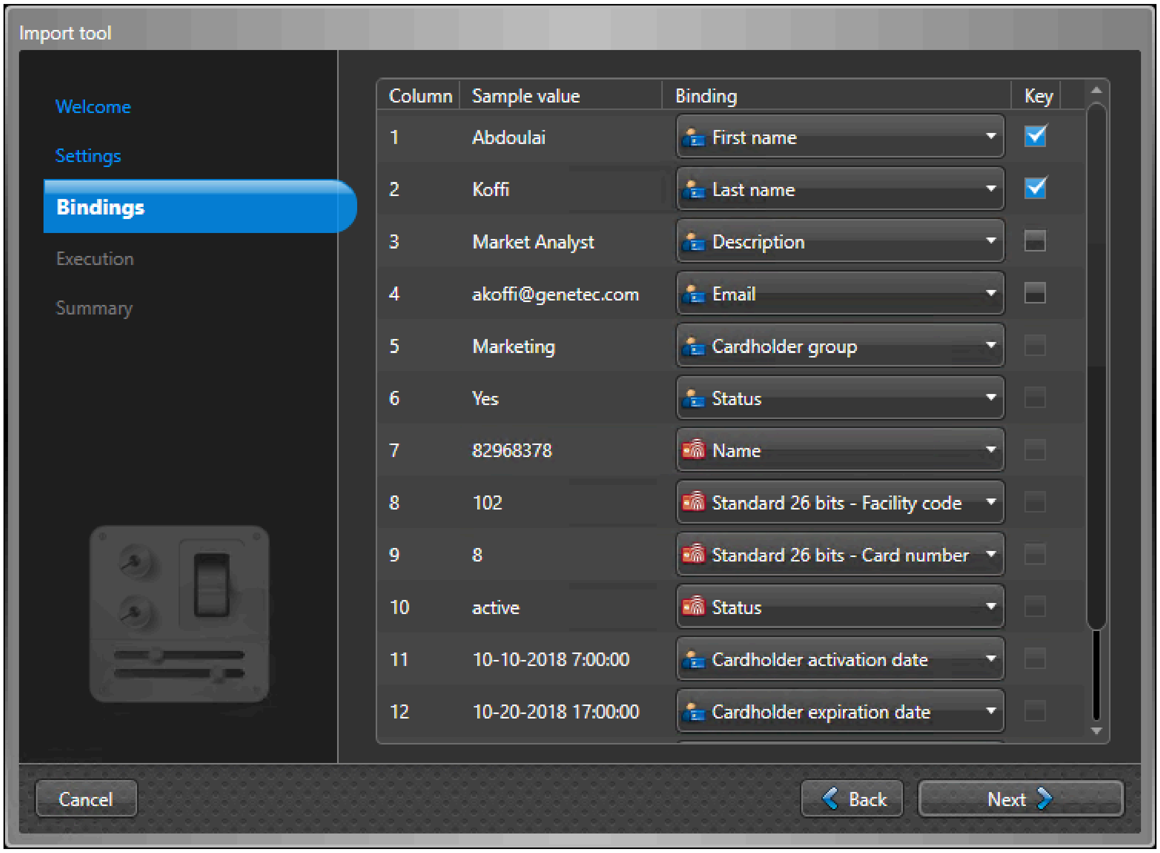
  NOTE: This option is only applicable when cardholders and credentials are imported from the same CSV file. When this solution is not applicable, other cardholder information can be used to strengthen the cardholder identification.
- **Card format:** Select the default card format to use when a card format is not specified in the CSV file.
- **Credential operation:** Select one of the following options:
  - **Add:** This is the default option. All credentials read from the CSV file are added as entities to your system. If a credential already exists in your database, it will be updated.
  - **Replace:** With this option, you can replace old credentials with new ones. On the *Bindings* page, you will find additional options to specify old (*previous*) and new credential values.
- **Cardholder group operation:** Select one of the following options:

    - **Add:** This is the default option. All cardholder groups from the CSV file are added to your system as entities. If a cardholder group already exists, the cardholder will be added to the group.
    - **Replace:** With this option, you can change a pre-existing cardholder's group membership. To reassign a cardholder to a new group, change their group value in the CSV file, then set the cardholder group column to **Cardholder group** on the *Bindings* page.

- **Transparency color:** (Optional) If the cardholder pictures you are importing were taken in front of a chroma key screen, you can make the picture background transparent. This is helpful if you created a badge template with a background image. To set the background transparency of imported cardholder pictures, turn the option on, select the color of the chroma key screen the cardholder pictures were taken in front of (usually green or blue), and then set the transparency percentage.

4 Click **Next**.

The *Bindings* page opens.



Column	Sample value	Binding	Key
1	Abdoulai	First name	☑
2	Koffi	Last name	☑
3	Market Analyst	Description	□
4	akoffi@genetec.com	Email	□
5	Marketing	Cardholder group	□
6	Yes	Status	□
7	82968378	Name	□
8	102	Standard 26 bits - Facility code	□
9	8	Standard 26 bits - Card number	□
10	active	Status	□
11	10-10-2018 7:00:00	Cardholder activation date	□
12	10-20-2018 17:00:00	Cardholder expiration date	□

5 On the *Bindings* page, for each sample value, select a corresponding database field in the *Binding* column.

If you need to skip a column in your CSV file, leave the *Binding* column blank.

NOTE: For entities like cardholders and credentials, a minimum amount of information is required to complete the import.

6 (Optional) Add more fields to the cardholder key.

If you need to differentiate cardholders, you can add additional information by selecting the **Key** check box beside each field you want to add to the cardholder key. The check box is disabled for ineligible fields.

TIP: The other method to strengthen the cardholder identification is to add the credential data to the cardholder key.

7 Click **Next**.

The Import tool imports the contents of your CSV file into the database. A summary window opens, confirming the number of entities imported and the number of errors encountered.

8 Click 📋 to copy and paste the contents of the report.

9 Click **Close**.

Related Topics

Database fields supported by the Import tool on page 919
CSV files and the Import tool on page 909
Defining the maximum file size of pictures on page 823
Replacing credentials on page 916
Designing badge templates on page 888

Replacing credentials

If you have multiple credentials that must be replaced, you can replace them all at the same time, using the *Import* tool.

Before you begin

Create a CSV file with both old and new credential values. Each line must contain both the old credential and the new credential to replace it with.

What you should know

The old and new credential must use the same card format. If the new credentials are to be assigned to the same cardholders, they must also be specified in the CSV file, and cannot be different than the current cardholder of the old credentials.

For example, replacing credentials is helpful if you want to give all the employees in your company new ID cards.

To replace a credential:

1. From the homepage, click **Tools** > **Import tool**.
2. Enter the path to the CSV file you want to import, and click **Next**.
3. On the *Settings* page, select **Replace** as **Credentials operation** and click **Next**.
4. On the *Bindings* page, bind the old credential values with the fields labelled as **(previous value)** and the new credential values with the fields not labelled as **(previous value)**.
5. Click **Next**.

   The Import tool changes the status of the old credential to **Inactive**, while creating the new credential as **Active**. If the cardholders are also imported in the same file, the new credentials are associated to the cardholders.

   The result of the operation are displayed in a summary window.
6. Click 📋 to copy and paste the contents of the report.
7. Click **Close**.

Related Topics

Importing cardholders and credentials on page 912

Replacing cardholder groups

If you have to reassign multiple cardholders to new groups, you can reassign them all at the same time using the Import tool.

Before you begin

Create a copy of the cardholder's existing CSV file, then update the cardholder groups data.

NOTE: If you want to remove all cardholder groups from the cardholder, enter <NOGROUP> as the group in the CVS file.

What you should know

Replacing cardholder groups in batches is useful in contexts like that of a student who changes groups between semesters because different courses might dictate different access permissions.

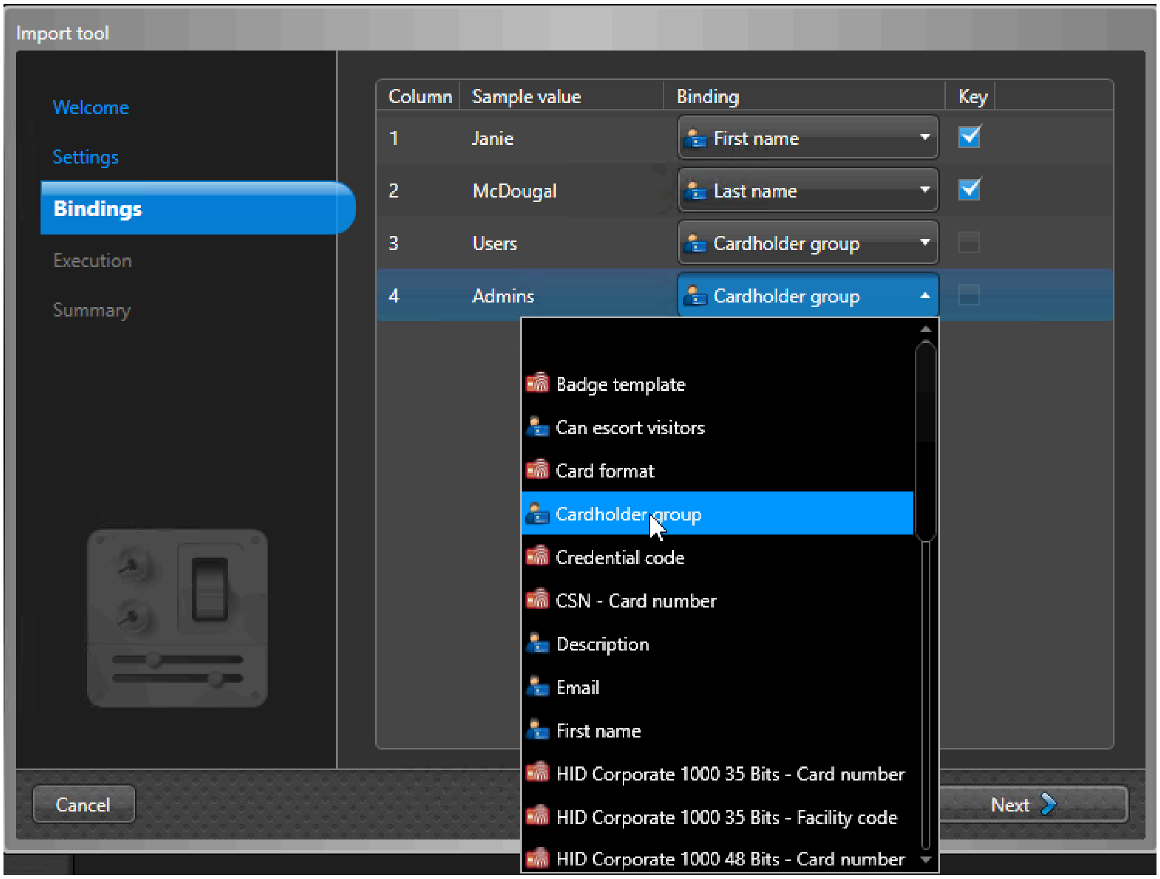
To replace a cardholder group:

1 From the Config Tool home page, click **Tools** > **Import tool**.

2 Enter the path to the CSV file you want to import, and click **Next**.

3 On the *Settings* page, from the **Cardholder group operation** list, select **Replace** and click **Next**.

4 On the *Bindings* page, set the new cardholder group columns to **Cardholder group**.



Column	Sample value	Binding	Key
1	Janie	First name	☑
2	McDougal	Last name	☑
3	Users	Cardholder group	□
4	Admins	Cardholder group	□

5 Click **Next**.

The Import tool updates the cardholder's group memberships to the new cardholder groups, and displays a summary.

6 (Optional) Click 📋 to copy and paste the contents of the report.

7 Click **Close**.

Database fields supported by the Import tool

Using the Import tool, you can import many database fields from a CSV file.

Field name	Field type	Description
👤 / 💳 **Activation date**	String	Strings in time and date format.
👤 / 💳 **Expiration date**	String	Strings in time and date format.
👤 / 💳 **Expires after X days of inactivity**	Unsigned integer	Number of days for an inactive credential or cardholder to expire.
👤 / 💳 **Expires X days after first use**	Unsigned integer	Number of days after first user for a credential or cardholder to expire.
💳 **Badge template**	String	Credential badge template.
💳 **Card format**	Unsigned integer or string	Credential card format. You can use one of the following values: • 0 = Standard 26 bits • 1 = HID H10306 34 Bits • 2 = HID H10302 37 Bits • 3 = HID H10304 37 Bits • 4 = HID Corporate 1000 35 Bits • 5 = HID Corporate 1000 48 Bits • CSN To specify a custom card format, you must spell it exactly as you created it. If no card format is specified in a CSV line, the default format specified on the import settings page is used.
💳 **{Format} - Field name**	Standard card format	You can specify a field in a specific card format, including custom card formats.
💳 **{Format} - Field name (previous value)**	Standard card format	Field of an old credential to replace. These “(previous value)” choices appear only if you selected *Replace* as *Credential operation*.
👤 **Cardholder <Field name>**	As defined by the custom field	Cardholder custom field.
👤 **Cardholder group**	String	Name of the cardholder group the cardholder should belong to. If the cardholder group does not exist, it is created in the same partition as the cardholder.

Field name	Field type	Description
CanEscort	Boolean	Valid inputs: • 0 • 1 • True • False • Yes • No • On • Off To specify a custom card format, you must spell it exactly as you created it. If no card format is specified in a CSV line, the default format specified on the import settings page is used.
Credential <Field name>	As defined by the custom field	Credential custom field.
Credential card data	String	The card data field allows the user to fill in the data for both standard and custom card formats. When this field is specified, the facility code and the card number fields are ignored. For all standard card formats, the string must contain the facility code followed by the card number. The accepted separators are the '/' and '|' characters. For example, "35/20508" corresponds to Facility code= 35 and Card number = 20508. For a custom card format, the data should be arranged according to the custom card format definition.
Description	String	Cardholder entity description.
Email	String	Cardholder email address.
First name	String	Cardholder first name. This field is part of the default cardholder key.
Last name	String	Cardholder last name. This field is part of the default cardholder key.
License plate	String	License plate reader. Valid length 1-32 digits.
Mobile phone number	String	Cardholder's mobile phone number.
Name	String	Credential entity name. If no name is specified, the default value "Imported credential" or "Unassigned imported credential" is used.
Partition	String	Name of the partition the cardholder should belong to. If the partition does not exist, it is created. If it is not specified, the cardholder is put in the system partition.

Field name	Field type	Description
🪪 **Partition**	String	Name of the partition the credential should belong to. If the partition does not exist, it is created. If it is not specified, the credential is put in the system partition.
👤 **Picture**	String	Path to a cardholder picture file (bmp, jpg, gif, or png). The path must reference a file located on the local machine or on the network.
🪪 **PIN**	String	Credential corresponding to a PIN. The maximum length is 15 digits.
👤 **Status**	Boolean	Cardholder status. The following values are accepted (not case-sensitive): • 1, True, Yes = Profile enabled • 0, False, No = Profile disabled
🪪 **Status**	String	Credential status. The following values are accepted (not case-sensitive): • Active • Inactive • Lost • Stolen • Expired

Related Topics

About partitions on page 423
CSV files and the Import tool on page 909
Creating custom card formats on page 884
Replacing credentials on page 916
How credential card formats work with Active Directory in Security Center on page 880

40

Testing your access control system

This section includes the following topics:

Access troubleshooter tool

The Access troubleshooter tool allows you to test and troubleshoot your access control system after it is set up, such as your access rules, and door and elevator configurations.

If you have a large system, you might have multiple schedules (Office hours/Office closed/Holidays/Weekends/Special events), multiple areas and sub-areas, multiple cardholder groups, and so on. As you build your system, and continue to create entities, the basic access logic applied at a door can become more difficult to determine.

You can use the Access troubleshooter to find out the following:

- Who is allowed to pass through an access point at a given date and time
- Which access points a cardholder is allowed to use at a given date and time
- Why a given cardholder can or cannot use an access point at a given date and time

The Access troubleshooter is most accurate when examining an event that just occurred. When using the troubleshooter to investigate a past event (for example, an access denied event), keep in mind that your settings might have changed since that event occurred. The troubleshooter does not take past settings into consideration. It only evaluates a situation based on the current settings.

Testing access rules at doors and elevators

You can find out who has the right to pass through a door side or elevator floor at a given date and time, using the *Access troubleshooter* tool.

What you should know

The door troubleshooter does not examine each cardholder’s credentials. You can further diagnose the cardholder’s access rights by clicking the *Access diagnosis* tab ().

To test the access rules at a door or elevator:

1 From the homepage, click **Tools** > **Access troubleshooter**.

2 In the *Access troubleshooter* dialog box, click the **Door troubleshooter** tab.

3 Select the date and time you want to the troubleshooter to base its evaluation on.

Only *access rules* are evaluated based on the specified date and time.

4 Select the access point that you want the troubleshooter to examine:

- If you select a door, specify a door side.
- If you select an elevator, specify a floor.

5 Click **Go**.

The active cardholders who have the rights to use the selected access point at the specified time, based on the current access rules, are listed.

Related Topics

Testing cardholder access rights based on credentials on page 928

Identifying who is granted access to doors and elevators

You can verify which cardholders are granted access to a particular door side or elevator floor at a specific date and time, using the *Door troubleshooter* report.

What you should know

This report is helpful, because it allows you to see what the configuration of a door or elevator is, and determine if their properties must be adjusted.The door troubleshooter does not examine each cardholder's credentials. You can further diagnose the cardholder's access rights using the *Access troubleshooter* tool.

To identify who is granted access to a door or elevator:

1. From the homepage, open the *Door troubleshooter* task.
2. In the *Filters* tab, select a date and time for the report.
3. Select a door or elevator you want to investigate.
4. From the **Access point** list, select the access point (door side or elevator floor) you want to verify.
5. Click **Generate report**.
   All cardholders who can go through the selected access point at the specified time are listed in the report pane.

After you finish

If necessary, test your access control configuration.

Related Topics

Testing access rules at doors and elevators on page 924
Creating doors on page 780
Creating elevators on page 787
Searching for entities on page 80

Report pane columns for the Door troubleshooter task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Door troubleshooter task.

- **Cardholder:** Cardholder entity name.
- **Custom fields:** Predefined custom fields for the entity. The columns only appear if custom fields are defined for the entity and were made visible to you when they were created or last configured.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.

Identifying who is granted or denied access at access points

You can find out which cardholders are currently granted or denied access to selected areas, doors, and elevators, using the *Cardholder access rights* report.

What you should know

This report is helpful because it shows you where a cardholder can go, and when, and determine if their access rule properties must be adjusted.

TIP: Perform your query on one access point at a time, so your report is more specific.

To identify who is granted or denied access at an access point:

1. From the homepage, open the *Cardholder access rights* task.
2. Set up query filters for your report. Choose one or more of the following filters:
   - **Doors - Areas - Elevators:** Restrict the search to activities that took place at certain doors, areas, and elevators.
   - **Cardholders:** Restrict the search to specific cardholders, cardholder groups, or visitors.
   - **Ignore access denied:** Turn on this filter to exclude cardholders and visitors who have only been denied access, and have not been granted access.
3. Click **Generate report**.

   The cardholders associated with the selected access point through an access rule are listed in the report pane. The results indicate if the cardholder is granted or denied access, and by which access rule.
4. To show a cardholder in a tile, double-click or drag a cardholder from the report pane to the canvas.
5. To view additional cardholder information in the tile, click ⓘ.

After you finish

If necessary, modify the cardholder's access rights.

Related Topics

Assigning access rules to cardholders on page 817

Report pane columns for the Cardholder access rights task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Cardholder access rights task.

- **Cardholder:** Cardholder entity name.
- **First name:** Cardholder or visitor’s first name.
- **Last name:** Cardholder or visitor’s last name.
- **Picture:** Cardholder or visitor’s picture.
- **Member of:** All groups the cardholder belongs to.
- **Granted access by:** Access rules granting the cardholder access to at least one of the selected entities (area, door, etc.).
- **Denied access by:** Access rules denying access to at least one of the selected entities to the cardholder.
- **Access to:** The access points that the cardholder or visitor has access to.
- **Activation:** (Temporary access rule only) Access rule activation time.

- **Expiration:** (Temporary access rule only) Access rule expiration date and time.
- **Custom fields:** Predefined custom fields for the entity. The columns only appear if custom fields are defined for the entity and were made visible to you when they were created or last configured.

Testing cardholder access rights

You can find out which access points a cardholder is allowed to use at a given date and time, using the *Cardholder troubleshooter* tab in the Access troubleshooter tool.

What you should know

The cardholder troubleshooter does not examine each cardholder's credentials. You can further diagnose the cardholder's access rights by clicking the *Access diagnosis* tab ().

To troubleshoot a cardholder's access rights:

1 From the homepage, click **Tools** > **Access troubleshooter**.

2 In the *Access troubleshooter* dialog box, click the **Cardholder troubleshooter** tab.

3 Select the date and time you want to the troubleshooter to base its evaluation on. Only *access rules* are evaluated based on the specified date and time.

4 Select the cardholder that you want the troubleshooter to examine. Instead of a cardholder, you can also select a *credential* or a visitor.

The entities that are currently inactive are greyed out.

5 Click **Go**.

The access points that the selected cardholder (or visitor) has the right to use at the specified time, based on the current access rules, are listed.

Testing cardholder access rights based on credentials

You can diagnose why a cardholder with a given credential can, or cannot access a given door or elevator, at a given date and time, using the *Access troubleshooter* tab in the Access troubleshooter tool.

To test a cardholder's access rights based on their credential:

1 From the homepage, click **Tools** > **Access troubleshooter**.

2 In the *Access troubleshooter* dialog box, click the **Access diagnosis** () tab.

3 Select the date and time you want to the troubleshooter to base its evaluation on.

4 Select the cardholder you want to examine. Instead of a cardholder, you can also select a credential or a visitor.

5 If the selected cardholder has more than one credential, specify the one you want to examine.

6 Select an access point to examine.

- If you select a door, specify a door side.
- If you select an elevator, specify a floor.

7 Click **Go**.

The troubleshooter produces a diagnosis based on the current system configuration, taking into consideration the access rules, and both the cardholder's and the credential's activation and expiration dates.

Viewing credential properties of cardholders

You can view credential properties (status, assigned cardholder, card format, credential code, custom properties, and so on) of cardholders, using the *Credential configuration* report.

What you should know

For example, the *Credential configuration* report is helpful if you requested a credential for a cardholder, and want to see if it was activated. If you search by cardholder, the *Credential status* column indicates whether the credential is in the *Requested* or *Active* state. You can also search if there are any credentials currently listed as lost or stolen.

To view the credential properties of a cardholder:

1. Open the *Credential configuration* task.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **Unused credentials:** Search for credentials that have not produced an *access granted* event within a certain time range.

     NOTE: For the report to generate results, all Access Manager roles must be active and online.
   - **Credential:** Specify whether or not the credential is assigned.
   - **Cardholders:** Restrict the search to specific cardholders, cardholder groups, or visitors.
   - **Credential information:** Restrict the search to specific card formats, facility codes, card numbers, or license plates.
   - **Status:** The status of the cardholder or visitor’s profile: *Active*, *Expired*, *Inactive*, *Lost*, *Stolen*.
3. Click **Generate report**.

   The credential properties the selected cardholder are listed in the report pane.
4. To show a cardholder in a tile, double-click or drag a cardholder from the report pane to the canvas.
5. To view additional cardholder information in the tile, click ⓘ.

Report pane columns for the Credential configuration task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Credential configuration task.

- **Credential:** Credential name used by the cardholder.
- **Card format:** Credential card format.
- **Credential code:** Facility code and card number.
- **Credential status:** The status of the cardholder or visitor’s credential: Active; Inactive.
- **Email address:** Cardholder or visitor’s email address.
- **Mobile phone number:** Cardholder or visitor's mobile phone number.
- **Last access grant:** Time the cardholder entered the area.
- **Cardholder status:** The cardholder’s profile status.
- **Cardholder:** Cardholder entity name.
- **First name:** Cardholder or visitor’s first name.
- **Last name:** Cardholder or visitor’s last name.
- **Picture:** Cardholder or visitor’s picture.
- **Cardholder activation date:** Date and time that the cardholder profile activates.
- **Cardholder expiration date:** Date and time that the cardholder profile expires.
- **Credential activation date:** Date and time that the cardholder’s credential was activated.
- **Credential expiration date:** Date and time that the cardholder’s credential expires.

- **Description:** Description of the event, activity, entity, or incident.

  IMPORTANT: To comply with State laws, if the **Report generated** option is used for an Activity trails report that contains ALPR data, the reason for the ALPR search is included in the **Description** field.
- **PIN:** Credential PIN.
- **Role:** Role type that manages the selected entity.
- **Custom fields:** Predefined custom fields for the entity. The columns only appear if custom fields are defined for the entity and were made visible to you when they were created or last configured.

Viewing properties of cardholder group members

You can find out the members of a cardholder group, and view any associated cardholder properties (first name, last name, picture, status, custom properties, and so on), using the *Cardholder configuration* task.

What you should know

You can search for a specific cardholder group to see which cardholders are members of that group. You also can search for expired or inactive cardholders to see if there are any in your system.

To view the properties of cardholder group members:

1. From the home page, open the *Cardholder configuration* task.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **Activation date:** Specify a time range during which the cardholder profile activates.
   - **Expiration date:** Specify a time range during which the cardholder or visitor profile expires.
   - **Unused cardholders:** Search for cardholder or visitors for whom no assigned credentials have produced an *access granted* event within a certain time range.

     NOTE: For the report to generate results, all Access Manager roles must be active and online.
   - **Status:** The status of the cardholder or visitor’s profile: *Active*, *Expired*, or *Inactive*.
   - **First name:** Cardholder or visitor’s first name.
   - **Last name:** Cardholder or visitor’s last name.
   - **Email address:** Cardholder or visitor’s email address.
   - **Mobile phone number:** Cardholder or visitor's mobile phone number.
   - **Description:** Restrict the search to entries that contain this text string.
   - **Picture:** Whether or not the cardholder or visitor has a picture assigned.
   - **Partition:** Partition that the entity is a member of.
   - **Cardholder groups:** Restrict the search to specific cardholder groups.
   - **Credential:** Whether or not the cardholder or visitor has a credential assigned.
   - **Credential name:** Credential's name.
   - **Credential status:** The status of the cardholder or visitor’s credential: Active; Expired; Inactive; Lost; Stolen. Not all statuses are available for every task.
   - **Credential information:** Restrict the search to specific card formats, facility codes, card numbers, or license plates.
   - **Custom fields:** Restrict the search to a predefined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
   - **Can escort visitors:** Indicates whether or not the cardholder can act as a visitor host (can be switched on or off).
3. Click **Generate report**.

   The cardholders that are members of the selected cardholder groups are listed in the report pane.
4. To show a cardholder in a tile, double-click or drag a cardholder from the report pane to the canvas.
5. To view additional cardholder information in the tile, click ⓘ.

Report pane columns for the Cardholder configuration task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Cardholder configuration task.

- **Cardholder:** Cardholder or visitor entity name.

- **First name:** Cardholder or visitor’s first name.
- **Last name:** Cardholder or visitor’s last name.
- **Picture:** Cardholder or visitor’s picture.
- **Cardholder status:** The cardholder’s profile status.
- **Cardholder groups:** Cardholder groups that the cardholder or visitor belongs to.
- **Email address:** Cardholder or visitor’s email address.
- **Mobile phone number:** Cardholder or visitor's mobile phone number.
- **Last access time:** Time of the last access event involving the cardholder, visitor, or credential.
- **Last access location:** Location of the last access event involving the cardholder, visitor, or credential.
- **Last access decision:** Result of the last access event involving the cardholder, visitor, or credential.
- **Can escort visitors:** Indicates whether or not the cardholder can act as a visitor host (can be switched on or off).
- **Security clearance:** The cardholder’s security clearance level.
- **Activation date:** Date and time that the cardholder profile activates.
- **Description:** Description of the cardholder or visitor.
- **Expiration date:** Date and time that the cardholder profile expires.
- **Role:** Role type that manages the selected entity.
- **Custom fields:** Predefined custom fields for the entity. The columns only appear if custom fields are defined for the entity and were made visible to you when they were created or last configured.

Identifying which entities are affected by access rules

You can find out which entities and access points are affected by a given access rule, using the *Access rule configuration* report.

What you should know

In the report results, you can see the members of the access rule, such as the cardholders, doors, and the associated schedule. This helps you determine if you must add or remove entities, or adjust the schedule.

To identify which entities are affected by an access rule:

1. From the homepage, open the *Access rule configuration* task.
2. Set up the query filters for your report. Choose one or more of the following:
   - **Access rule:** Select the access rule to investigate.
   - **Cardholder status:** Select the cardholder status to investigate: Active; Expired; Inactive.
   - **Expand cardholder groups:** Turn on to list the members of the affected cardholder groups in the report instead of the cardholder groups themselves.
   - **Include perimeter entities:** Turn on to include the perimeter entities of the affected areas in the report.
   - **Type:** Select the entities to investigate: area, cardholder, cardholder group, door, elevator, schedule, visitor.
3. Click **Generate report**.

   The entities and access points affected by this access rule are listed in the report pane.

Related Topics

Creating access rules on page 807

Report pane columns for the Access rule configuration task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the *Access rule configuration* task.

- **Access rules:** Name of the access rules.
- **Activation:** (Temporary access rule only) Access rule activation time.
- **Expiration:** (Temporary access rule only) Access rule expiration date and time.
- **Member:** Name of the affected entity.
- **Access point:** Access point involved (only applicable to areas, doors, and elevators).
- **Type:** Affected entity type.
- **Cardholder status:** The cardholder or visitor’s profile status.
- **Email address:** Cardholder or visitor’s email address.
- **Custom fields:** Predefined custom fields for the entity. The columns only appear if custom fields are defined for the entity and were made visible to you when they were created or last configured.

Viewing I/O configuration of access control units

You can view the I/O configurations (controlled access points, doors, and elevators) of access control units, using the *I/O configuration* report.

What you should know

For example, you can use the *I/O configuration* report to search for a specific door, and see how the access through each door side is configured (REX, readers, I/O modules, and so on).

To view the I/O configuration of an access control unit:

1. Open the *I/O configuration* task.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **Access point:** Restrict the search to specific access points (input, output, and reader).
   - **Devices:** Select the devices to investigate.
   - **Location:** Specify the areas where the devices are located.
3. Click **Generate report**.

   The input and output configurations of the selected access control units are listed in the report pane.

Related Topics

Viewing unit properties on page 229

Report pane columns for the I/O configuration task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the I/O configuration task.

- **Access point:** Access point involved (only applicable to areas, doors, and elevators).
- **Access Manager:** Access Manager controlling the unit.
- **Controlling:** Door controlled by the device.
- **Custom fields:** Predefined custom fields for the entity. The columns only appear if custom fields are defined for the entity and were made visible to you when they were created or last configured.
- **Device:** Device involved on the unit (reader, REX input, I/O module, strike relay, and so on).
- **IP address:** IP address of the unit or computer.

  NOTE: The IP address is not shown for units enrolled with the hostname and units that belong to an ACaaS system.
- **Manufacturer:** Manufacturer of the unit.
- **Physical name:** Device name.
- **Unit:** Name of the unit.
- **Unit type:** Type of unit (Access control, ALPR, Intrusion detection, or Video).

41

Troubleshooting access control

This section includes the following topics:

Viewing access control health events

You can view events related to the health of the access control entities in your system, using the *Access control health history* report.

What you should know

The *Access control health history* report only lists events for access control units, areas, doors, elevators, and zones. Unlike the events in the *Health history* report, the events in the *Access control health history* report are not generated by the Health Monitor role, identified by an event number, or categorized by severity.

To search for access control health events:

1. Open the *Access control health history* task.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **Sources:** Source entity of the event.
   - **Event timestamp:** Define the time range for the query. You can define the time range for a specific period or a relative period, such as the previous week or the previous month.
3. Click **Generate report**.

   The access control events are listed in the report pane.

Report pane columns for the Access control health history task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the *Access control health history* task.

- **Source:** Source entity of the event.
- **Event:** Event name.
- **Unit:** Name of the unit.
- **Product type:** Model of the unit.
- **Event timestamp:** Date and time that the event occurred.
- **IP address:** IP address of the unit or computer.

  NOTE: The IP address is not shown for units enrolled with the hostname and units that belong to an ACaaS system.
- **Firmware version:** Firmware version installed on the unit.
- **Time zone:** Time zone of the unit.
- **Device:** Device involved on the unit (reader, REX input, I/O module, strike relay, and so on).
- **Description:** Reports the reason for a failed firmware upgrade.
- **Custom fields:** Predefined custom fields for the entity. The columns only appear if custom fields are defined for the entity and were made visible to you when they were created or last configured.

Investigating events related to access control units

You can investigate events related to access control units, using the *Access control unit events* report.

What you should know

For example, you can use the *Access control unit events* report to see if any critical events relating to access control units occurred in the last week by searching for the specific event and setting the time range.

To investigate access control unit events:

1. From the homepage, open the *Access control unit events* task.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **Access control units:** Select the access control units to investigate.
   - **Event timestamp:** Define the time range for the query. You can define the time range for a specific period or a relative period, such as the previous week or the previous month.
   - **Events:** Select the events of interest. The available event types depend on the task you are using.
3. Click **Generate report**.

   The access control unit events are listed in the report pane.

   IMPORTANT: You get an error message for each Access Manager role that is offline when you run the query, even for roles unrelated to the selected access control units. This happens because the system cannot determine whether an offline Access Manager role managed any of the selected access control units in the past.

Report pane columns for the Access control unit events task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the *Access control unit events* task.

- **Event timestamp:** Date and time that the event occurred.
- **Unit:** Name of the unit.
- **Event:** Event name.
- **Tamper:** Name of the interface module that has been tampered with.
- **Description:** Reports the reason for a failed firmware upgrade.
- **Insertion timestamp:** Date and time that the event was saved in the Access Manager database. This timestamp can differ from the event timestamp if a unit was offline while the event occurred because the event is only saved in the Access Manager after the unit comes back online.
- **Occurrence period:** Period when the event occurred.
- **Product type:** Model of the unit.
- **Custom fields:** Predefined custom fields for the entity. The columns only appear if custom fields are defined for the entity and were made visible to you when they were created or last configured.

Moving access control units to a different Access Manager

If you want a different Access Manager role to manage and control an access control unit, for load distribution or another purpose, you can move the unit to another Access Manager using the Move unit tool.

Before you begin

- Make sure that the Access Manager role is on the same LAN as the access control unit it controls.
- Create the extension for the unit.

What you should know

To move access control units from one hosted SaaS Access Manager role to another hosted SaaS Access Manager role, you must contact our Technical Assistance personnel.

To move an access control unit to a different Access Manager:

1. From the homepage, click **Tools** > **Move unit**.
2. From the **Unit type** list, select **Access control unit**.
3. Under **Access control unit**, select the units you want to move.
4. Under **Access Manager**, select the new Access Manager role to control the unit.
5. Click **Move** > **Close**.

Moving Mercury and Honeywell controllers to different Synergis units

If you want a different Synergis™ unit to manage your Mercury and Honeywell controllers, you can move the controllers in Config Tool, using the **Move to a different unit** button, instead of deleting and re-adding them.

What you should know

Moving controllers from one Synergis unit to another can be useful in staging scenarios where you have enrolled controllers under one unit, and then want to move them to another unit after it is set up.

- The Synergis units can be under different Access Manager roles.
- The Access Manager roles, Synergis units, and controllers can be offline.

To move a controller to a different Synergis unit:

1. From the homepage, open the *Access control* task, and click the **Roles and units** view.
2. In the entity tree, expand the Access Manager, and click the access control unit of the controller.
3. Click the **Peripherals** tab, and select the controller you want to move.
4. Click **Move to a different unit** ().

   The *Select destination unit* dialog box opens.
5. Click the access control unit you want the controller moved to, and then click **OK**.

The controller and all its child entities are moved under the selected Synergis unit.

Preparing to replace an access control unit

Before you replace an access control unit with a new one, there are steps you must perform.

Before you begin

You can only replace an access control unit with a new one if the two are of the same brand and model. The exception to this rule is if you are replacing an HID VertX V1000 unit with a Synergis™ unit. In every case, the same interface modules (brand and model) must be connected to the new unit. If there is any difference other than the mentioned exception, the unit replacement will not be accepted.

What you should know

For more information about Synergis™ Cloud Link configuration, see the following guides, depending on your unit:

- For Synergis Cloud Link units, see the *Synergis™ Cloud Link Administrator Guide*.
- For legacy Synergis Cloud Link units, see the *Synergis™ Appliance Configuration Guide*.

To prepare to replace an access control unit:

1 Back up the Directory database from Server Admin.

2 For Synergis units, back up the unit configuration files.

NOTE: If the Synergis unit is no longer reachable, and you do not have a backup file, then some configuration must be manually done on the new unit to match the old one.

3 Physically disconnect the old unit and make sure it is offline in Security Center ().

4 Physically install the new unit:

- For Synergis Cloud Link units, see the *Synergis™ Cloud Link Hardware Installation Guide*.
- For legacy Synergis Cloud Link units, see the *Synergis™ Cloud Link Appliance Hardware Installation Guide*.
- Install the HID unit.

5 For RS-485 integrations, physically disconnect the RS-485 interface modules from the old unit and connect them to the new unit using the same channels.

IMPORTANT: Do not change the physical addresses of the interface modules.

6 For Synergis units, restore the old unit's configuration files on the new unit.

The admin password, network settings and Synergis key store are not restored.

7 Add the new unit in Security Center:

- Add the Synergis unit.

  NOTE: If you want to use the IP address of the old unit on the new unit, you must first configure the old unit to use an unused IP address. This is configured on the unit's *Properties* page in Config Tool.
- Add the HID unit.

After you finish

Replace the old unit with the new one.

Replacing access control units

If an access control unit fails, you can replace it with a new, compatible unit. This process copies over the configuration settings; associations to doors, elevators, and zones; and event logs to the new unit.

Before you begin

Prepare to replace your access control unit.

NOTE: If the old Synergis™ unit is no longer reachable, and you did not back up the unit configuration, then you must add the hardware that was on the old unit to the new unit before replacing the unit. This is not required for the Mercury or Honeywell controller integrations.

What you should know

Replacing your access control unit requires that you temporarily deactivate the Access Manager role.

To replace an access control unit:

1 Temporarily deactivate the Access Manager role.

  a) From the Config Tool home page, open the *Access control* task, and click the **Roles and units** view.

  b) Right-click the Access Manager role, and click **Maintenance** > **Deactivate role** ( ).

  c) In the confirmation dialog box that opens, click **Continue**.

  The Access Manager and all the access control units controlled by the role turn red.

2 Click the home page, click **Tools** > **Unit replacement**.

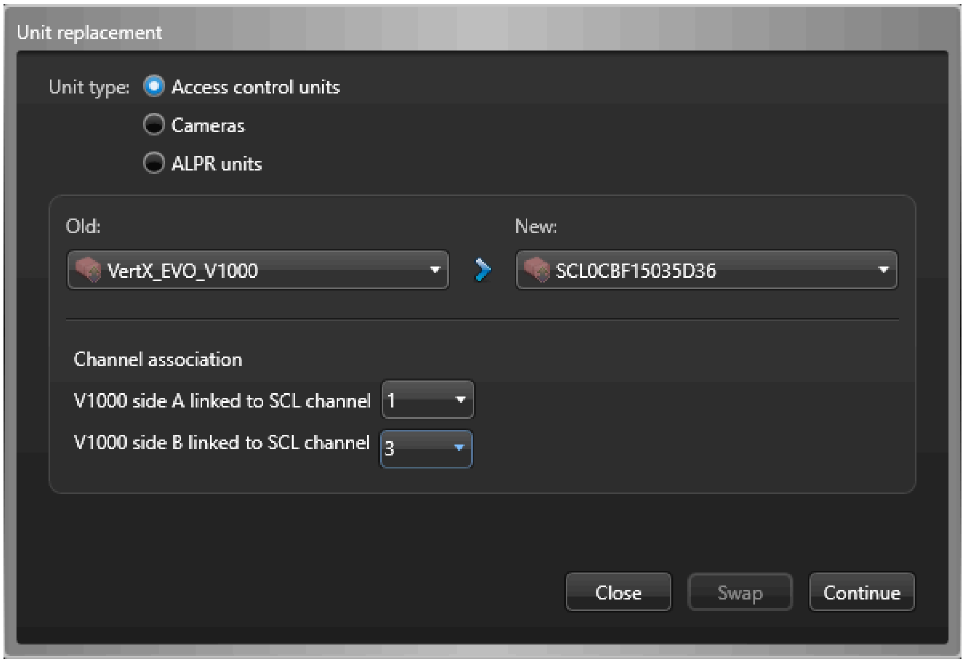
  The *Unit replacement* dialog box opens.

3 In the **Unit type** option, select **Access control units**.

4 Select the **Old** and the **New** access control units.

5 Click **Swap**.

  For V1000 to Synergis replacements, if the V1000 had subpanels (interface modules) using the same physical address, link the V1000 sides to the Synergis unit channels, and click **Continue**.



Unit replacement

Unit type: ● Access control units ○ Cameras ○ ALPR units

Old: VertX_EVO_V1000

New: SCL0CBF15035D36

Channel association

V1000 side A linked to SCL channel 1

V1000 side B linked to SCL channel 3

The configuration settings of the old access control unit are copied to the new one.

6. Reactivate the Access Manager role:
   a) Open the *Access control* task, right-click the Access Manager role, and click **Maintenance** > **Activate role** ( ).
7. In the area view, select the new unit, and verify that the configuration settings are correct.
8. Verify that all doors controlled by the new unit are operating properly.
9. Right-click the old unit, and click **Delete** (✖).
10. In the confirmation dialog box that opens, click **Continue**.

After you finish

If the old Synergis unit is no longer reachable, and you did not back up the unit configuration, then you must configure the following on the new unit to match the old one:

- Supervised input resistor values
  NOTE: This is not required for the Mercury or Honeywell controller integrations.
- Primitive rules

Related Topics

Searching for entities using the search tool on page 80

Upgrading access control unit firmware and platform, and interface module firmware

You can upgrade the firmware and platform of one or more access control units, or the firmware of one or more interface modules directly from Config Tool.

Before you begin

Upgrading your access control unit or interface module requires the following:

- For downstream devices, ensure that the device can be upgraded in Config Tool, according to the Synergis™ Softwire version running on the Synergis™ Cloud Link unit. See "Downstream devices supported for upgrade in Security Center" in the *Synergis™ Softwire Release Notes*.
- For HID EVO, verify the upgrade path for the unit you want to upgrade.
- Ensure that Power over Ethernet (PoE) units have battery backup if there is a power failure during the upgrade process.
- Download a supported firmware version or cumulative security rollup for the unit from GTAP.

  For HID EVO firmware download links, see HID firmware upgrade procedure for EVO units on the Genetec™ TechDoc Hub.
- For HID EVO units, ensure that the Admin password is set in Config Tool under the unit's properties.

What you should know

- You cannot upgrade to the same or an older version.
- Schedule upgrades outside of core business hours.

  IMPORTANT: Upgrading the platform can cause 30 - 60 minutes of downtime. During that time, the unit might reboot twice to complete the installation of the cumulative security rollup.
- The system can upgrade up to 10 units concurrently. If more than 10 units are selected for upgrade, the excess units are queued.
- You cannot cancel an upgrade in progress. You can only cancel an upgrade if the unit's *upgrade status* in the *Hardware inventory* report is *scheduled*.
- Doors assigned to the access control unit being upgraded do not function during a firmware or cumulative security rollup upgrade.

The following conditions must be met for the **Upgrade** button to be displayed:

- The interface modules are supported for upgrade in Config Tool. This requires Synergis Softwire 11.1 or later, depending on the interface module you want to upgrade.
- All the units or interface modules you want to upgrade are of the same product type.

  NOTE: The AXIS A1210 Powered by Genetec and AXIS A1610 Powered by Genetec units do not share the same platform upgrade packages, therefore, cannot be upgraded together.
- None of the units are Streamvault™ appliances.
- None of the units have a scheduled firmware upgrade pending.
- None of the units are federated.
- You have the *Upgrade access control units* and the *Unit enrollment* user privileges.
- The Access Manager role is not in backward compatibility mode.

To upgrade the access control unit or interface module:

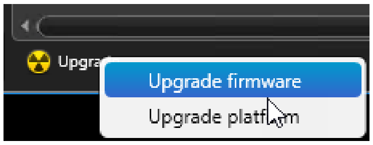
1 In Config Tool, generate a hardware inventory report for the units or interface modules you want to upgrade.

2 Select the units or interface modules that you want to upgrade.

The **Proposed firmware version** field displays the recommended firmware version. If the firmware version is the same as the proposed version, it displays *Up to date*.

3 For Legacy Synergis Cloud Link units, click **Upgrade** (☢), and select one of the following:

- To upgrade the firmware, select **Upgrade firmware**.
- To install a cumulative security rollup, select **Upgrade platform**.

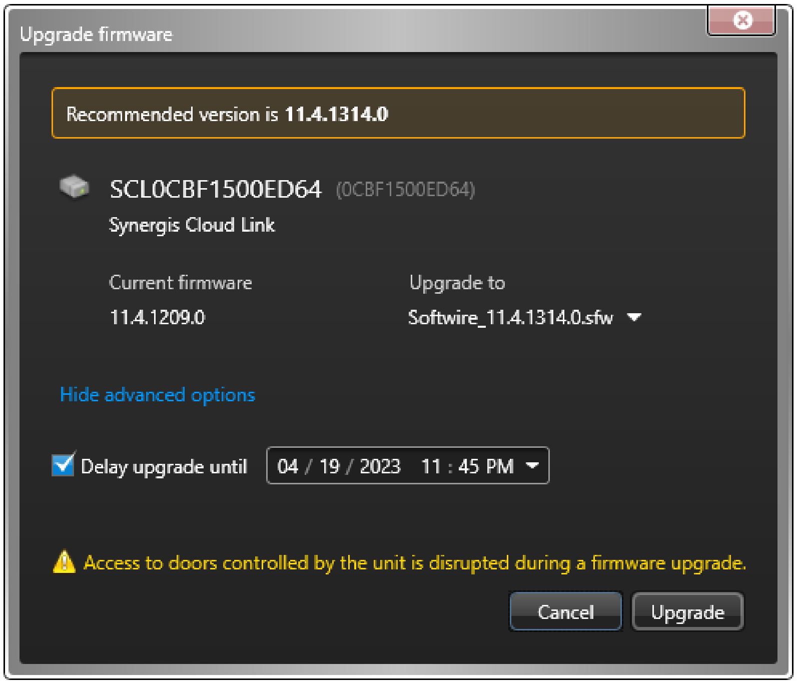


4 For all other device types, click **Upgrade** (☢).

5 In the upgrade dialog box that opens, click the browse button, select the firmware or cumulative security rollup file that you downloaded from GTAP, and click **Open**.

6 (Optional) To delay the upgrade, click **Advanced options**, and select **Delay upgrade until**, and enter the upgrade date and time.

The following screenshot is only an example. The actual dialog box might look different depending on the type of device you selected.



Upgrade firmware

Recommended version is **11.4.1314.0**

SCL0CBF1500ED64 (0CBF1500ED64)

Synergis Cloud Link

Current firmware: 11.4.1209.0

Upgrade to: Softwire_11.4.1314.0.sfw

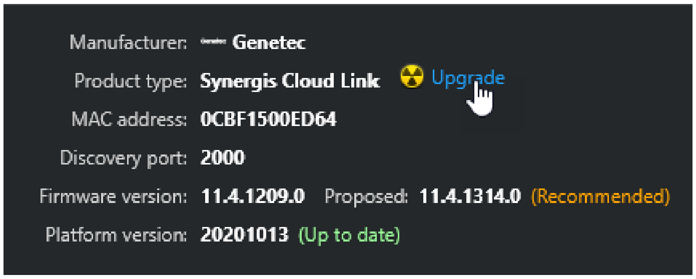
Hide advanced options

☑ Delay upgrade until 04 / 19 / 2023 11 : 45 PM

⚠ Access to doors controlled by the unit is disrupted during a firmware upgrade.

7 Click **Upgrade**.

NOTE: Individual access control units can also be upgraded in the *Access control* task in Config Tool from the unit's *Identity* page in the **Roles and units** view.



Manufacturer: Genetec
Product type: Synergis Cloud Link
MAC address: 0CBF1500ED64
Discovery port: 2000
Firmware version: 11.4.1209.0 Proposed: 11.4.1314.0 (Recommended)
Platform version: 20201013 (Up to date)

The system upgrades the access control units or interface modules' firmware or platform version, and then the units and interface modules restart.

After you finish

- When the units or interface modules return online, generate another *Hardware inventory* report in Config Tool and confirm the firmware or platform version displayed.
- Verify that all doors controlled by the upgraded units or interface modules operate properly.

Supported HID EVO firmware upgrade paths

It is important to know which firmware versions can be upgraded directly to the latest releases, and which require more steps.

To upgrade HID EVO units from an earlier firmware version (2.3.1.603 or 2.3.1.605 for Edge EVO, and 2.3.1.542 or 2.3.1.673 for VertX EVO) to the recommended firmware version, specific upgrade paths must be followed:

- HID Edge EVO: (EH400, EH400-K)

  Supported upgrade path: 2.3.1.603 or 2.3.1.605 → 2.3.1.841 → any later version
- HID Vertx EVO: (V1000, V2000)

  Supported upgrade path: 2.3.1.542 or 2.3.1.673 → 2.3.1.791 → any later version

  CAUTION: Upgrading directly from the earlier firmware to the recommended firmware will cause irreparable damage to your unit. Moreover, you cannot downgrade the firmware after it has been upgraded to 2.3.1.841 on Edge EVO or to 2.3.1.791 on VertX EVO.

Enabling or disabling support logs for access control units

The Synergis™ appliance can keep detailed logs for troubleshooting and support. You can manually enable or disable support logs if requested by Genetec™ Technical Assistance Center.

What you should know

You can enable or disable support logs for multiple units simultaneously in Security Center using the following instructions. You can also enable support logs for individual units in the Synergis™ Appliance Portal. For more information on configuring event logging options in the Synergis™ Appliance Portal, refer to the *Synergis™ Appliance Configuration Guide*.

To enable or disable support logs for access control units:

1 In Config Tool, open the *Access control* task and select the *Roles and units* view.

2 Under the Access Manager, select one or more access control units.

NOTE: Clicking the Access Manager selects all control units enrolled under it.

3 From the right-click menu, or on the contextual command bar at the bottom of the screen, click **Maintenance**, and select **Enable unit support logs** or **Disable unit support logs**.

Troubleshooting: HID unit discovery and enrollment issues

If you cannot discover or enroll an HID access control unit, there are some common troubleshooting steps you can use to try and resolve the issues.

To troubleshoot why an HID unit cannot be discovered or enrolled:

1 Make sure that the computers Config Tool and Access Manager are running on are behind a firewall.

2 Make sure that all Synergis™-specific ports are opened and unblocked.

3 Make sure the HID VertX extension has been added to the Access Manager in Config Tool.

4 Validate that the HID VertX extension is properly loaded in the Access Manager, as follows:

a) To open a console session to the Access Manager, open a web browser, and go to the URL http://(server name or IP)/Genetec/console.

NOTE: If you cannot connect to the console ensure that console access is enabled in the *Server Admin* , under the **Genetec™ Server** tab.

b) Click the **Commands** tab at the top of the page.

c) Under the column **User Commands** on the left, expand **Access Manager** and click **Status**.

d) A status query is sent to the Access Manager and the response contains the extensions that are loaded.

e) Ensure that the following line is shown in the status results: **HID VertX:4070 =** X **units**.

5 Check if the unit has a static IP address.

6 If the unit's IP address is static, you must set the DNS, or the unit might have issues enrolling or connecting.

a) To access the HID Configuration GUI, enter the unit's IP address in a web browser.

b) In the HID Configuration GUI, set the primary and secondary DNS to the appropriate values.

If you do not know your network's DNS, set the unit's own IP address as the primary and secondary DNS server.

7 Make sure there are no other applications blocking the ports needed by the HID units:

a) Stop the Access Manager.

b) In Windows, click **Start** > **Run**, and type **cmd** to open the Command Prompt, and then run **netstat -na**.

Troubleshooting: HID units cannot be discovered

If you cannot discover an HID access control unit using the *Unit enrollment* tool, you can troubleshoot the cause of the issue.

Before you begin

Perform the common troubleshooting steps for resolving HID discovery and enrollment issues.

To troubleshoot why an HID unit cannot be discovered:

1 In the Advanced Setup of HID VertX web page, make sure the Host Name is set, and that is does not have more than 15 characters.

The Host Name must be set, and it must have less than 15 characters to be discovered.

2 Make sure the unit is on the same network subnet as the computer where Config Tool is running.

Discovery only works within the same *broadcast* domain.

3 Make sure the unit firmware is up to date.

For a list of supported firmware versions, see the *Security Center Release Notes*.

Troubleshooting: HID units cannot be enrolled

If you cannot enroll an HID access control unit, you can troubleshoot the cause of the issue.

Before you begin

Perform the common troubleshooting steps for resolving HID discovery and enrollment issues.

What you should know

If you are experiencing enrollment issues, the following can occur:

- Unit cannot be enrolled
- Unit is enrolled but its icon remains red
- Unit connects and disconnects continuously
- Unit begins enrolling and fails at 67%

To troubleshoot why an HID unit cannot be enrolled:

1 Check if there is connectivity to the unit, as follows:

  a) Ping the unit from the computer running the Access Manager: In Windows, click **Start** > **Run**, and type **cmd** to open the Command Prompt, and then run **ping w.x.y.z**.

  NOTE: w.x.y.z is the IP address of the unit.

  A report is generated. Make sure no packets were lost.

  b) Telnet the unit from the computer running the Access Manager to check its credentials: In Windows, click **Start** > **Run**, and type **cmd** to open the Command Prompt, and then run **telnet w.x.y.z**.

  c) Log onto the unit.

  The default username and password pair is root/pass.

  If the logon is successful, there is connectivity to the unit.

2 Check if the unit is on the same network subnet as the computer where the Access Manager is running.

  If it is not, you can enroll the unit manuallyyou can enroll the unit manually as long as you know its IP address (the unit must be set to use a static IP address).

3 Make sure the unit firmware and the interface board firmware is up to date.

  For a list of supported firmware versions, see the *Security Center Release Notes* Security Center Release Notes.

4 Make sure the network card binding and database configuration for the Access Manager is set correctly.

5 If the Access Manager is behind a NAT, you must specify the translated host address for the Access Manager.

6 Make sure no other Access Manager is connected to the HID unit, as follows:

  a) Stop your Access Manager.

  b) Telnet the unit: In Windows, click **Start** > **Run**, and type **cmd** to open the Command Prompt, and then run **telnet w.x.y.z**.

  c) Log onto the unit.

  The default username and password pair is root/pass.

  d) At the prompt, type **netstat -na**.

  A list of network connections appears. Ensure that the port used by the HID unit is open.

7 Make sure the HID units (and connected interfaces) are wired to not generate tamper or door held open alarms, access granted or access denied events.

  Tamper and door held open alarms trigger repeatedly. Upon connection, any such alarms and events have to be downloaded from the unit which can slow-down the enrollment process. Symptoms of this is the unit is difficult to enroll, the unit connects and disconnects, or the unit beeps.

8. Upgrade the unit’s firmware.

   For a list of supported firmware versions, see the *Security Center Release Notes*.

Troubleshooting: Too many request to exit door events

If the logs for a door show far too many request to exit events for the actual amount of door activity, you can try to reduce the number of false request to exit events from the options in the door *Properties* tab.

What you should know

If your door is equipped with an automatic request to exit device (based on a *motion detection* sensor), sometimes a *request to exit* event is triggered when people are entering an area. Depending on the quality of the automatic request to exit device and how it is installed, the device might trigger on any activity near the door.

To reduce the number of request to exit door events:

1. From the Config Tool home page, open the *Area view* task.
2. Select the door that is causing the issues, and click the **Properties** tab.
3. Set the following **Request to exit** options as necessary:
   - **Time to ignore 'Request to exit' after granted access:** Ignore any requests to exits for this long after access has been granted.
   - **Unlock on request to exit:** Set to **ON** if a REX is being used, and you want to automatically grant the request to exit.
   - **Ignore 'Request to exit' events while door is open:** Do not generate REX when door is open.
   - **Time to ignore 'Request to exit' after door closure:** Once the door has closed, wait this long before generating any more *Request to exit* events.
4. Click **Apply**.

Troubleshooting: Credentials not working

If a credential does not work at a door or elevator, you can test the reason why access is denied.

What you should know

For a credential to be granted access at a given *door side* or elevator floor, the following conditions must be met:

- The credential's profile must be enabled
- The credential must be associated to a cardholder
- The cardholder's profile must be enabled
- There must be at least one *access rule* that specifically grants access for that cardholder or the cardholder's cardholder group.

If these settings are not correct, access is denied.

To troubleshoot why access is denied:

- Use the Access troubleshooter tool to determine why the cardholder does not have access to a door or elevator.

Troubleshooting: Cards not working at readers

If a card is not working at a door reader, you can troubleshoot the cause of this issue.

To troubleshoot why a credential is not working at a card reader:

1. Make sure you are using the right type of card technology for the reader.

   For example, some readers are multi-technology (can read 125 kHz and 13.56 MHz cards), and other readers can only read one card type.
2. Test if the card is defective by trying another card.
3. Test if the reader is installed too close to another reader by disconnecting the power to one reader.

   If the other reader starts to operate correctly, they were installed too closely. Readers emit an electromagnetic field that can interfere with other readers located nearby.
4. Test if your are using the proper cable for the reader by connecting a spare reader directly to the unit with a short cable.

   If the spare reader works, you should change the cable of the original reader. For the maximum cable length and type, see the reader and unit documentation.

Part VI

License plate recognition

This part includes the following chapters:

42

ALPR at a glance

This section includes the following topics:

About Security Center AutoVu

The AutoVu™ automatic license plate recognition (ALPR) system automates license plate reading and identification, making it easier for law enforcement and for municipal and commercial organizations to locate vehicles of interest and enforce parking restrictions. Designed for both fixed and mobile installations, the AutoVu™ system is ideal for a variety of applications and entities, including law enforcement, municipal, and commercial organizations.

Depending on the Sharp hardware you install, you can use AutoVu in a fixed configuration such as on a pole in a parking lot, or in a mobile configuration such as on a patrol vehicle.

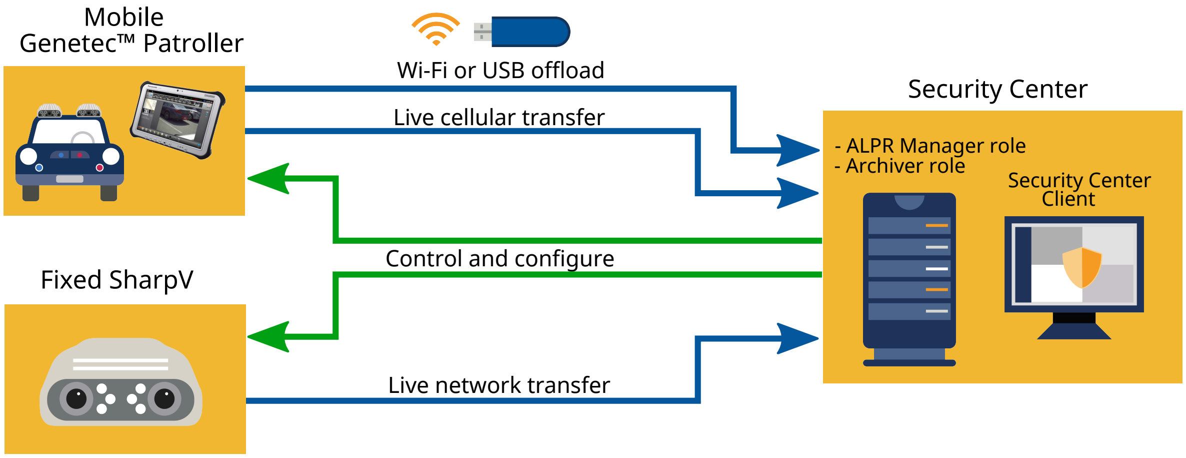
You can use AutoVu for the following:

- Scofflaw and wanted vehicle identification
- City-wide surveillance
- Parking enforcement
- Parking permit control
- Vehicle inventory
- Security
- Access control

AutoVu system architecture

In an AutoVu system, Sharp cameras send license plate images to Genetec Patroller™ or Security Center to be matched against lists of vehicles of interest (hotlists) and vehicles with permits (permit lists). Alternatively, you can send read data for processing in the cloud or using FTP or HTTP.

The following diagram shows how a typical AutoVu system works:



Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

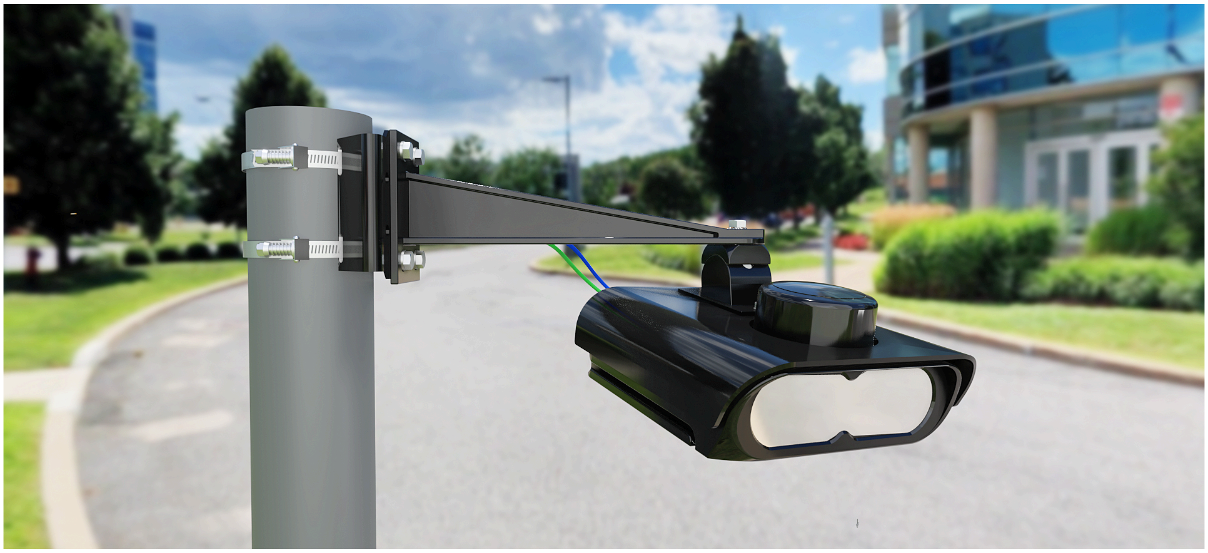
About Sharp ALPR units

An ALPR unit is a device that captures license plate numbers. An ALPR unit typically includes a context camera and at least one ALPR camera.

AutoVu™ Sharp cameras are the ALPR units produced by Genetec Inc. for use with Security Center. Sharp cameras include license plate capturing and processing components, as well as digital video processing functions, enclosed in a ruggedized casing. Sharp cameras are available for mobile and fixed installations.

- **Mobile AutoVu installation**: The SharpZ3 camera is mounted on a vehicle and is integrated into Genetec Patroller™ (the in-vehicle software of the AutoVu ALPR system), which in turn is integrated into Security Center. The ALPR Manager detects mobile SharpZ3 cameras through the AutoVu Patroller system they are connected to.

- **Fixed AutoVu installation**: The SharpV camera is mounted in a fixed location, such as on a pole, and is integrated directly into Security Center. The ALPR Manager detects SharpV camera directly through the Security Center *discovery port*.



Entities related to AutoVu ALPR

The AutoVu™ automatic license plate recognition (ALPR) system supports many of the entities that are available in Security Center.

The following table lists the entities related to ALPR.

Icon	Entity	Description
	ALPR Manager (role)	Role that stores all ALPR data collected from the ALPR units (fixed Sharps) and patrol vehicles that it manages.
	Archiver (role)	The Archiver stores the ALPR images that are associated with the reads and hits.
	ALPR unit	IP-based ALPR device.
	Hotlist	List of vehicles.
	Overtime rule	Type of hit rule that specifies a time limit for parking within a restricted area.
P	**Parking facility**	Defines a parking area or parking garage as a number of sectors and rows, to track vehicles inside that parking facility.
P	**Parking rule**	A parking rule defines how and when a parking session is either considered to be valid or in violation.
	Patroller	A patroller entity in Security Center represents a patrol vehicle equipped with an in-vehicle computer running Genetec Patroller™ software.
	Permit	Defines a parking permit holder list.
	Permit restriction	Type of hit rule that specifies where and when permit holders can park.
	User	Person who uses Security Center applications.
	User group	Group of users sharing common characteristics.

43

ALPR roles and units

This section includes the following topics:

About the ALPR Manager role

The ALPR Manager role manages and controls the patrol vehicle software (Genetec Patroller™), Sharp cameras, and parking zones. The ALPR Manager stores the ALPR data (reads, hits, timestamps, GPS coordinates, and so on) collected by the devices.

Multiple instances of this role can be created on the system to provide scalability and partitioning. For example, different fleets of patrol vehicles can be managed by different *ALPR Managers*.

ALPR Manager root folder

The root folder is the main folder on the computer hosting the ALPR Manager. It is where all the configuration files are created, saved, and exchanged between the ALPR Manager and the Genetec Patroller™ units it manages.

When you create an ALPR Manager role, the root folder is created automatically on your computer, located at: *C:\Genetec\AutoVu\RootFolder*. If you create multiple ALPR Manager roles, new folders are created at the same location. For example, if you create three ALPR Manager roles, Security Center automatically creates the following folders:

- *C:\Genetec\AutoVu\RootFolder1*
- *C:\Genetec\AutoVu\RootFolder2*
- *C:\Genetec\AutoVu\RootFolder3*

NOTE: ALPR Manager roles on the same server cannot share a root folder. Likewise, ALPR Manager roles on separate servers cannot share a root folder on a shared network drive.

Each ALPR Manager root folder includes the following subfolders:

- **ManualTransfer:** Contains the configuration and data files to transfer to Patroller manually using a USB key or similar device.
- **Offload:** Contains the ALPR data offloaded by Patroller.
- **Rules:** Contains the delta files used by Security Center to transfer hotlist and permit list changes. Do **not** copy or move anything in this folder.

ALPR data management

ALPR data in is managed in Security Center by the ALPR Manager role and by the Archiver role. Both roles work in tandem. In a new Security Center system with AutoVu licenses, an ALPR Manager role and an Archiver role are created by default on the main server.

If the Archiver cannot store the images (for example, when the disks are full), the ALPR Manager stops storing the ALPR metadata, and the Genetec Patroller™ installations and SharpV units that are controlled by the ALPR Manager temporarily store the data locally until the problem is resolved.

- **ALPR Manager**:
  - The ALPR metadata (reads, hits, timestamps, Patroller positions, and so on) are stored by the ALPR Manager role in a SQL Server database.
  - If you have many ALPR Manager roles in your system, they can all be linked to the same Archiver role.
- **Archiver**:
  - The ALPR images (captured by context cameras, ALPR cameras, and wheel imaging cameras) associated to the reads and hits are stored in the file system by an Archiver role.
  - The Archiver role follows the data retention periods configured for the ALPR Manager.

Configuring the ALPR Manager role

To manage reads, hits, and parking events, you must first configure the ALPR Manager role settings such as Genetec Patroller™ user groups, data retention periods, and so on, and assign an Archiver role to manage the ALPR images (captured by context cameras, ALPR cameras, and wheel imaging cameras) associated to the reads and hits.

What you should know

- A SQL Server Express database might fill up before the retention period ends. Contact GTAP to help you evaluate your database requirements.

  NOTE: When using SQL Server Express Edition, reducing the retention period makes space for new data, but it does not reduce the size of the database.
- If you have a large system, you can distribute the load by creating more ALPR Manager roles and hosting them on separate servers.

To configure the ALPR Manager role:

1. From the Config Tool home page, open the *ALPR* task, and click **Roles and units**.
2. Select the ALPR Manager you want to configure, and then click **Properties** > **General settings**.
3. To change the location of the ALPR Manager's **Root folder**, browse to a different folder on the local machine, or create a network folder.

   NOTE: If your computer is hosting more than one ALPR Manager, each ALPR Manager must have a different root folder.
4. If you have large hotlists or permit lists associated to individual Patroller units, turn on the **Optimize root folder disk space** option.

   IMPORTANT: If your Root folder is on a network drive, the Genetec™ Server service must be configured to run using a domain user and not a local user.

   Turning this option on enables the use of symbolic links to reduce the Root folder's disk space, and optimizes the in-vehicle computer's file transfer performance. On both the server and client machines (requires administrator rights), open Windows Command Prompt, and then type the following:

   - **To enable symbolic links:** Type `fsutil behavior set SymlinkEvaluation R2R:1`
   - **To disable symbolic links:** Type `fsutil behavior set SymlinkEvaluation R2R:0`.
5. From the **User group for Patrollers** list, select the user group that contains the list of users who are allowed to log on to the patrol vehicles managed by the ALPR Manager.

   In Genetec Patroller™ Config Tool, if the Patroller *Logon type* is *Secure name* or *Secure name and password*, the Patroller user must enter the username and password configured in Security Center. If secure logon names are in use, you can see in Security Desk who was driving the vehicle when a read or a hit occurred.

6. In the *Retention period* section, specify how long ALPR-related data can is kept:
   - **Genetec Patroller™ route retention period:** Number of days the Patroller *route* data (GPS coordinates) is kept in the database.
   - **Hit retention period:** Number of days the hit data is kept in the ALPR Manager database.
   - **Hit image retention period:** Number of days the hit image data is kept by the linked Archiver role. The *Hit image retention period* cannot exceed the *Hit retention period* since a hit image is always associated with a hit.
   - **Read retention period:** Number of days the *license plate reads* are kept in the ALPR Manager database. The *Read retention period* cannot exceed the *Hit retention period*. If the read retention is lower than the hit retention, only the reads that are associated with hits are kept.
   - **Read image retention period:** Number of days the read image data is kept by the linked Archiver role. The *Read image retention period* cannot exceed the *Read retention period* since a read image is always associated to a read.
   - **Event retention period:** Number of days Patroller events (user logged on, logged off, and patrol vehicle positions) are kept in the ALPR Manager database.
   - **Parking occupancy retention period:** Number of days the parking occupancy data is kept in the ALPR Manager database.
   - **Parking zone data retention period:** Number of days the parking zone data is kept in the ALPR Manager database. This data includes parking session information, for example, parking session start times and state transitions, as well as information on the events that occur within the parking zone. The *Parking zone data retention period* cannot exceed the *Read retention period*.

   The default value for each setting it 90 days, and the maximum is 4000 days. Expired data does not appear in Security Center queries and reports (Hit reports, Read reports, and so on).

   NOTE: You cannot reduce the size of the database by reducing the retention period settings. The retention cleanup algorithm is meant to make space for new data. However, the size of the database file on disk will never shrink.
7. Click **Apply**.
8. Click **Resources** > **Images saved to**, and select the Archiver designated to manage the image data for the ALPR Manager.

   In a new installation, the default Archiver is automatically assigned to the ALPR Manager. If your system is only used for ALPR, you can keep the default configuration. If you also intend to manage video on your system, we recommend that you create separate Archiver roles for video management.

   In an upgrade scenario, an Archiver is automatically assigned to an ALPR Manager only if it is the only Archiver in the system, and only if the Archiver does not manage any video units.
9. Click **Apply**.
10. If you selected an Archiver, click **Jump to** (➜) beside the Archiver name.

    This brings you directly to the **Resources** tab of the selected Archiver.

The basic ALPR Manager settings are configured. You can continue to customize your AutoVu™ system by configuring the other ALPR Manager settings.

After you finish

Set up the Archiver role for ALPR.

Related Topics

About the ALPR Manager role on page 959

ALPR Manager - Properties tab on page 1310

ALPR Manager - Resources tab on page 1337

Adding video units manually on page 572

Setting up the Archiver role for ALPR

You must link an Archiver to the ALPR Manager to store the ALPR images that are associated with the reads and hits.

What you should know

- By default, the Archiver uses the H.264 stream from SharpV cameras. If you want to use the MJPEG stream, you can select it in the **Configuration** > **Cameras** page in the Sharp Portal.
- If you need to manage both ALPR and video data, we recommend that you create separate Archiver roles, each handling only one function.
- Each Archiver role must store video on a separate drive or partition from other Archiver roles. If you are unable to have separate Archiver roles, you can manage both ALPR and video data with the same Archiver.

  NOTE: By default, the Archiver deletes the oldest files when its disks become full. This means that ALPR images might be deleted before their retention period is over. This does not affect ALPR metadata or the protected events and images.

To create an Archiver role for ALPR:

1 From the Config Tool home page, open the *Video* task.

2 Click the menu button beside **Video unit** (✚), and then click **Archiver** (▤).

The role creation wizard window opens.

3 On the *Specific info* page, set the following fields and then click **Next**.

- **Server:** This is only shown if you have more than one server in your system. If the ALPR Manager is hosted on its own server, we suggest using the same server to host the linked Archiver role. Make sure you have enough free space on disk to store the ALPR images. We recommend using a server where it is possible to configure the Archiver role with its dedicated local disk or disk partition.
- **Database server:** Name of the SQL Server service (default=(local)\SQLEXPRESS). If the Archiver is hosted on the same server as the ALPR Manager, we recommend using the same database server for both.
- **Database:** Name of the database instance (default=Archiver). We suggest using LPR_Archiver to differentiate it from video archive databases.

4 On the *Basic information* page, set the following fields, and then click **Next**.

- **Entity name:** Name of the Archiver role (default=Archiver).

  We suggest using LPR_Archiver to differentiate it from the Archiver role for video.
- **Entity description:** Role description. If this Archiver role is shared by many ALPR Manager roles, list them here.
- **Partition:** This is only shown if you have partitions defined in your system. Make sure you create this Archiver in the same partition as the ALPR Manager it is linked to. Only users who have access to the selected partition can view the ALPR data managed by these roles.

5 Verify that the information displayed in the *Creation summary* page is correct, and then click **Create**.

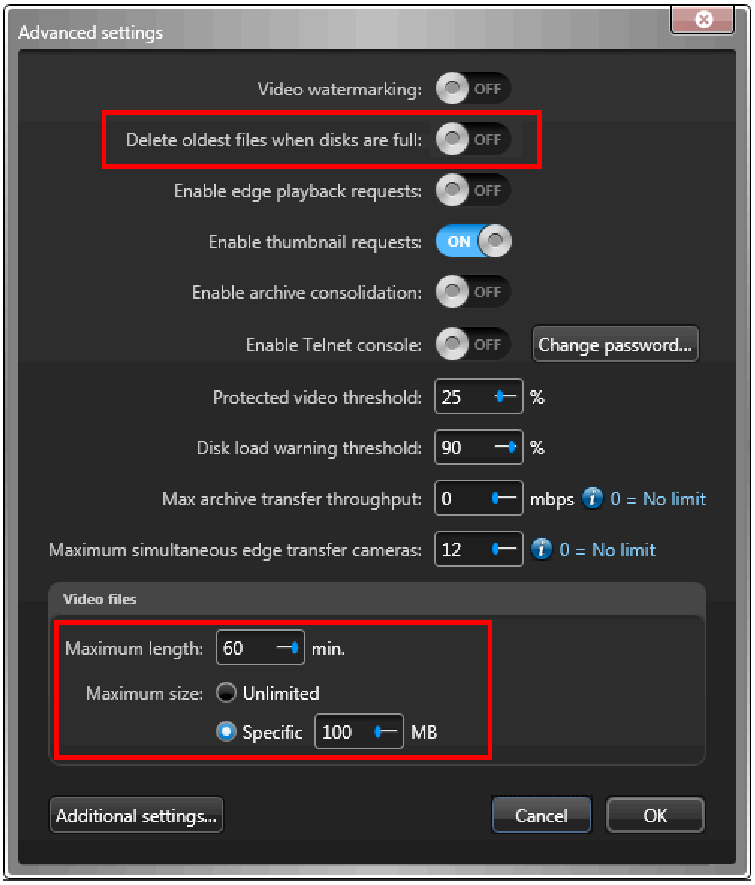
6 Click **Close**.

7 From the Archiver role's **Resources** tab, configure the archive storage settings.

IMPORTANT: Ensure you are not using the same disk as another Archiver role in your system, and that you have enough disk space for storing the ALPR images. For more information on the storage requirements for ALPR images, refer to the *Security Center Release Notes*.

NOTE: The Archiver follows the **Hit** and **Read image retention period** set for the ALPR Manager. If multiple ALPR Manager roles are linked to the same Archiver, the ALPR Manager with the longest image retention period has precedence. This means that the image data might be kept longer than necessary for some ALPR Manager roles, but it does not affect the ALPR metadata nor the ALPR reports. No ALPR data beyond the specified retention periods appear in reports.

8 Click **Advanced settings**, and optimize the settings for storing ALPR image data.



Advanced settings

Video watermarking: OFF

Delete oldest files when disks are full: OFF

Enable edge playback requests: OFF

Enable thumbnail requests: ON

Enable archive consolidation: OFF

Enable Telnet console: OFF Change password...

Protected video threshold: 25 %

Disk load warning threshold: 90 %

Max archive transfer throughput: 0 mbps 0 = No limit

Maximum simultaneous edge transfer cameras: 12 0 = No limit

Video files

Maximum length: 60 min.

Maximum size: ○ Unlimited

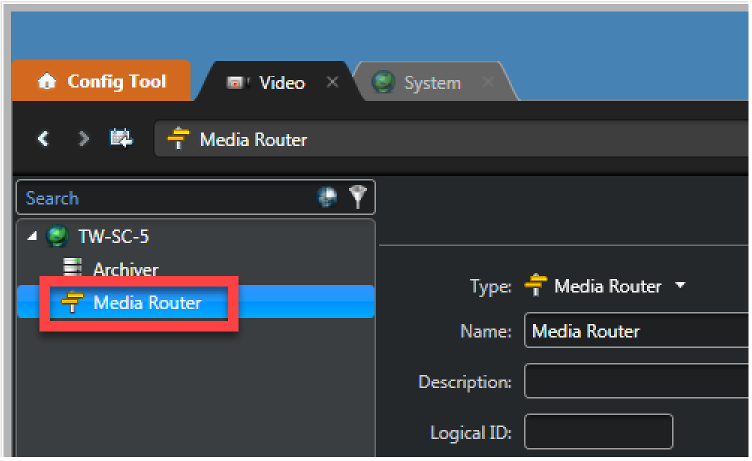
● Specific 100 MB

The recommended values are:

- **Delete oldest file when disks are full:** OFF (default setting for video is ON).
- **Maximum length:** 60 minutes (default value for video is 20 minutes).
- **Maximum size:** 100 MB (default value for video is 500 MB).

9 Click **OK** > **Apply**.

10 In the entity browser (left pane) of the *Video* task, make sure that the Media Router role is running.



Type: Media Router

Name: Media Router

Description:

Logical ID:

11 Click **Media Router** and configure the ports, redirectors, and network cards to make sure that the Archiver can deliver the ALPR images to all client workstations on your system.

If all your servers are on the same network, and all your servers have only one network card, the default settings should work without any change.

Related Topics

About the Media Router role on page 596

Configuring the Media Router role on page 597

Adding redirectors to the Media Router on page 598

About the Network view on page 154

Customizing network options on page 157

Migrating ALPR images to another server on page 1166

Storage requirement for ALPR images

The images associated with the reads and hits are stored on disk in G64 files by an Archiver. You can estimate the disk space required to store these images if you know the average number of reads and hits processed by the ALPR Manager per day.

For every license plate read or hit processed by the ALPR Manager, the Archiver stores a set of four images:

- One context camera image (in either high resolution or low resolution)
- One ALPR camera image (cropped to show only the license plate)
- One context camera thumbnail image
- One ALPR camera thumbnail image

The size of the image set depends on the model of the Sharp camera and whether the context camera is configured to take images in high resolution or low resolution.

Use the following formula to estimate the disk space you need for the desired image retention periods.

```
Disk space = (ReadsPD x ImageSize x ReadIRP) + (HitsPD x ImageSize x HitIRP)
```

where:

- **ReadsPD:** Average number of reads per day.
- **ImageSize:** Estimated image size per read (depends on the Sharp model and configuration).
- **ReadIRP:** Read image retention period (see ALPR Manager's **Properties** tab).
- **HitsPD:** Average number of hits per day.
- **HitIRP:** Hit image retention period (see ALPR Manager's **Properties** tab).

If your patrol vehicles are equipped with wheel imaging cameras, double the number of hits per day in your formula (there is typically one wheel image per hit).

The following table gives you the rough estimates of the image size per read based on the Sharp model and configuration.

Type of image	Sharp G1	SharpV G2	SharpV G3	SharpZ3
High-resolution configuration				
Context camera image	~120 KB	~120 KB	~250 KB	~160 KB
ALPR camera image (cropped)	~3 KB	~3 KB	~3KB	~2 KB
Context camera thumbnail image	~3 KB	~3 KB	~3KB	~2 KB
ALPR camera thumbnail image	~1 KB	~1 KB	~1KB	~1 KB
Total image size per read:	~127 KB	~127 KB	~257KB	~165 KB
Low-resolution configuration				
Context camera image	-	-	-	-
ALPR camera image (cropped)	~3 KB	~3 KB	-	-
Context camera thumbnail image	~3 KB	~3 KB	-	-

Type of image	Sharp G1	SharpV G2	SharpV G3	SharpZ3
ALPR camera thumbnail image	~1 KB	~1 KB	-	-
Total image size per read:	-	-	-	-

NOTE: If a read or hit is protected and must be kept beyond its specified retention period, it will require more disk space for its associated images than what is calculated for a single event. Because the Archiver stores multiple ALPR images in a single G64 file, if one image in the file is protected, then all other images in the file are also protected. This uses up more disk space over time. However, an image whose corresponding read or hit has been deleted can no longer be read because the G64 files are encrypted.

If the Archiver is assigned to more than one ALPR Manager, add the numbers for all ALPR Manager roles together.

ALPR matcher

The ALPR matcher is the AutoVu™ software engine that matches license plates captured by Sharp cameras to license plates in a data source such as a hotlist or permit list, or to previously captured license plates, such as for overtime enforcement. The ALPR matcher determines if a plate read results in a hit.

How ALPR matcher logic works

Real-world conditions make license plate recognition more challenging. License plates might have characters that are hidden by dirt or snow, while other plates might have chipped or faded paint. Some plates might even have pictures or screws that can be misread as legitimate license plate characters.

If the ALPR matcher were only capable of raising a hit based on an exact match, many plates that should be hits would instead be missed.

Example

A hotlist contains the plate ABC123. While on a patrol, a Sharp camera reads the license plate ABC12, but is unable to read the last character because the character's paint is chipped.

The ALPR matcher must be capable of more than "yes/no" logic because the plate read ABC12 *might* be a match. It would be better to raise the hotlist hit, and let the Genetec Patroller™ operator decide whether or not the hit is legitimate. To do this, the ALPR matcher uses different levels of "maybe" logic to allow for more possibilities for a plate match.

IMPORTANT: Adjusting matcher settings can have major effect on the performance of the system. Test the system thoroughly after modifying the settings. For assistance, contact the AutoVu Support team.

ALPR matcher technique: OCR equivalence

The ALPR matcher uses the *Optical Character Recognition (OCR) equivalence* technique to improve plate read accuracy rate.

Depending on the font design, some plate characters can look very similar to other characters. These are called "OCR equivalent characters".

You can configure how the ALPR matcher handles OCR equivalence by modifying the MatcherSettings.xml file. For more information, see MatcherSettings.xml file on page 976.

The default Latin-based OCR equivalent characters are the following:

- The number "0" and the letters "O", "D", and "Q".
- The number "1" and the letter "I".
- The number "2" and the letter "Z".
- The number "5" and the letter "S".
- The number "8" and the letter "B".
- The number "6" and the letter "G".

BEST PRACTICE: Do not allow more than two OCR equivalent characters because it results in too many false-positive matches.

Example

The following example uses a hotlist with the ALPR matcher configured to allow for one OCR equivalent character:

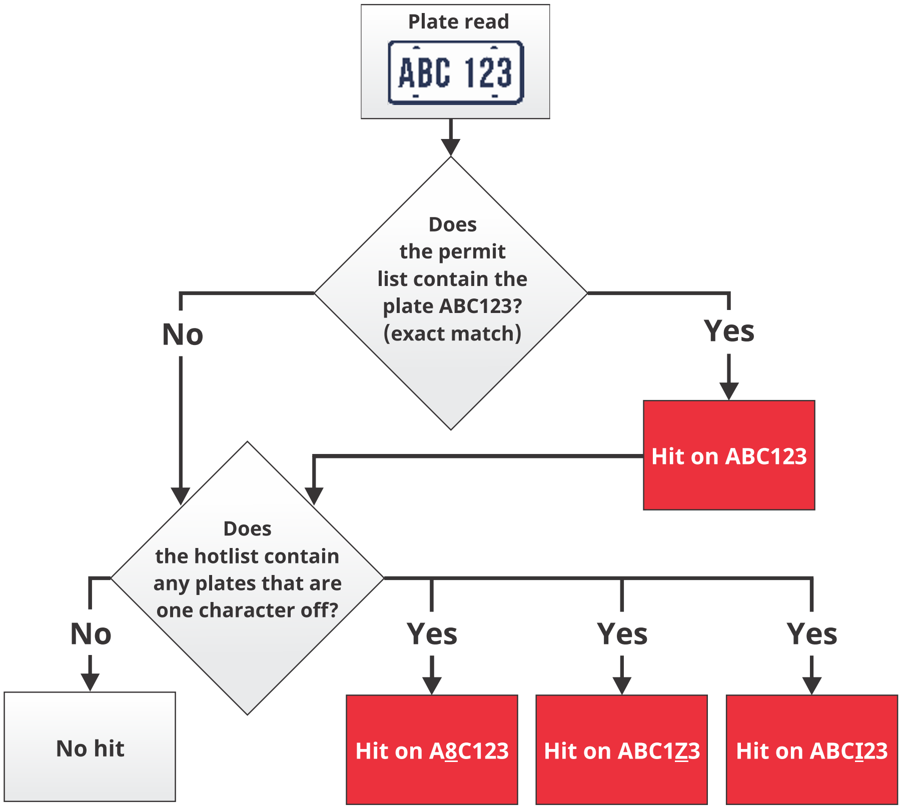


Plate read
ABC 123
Does the permit list contain the plate ABC123? (exact match)
No
Yes
Hit on ABC123
Does the hotlist contain any plates that are one character off?
No
Yes
Yes
Yes
No hit
Hit on A8C123
Hit on ABC1Z3
Hit on ABCI23

- The ALPR matcher finds the exact match ABC123 in the hotlist and raises a hit. It also looks for any plates that are one OCR equivalent character off, and finds A**8**C123, ABC1**Z**3, and ABC**I**23 in the hotlist, so it raises hits on them also.
- If the ALPR matcher found the plate A**8**C**IZ**3 (three OCR equivalent characters off), it would not raise a hit because the system is configured to accept a maximum of one OCR difference.

Related Topics

ALPR matcher technique: Common and contiguous characters on page 970

ALPR matcher technique: Number of character differences on page 969

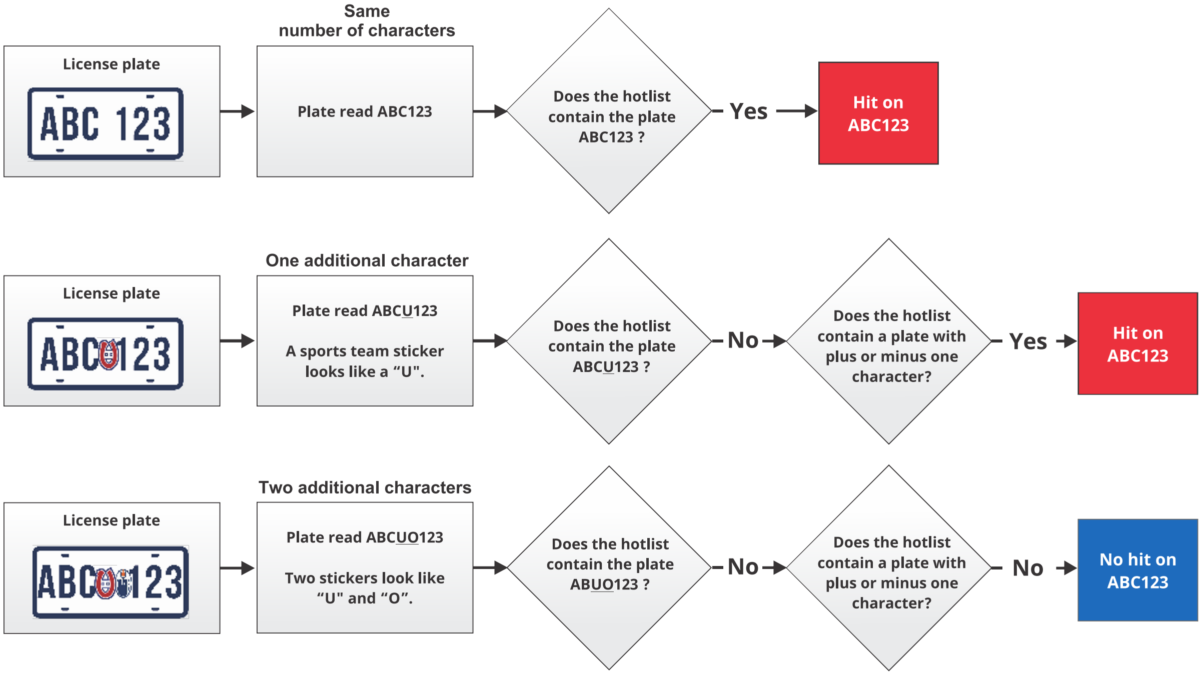
ALPR matcher technique: Number of character differences

The ALPR matcher uses the "Number of character differences" technique to improve the plate read accuracy rate.

This technique allows for a difference in the number of characters between the plate read and the plate number in the hotlist. This allows the system to account for characters in the plate that cannot be read (dirt, bad camera angle, and so on), and for objects on the plate that might be mistaken for legitimate characters (screws, pictures, and so on).

Example

In the following example, the hotlist contains the license plate ABC123. The ALPR matcher configured to allow for *one* difference in the number of characters.


Same number of characters
License plate
ABC 123
Plate read ABC123
Does the hotlist contain the plate ABC123 ?
Yes
Hit on ABC123
One additional character
License plate
Plate read ABCU123
A sports team sticker looks like a "U".
Does the hotlist contain the plate ABCU123 ?
No
Does the hotlist contain a plate with plus or minus one character?
Yes
Hit on ABC123
Two additional characters
License plate
Plate read ABCUO123
Two stickers look like "U" and "O".
Does the hotlist contain the plate ABUO123 ?
No
Does the hotlist contain a plate with plus or minus one character?
No
No hit on ABC123

- ABC**U**123 matches the plate ABC123 because you allowed one difference in the number of characters. With this configuration, a license plate with one more or one fewer characters generates a hit.
- AB**UO**123 does not match the plate ABC123 because it has more than one additional character.

Related Topics

ALPR matcher technique: Common and contiguous characters on page 970

ALPR matcher technique: OCR equivalence on page 968

ALPR matcher technique: Common and contiguous characters

The ALPR matcher uses the "Common and contiguous characters" technique to improve plate read accuracy rate (sometimes called "fuzzy matching").

NOTE: This method is used for overtime parking enforcement only.

You can configure how the ALPR matcher handles common and contiguous characters by modifying the MatcherSettings.xml file. For more information, see MatcherSettings.xml file on page 976.

The following settings are available when configuring common and contiguous characters:

- **Necessary common characters:** The minimum number of characters that need to be common to both the first and second plate read. The characters must also appear in the same order in the plate, but not necessarily in sequence.
- **Necessary contiguous characters:** Minimum character sequence length between the first and second plate read.

  In overtime enforcement, there is an extra margin of error because the ALPR matcher is comparing a plate read against another plate read, not against a hotlist or permit list created by a person.

Example

Here's an example with the ALPR matcher configured to look for five common characters and four contiguous characters (default). The ALPR matcher also allows for the default one OCR equivalent character, which can count as a common or contiguous character.

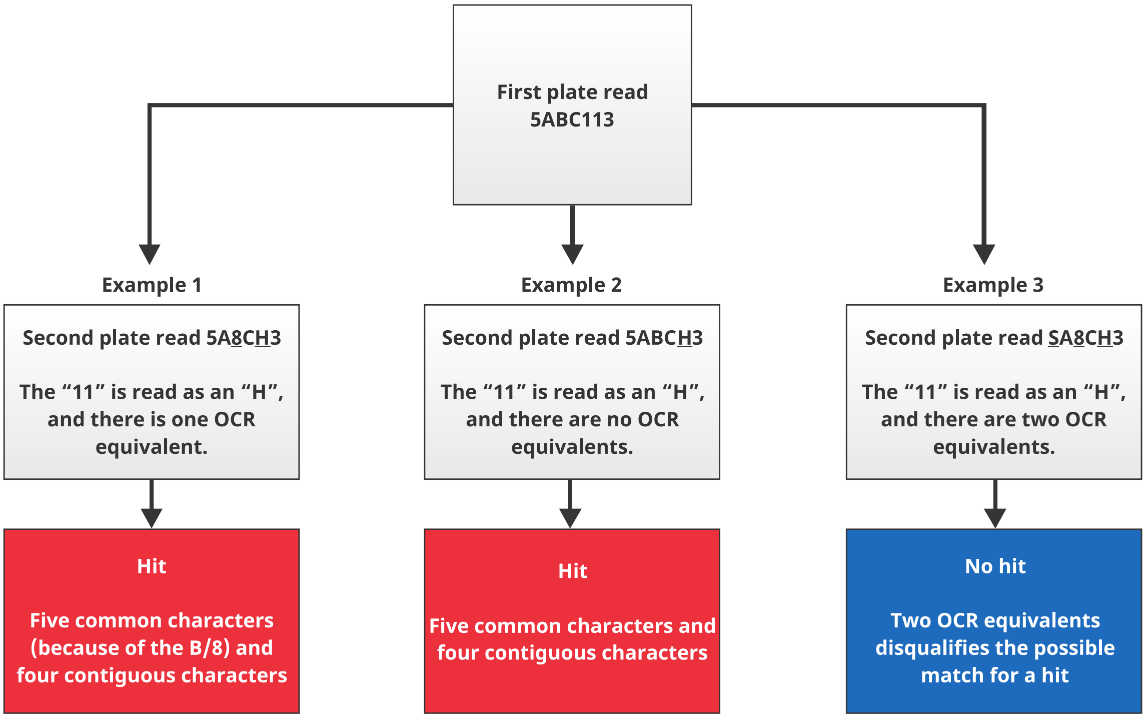

First plate read
5ABC113
Example 1
Second plate read 5A8CH3
The "11" is read as an "H", and there is one OCR equivalent.
Hit
Five common characters (because of the B/8) and four contiguous characters
Example 2
Second plate read 5ABCH3
The "11" is read as an "H", and there are no OCR equivalents.
Hit
Five common characters and four contiguous characters
Example 3
Second plate read SA8CH3
The "11" is read as an "H", and there are two OCR equivalents.
No hit
Two OCR equivalents disqualifies the possible match for a hit

Plate read 5ABC113 matches with 5A8CH3 (example 1) and 5ABCH3 (example 2) because the following conditions are met:

- **OCR equivalence:** The OCR equivalents B and 8 are considered the same character and apply towards the common and contiguous character count.
- **Five common characters:** Both reads have 5, A, B/8, C, and 3 in common, and they all appear in the same order. The "3" is not in sequence, but it respects the order.
- **Four contiguous characters:** Both reads have 5, A, B/8, and C in sequence.

Plate read 5ABC113 does *not* match with SA8CH3 (example 3) because there are two OCR equivalents in the second read (S/5 and B/8). You allowed for only one OCR equivalent.

Using common and contiguous characters helps reduce the margin of error involved when both first and second plate reads are coming from the Sharp.

Related Topics

ALPR matcher technique: OCR equivalence on page 968

ALPR matcher technique: Number of character differences on page 969

About matcher settings files

When dirty or damaged license plates are misread by a Sharp camera, different methods are available for matching the plate read to a permit. Which matcher settings file you need to configure depends on the AutoVu™ installation type.

The following ALPR matcher files and settings are available on the ALPR server:

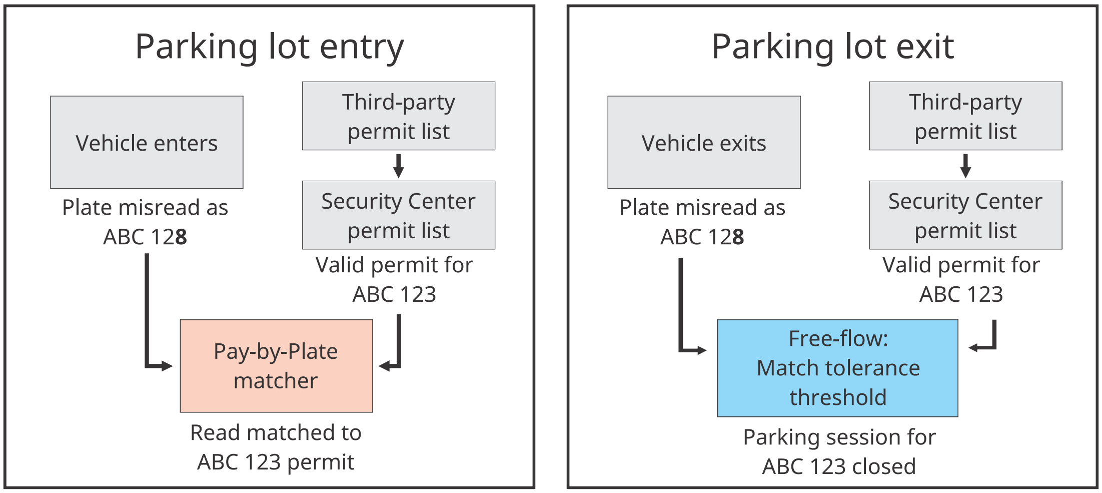
ALPR matcher	File or setting	Location
General matcher	MatcherSettings.xml	*C:\Program Files\Genetec Security Center X.X.*
Pay-by-Plate Sync matcher	*Genetec.Plugins.MobilePBP.dll.config*	*C:\Program Files (x86)\Security Center Plugins\MobilePBP*
AutoVu™ Free-Flow setting	Match tolerance threshold	*AutoVu™ Free-Flow* section of the ALPR Manager *Properties* page

Fixed SharpV cameras using Free-Flow and the Pay-by-Plate Sync plugin

In this case, the Pay-by-Plate Sync matcher settings are used to validate license plate reads at the parking lot entrance against the Security Center permit file that has been updated with third party permits by Pay-by-Plate Sync.

The **Match tolerance threshold** setting is used to close parking sessions if the plate is misread at the parking lot exit.

NOTE: In the following example, the matcher settings allow one OCR equivalent character.

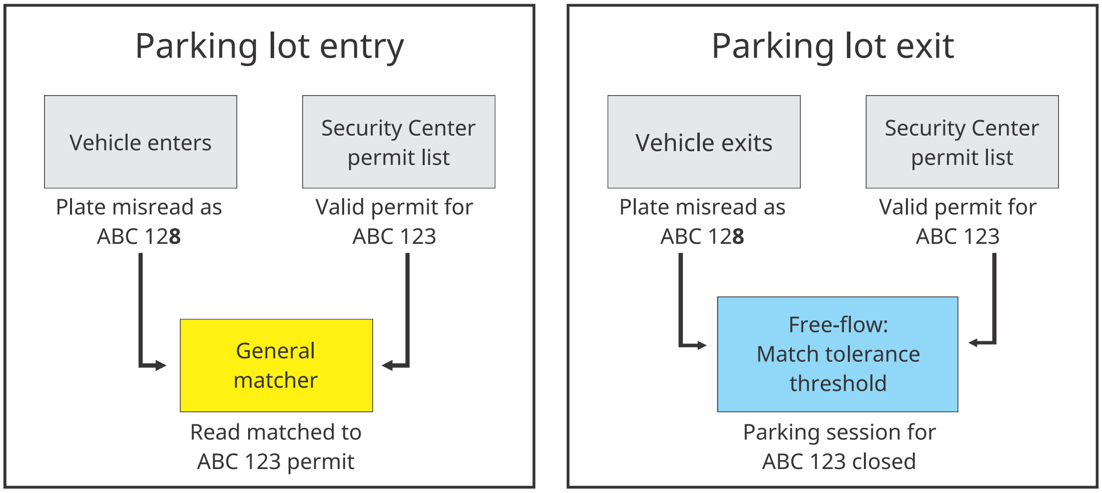


Fixed SharpV cameras using Free-Flow without the Pay-by-Plate Sync plugin

In this case, the general matcher file is used to validate license plate reads at the parking lot entrance against the Security Center permit list. No third-party lists are involved in this scenario.

The **Match tolerance threshold** setting is used to close parking sessions if the plate is misread at the parking lot exit.

NOTE: In the following example, the matcher settings allow one OCR equivalent character.

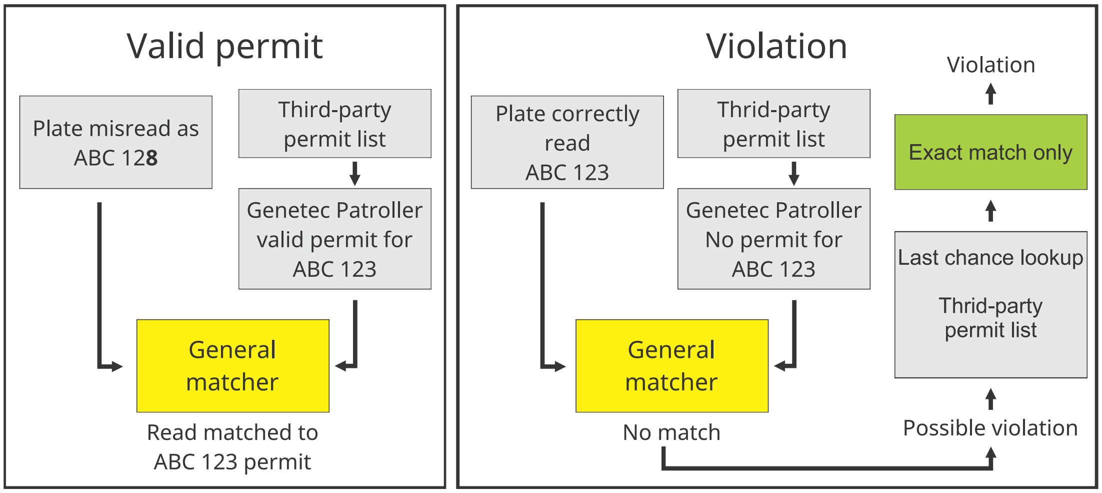


Mobile SharpZ3 cameras using the Pay-by-Plate Sync plugin

In this case, the general matcher file is used to validate license plate reads against the Genetec Patroller™ permit file that has been updated with third party permits by Pay-by-Plate Sync.

When the system performs a last chance lookup to verify that the permit has not recently been added to the list, no matcher settings are applied. Only an exact match triggers a violation.

NOTE: In the following example, the matcher settings allow one OCR equivalent character.

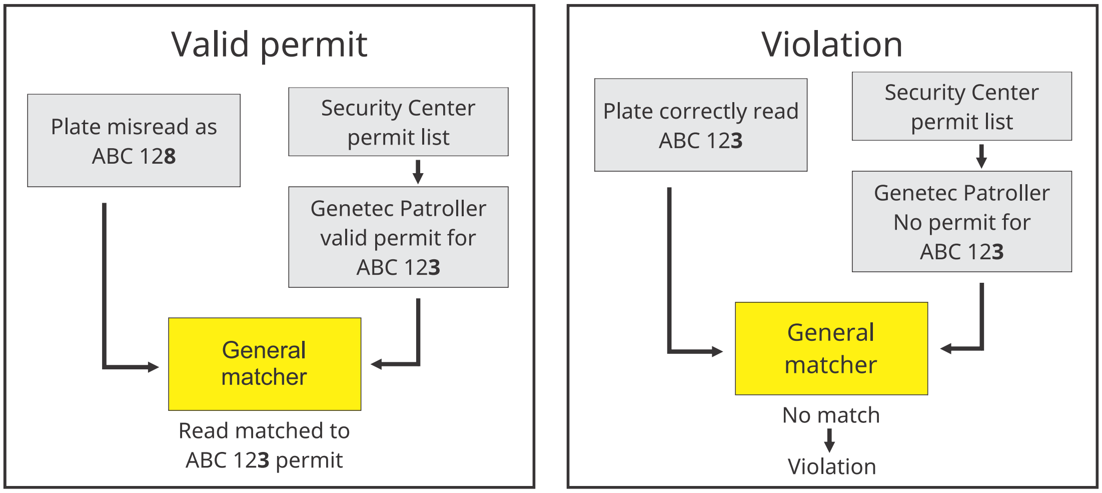


Mobile SharpZ3 cameras without the Pay-by-Plate Sync plugin

In this case, the general matcher file is used to validate license plate reads against the Patroller permit file that has been updated with the current Security Center permit list.

When the system performs a last chance lookup to verify that the permit has not recently been added to the list, no matcher settings are applied. Only an exact match triggers a violation.

NOTE: In the following example, the matcher settings allow one OCR equivalent character.


Valid permit
Plate misread as ABC 128
Security Center permit list
Genetec Patroller valid permit for ABC 123
General matcher
Read matched to ABC 123 permit
Violation
Plate correctly read ABC 123
Security Center permit list
Genetec Patroller No permit for ABC 123
General matcher
No match
Violation

Best practices for configuring ALPR matcher settings

How you configure the ALPR matcher depends on your enforcement scenario. In some AutoVu™ systems, you'll want an exact match only. In other systems, you'll benefit from having a false positive on a potential match because it decreases the chances of missing a vehicle of interest.

Use the following best practices when configuring ALPR matcher settings:

- **Exact match:** The ALPR matcher always looks for an exact match if possible, but you can configure it to allow *only* exact matches. This is typically used when you have very large hotlists (millions of entries). By limiting the number of possible matches, you lighten the processing load on the Genetec Patroller™ computer, and you decrease the number of false positives that you would normally get from a list of that size. To allow only exact matches, turn on the *Simplematcher* feature in Patroller Config Tool, and turn off OCR equivalence.
- **OCR equivalence:** By default, the ALPR matcher allows for one OCR equivalent character. You can allow as many as you want, but generally you should not allow more than two because you'll get too many false positives.
- **Number of differences allowed:** By default, the ALPR matcher does not allow any number of differences. The number you allow depends on the plates in your region. The more characters on a plate, the more differences you can allow, but generally you should not allow more than two because you'll get too many false positives.
- **Common and contiguous characters:** (Used for overtime enforcement only) By default, the ALPR matcher looks for five common, and four contiguous characters to generate an overtime hit. The number you specify depends on the plates in your region. The more characters on a plate, the more common and contiguous characters you can allow.

Related Topics

Configuring ALPR matcher settings on page 978

MatcherSettings.xml file

The *MatcherSettings.xml* file contains the settings for the techniques used by the ALPR matcher: OCR equivalence, number of character differences, and common and contiguous characters.

The file is located on the computer hosting the Security Center Directory role, in the folder *C:\Program Files \Genetec Security Center 5.11*.

NOTE: If you have a mobile AutoVu™ system, a copy of the same file is located on the Genetec Patroller™ in-vehicle computer. You make your changes in the Security Center version of the file. The file on the Patroller computer is overwritten the next time Patroller connects to Security Center wirelessly, or when you manually transfer Patroller settings with a USB key.

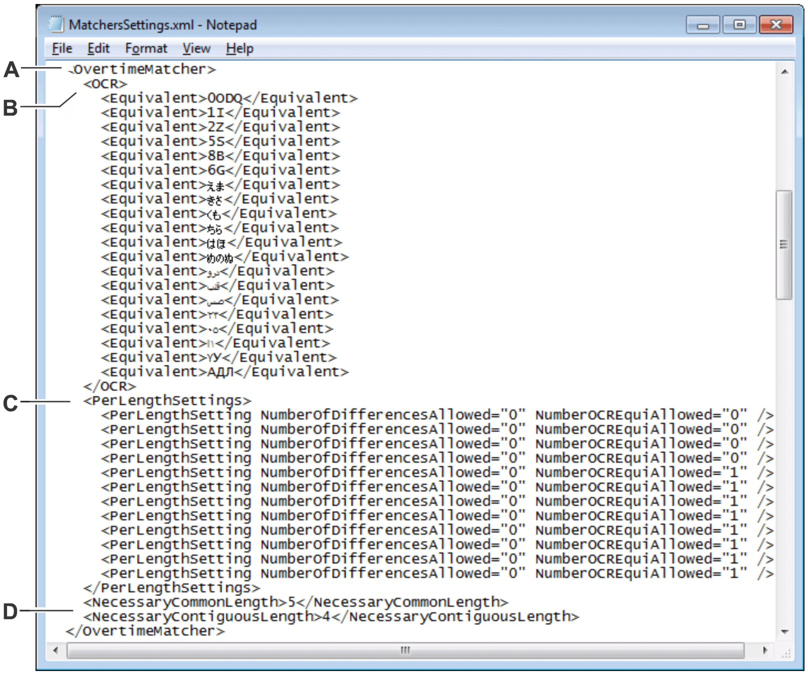
The *MatcherSettings.xml* file is composed of <Matcher> tags that define the settings for each type of matching scenario:

- **<HotlistMatcher>:** Settings for matching plate reads with hotlists.
- **<OvertimeMatcher>:** Settings for matching a plate read against all other plate reads in the Patroller database.
- **<PermitMatcher>:** Settings for matching plate reads with permit lists.
- **<MLPIMatcher>:** Settings for reconciling inventories in Security Desk.

The structure of the *MatcherSettings.xml* file allows you to have different behavior for the different enforcement scenarios. For example, to maximize your plate read accuracy rate in an enforcement scenario that includes both permits *and* hotlists, you'll typically want to use only OCR equivalence for the hotlist matcher, but also allow one difference in the number of characters for the permit matcher to decrease false-positives.

MatcherSettings.xml file example

The following is an example of the *MatcherSettings.xml* file:



```
<OvertimeMatcher>
  <OCR>
    <Equivalent>0ODQ</Equivalent>
    <Equivalent>1I</Equivalent>
    <Equivalent>2Z</Equivalent>
    <Equivalent>5S</Equivalent>
    <Equivalent>8B</Equivalent>
    <Equivalent>6G</Equivalent>
    <Equivalent>えま</Equivalent>
    <Equivalent>きさ</Equivalent>
    <Equivalent>くも</Equivalent>
    <Equivalent>ちら</Equivalent>
    <Equivalent>はほ</Equivalent>
    <Equivalent>めのぬ</Equivalent>
    <Equivalent>رو</Equivalent>
    <Equivalent>قب</Equivalent>
    <Equivalent>صس</Equivalent>
    <Equivalent>٢٣</Equivalent>
    <Equivalent>٠٥</Equivalent>
    <Equivalent>١١</Equivalent>
    <Equivalent>٧У</Equivalent>
    <Equivalent>АДЛ</Equivalent>
  </OCR>
  <PerLengthSettings>
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  </PerLengthSettings>
  <NecessaryCommonLength>5</NecessaryCommonLength>
  <NecessaryContiguousLength>4</NecessaryContiguousLength>
</OvertimeMatcher>
```

A: Matcher-specific settings

Each enforcement type (hotlist, permit, overtime, and MLPI) has its specific settings listed between the opening and closing <Matcher> tags.

For example, overtime matcher settings are listed between <OvertimeMatcher> and </OvertimeMatcher>.

B: OCR equivalent characters

The default OCR equivalent characters for each enforcement type are listed as between <OCR> and </OCR>.

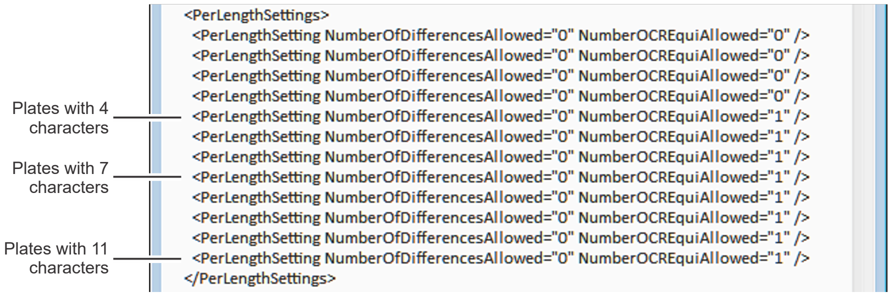
C: PerLength settings

For each matcher, specify the number of differences allowed, and the number of OCR equivalents allowed for license plates of different character lengths.

BEST PRACTICE:

- There are 12 PerLengthSetting lines, each containing NumberOfDifferencesAllowed and NumberOCREquiAllowed tags.
- Each PerLengthSetting line corresponds to a plate character length. The line you edit depends on the number of characters on the license plates in your patrol region.
- Ignore the first line because it represents plates with zero characters. The second line represents plates with one character, the third line represents plates with two characters, and so on for a maximum of 11 possible plate characters.
- You can edit more than one line to apply settings to plates of different character lengths.

The default settings are PerLengthSettings. No differences are allowed, and one OCR equivalent is allowed for plates that have 5 to 11 characters.



```
<PerLengthSettings>
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
</PerLengthSettings>
```

D: Common and contiguous character settings

These settings apply to overtime parking enforcement only.

- **<NecessaryCommonLength>:** Specify the minimum number of characters that must be common to both the first and second plate read. The characters must also appear in the same order in the plate, but not necessarily in sequence.
- **<NecessaryContiguousLength>:** Minimum character sequence length between the first and second plate read.

Configuring ALPR matcher settings

To adjust how license plates captured by Sharp are matched to license plates in a hotlist or permit list, you must configure the ALPR matcher logic.

Before you begin

Read the best practices for configuring ALPR matcher settings.

IMPORTANT: Test your system with the default ALPR matcher settings. If the read accuracy rate meets your requirements, then do **not** adjust the ALPR matcher settings.

What you should know

You configure ALPR matcher settings in the *MatcherSettings.xml* file, and then apply your changes in Server Admin and the Server Admin console.

The overtime matcher is used as an example, but the same steps apply to all the matchers in the XML file.

To configure ALPR matcher settings:

1. On the computer hosting the Security Center Directory role, open Windows Explorer and then go to *C:\Program Files\Genetec Security Center 5.11*.
2. Open *MatcherSettings.xml* in Notepad or a similar text editor.
3. Add or remove OCR equivalent characters from the list.

   The default OCR equivalent characters are listed between the <OCR> and </OCR> tags. Add new <Equivalent>____</Equivalent> lines, or delete the lines you do not want.
4. Specify the number of character differences that you want to allow.

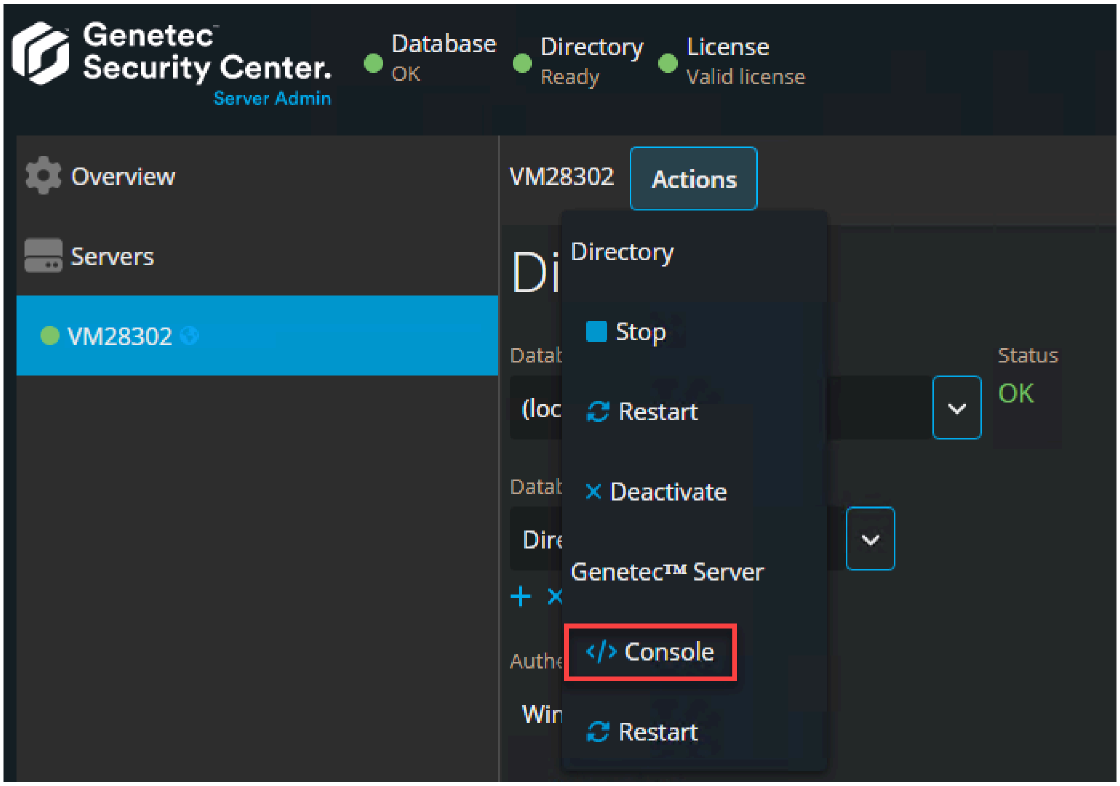
   Edit the PerLengthSetting line that applies to the plates in your region. For example, Quebec plates typically have six or seven characters, so edit the NumberOfDifferencesAllowed value in the sixth and seventh PerLengthSetting lines.

   NOTE: A value of "0" turns the setting off.
5. Specify the number of OCR equivalent characters that you want to allow by editing the NumberOCREquiAllowed value. This turns on OCR equivalence.

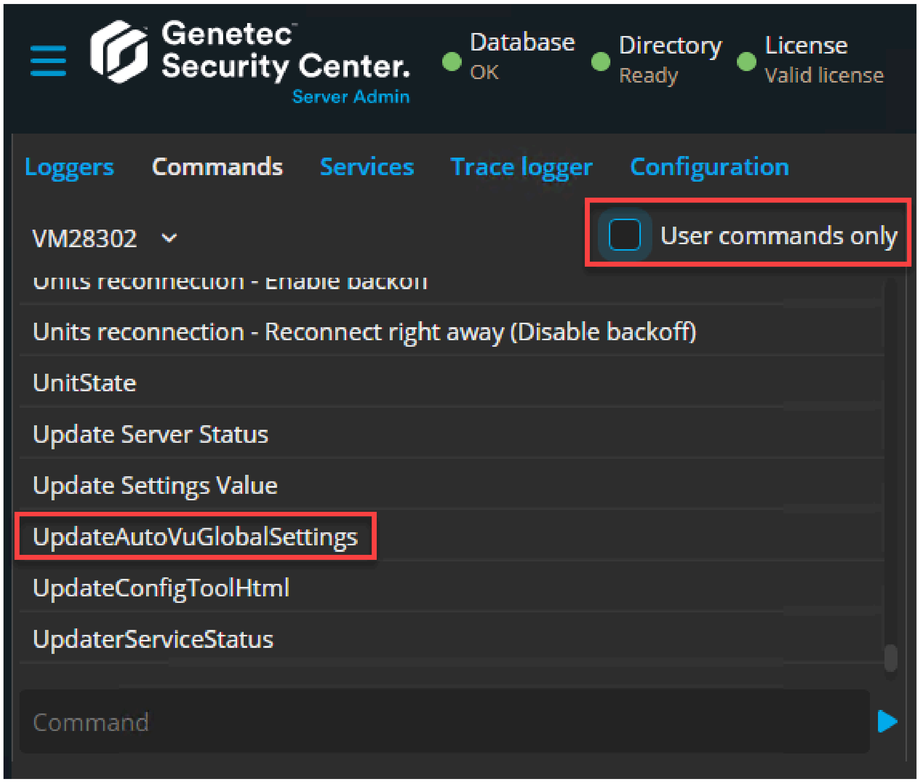
   NOTE: A value of "0" turns the setting off.
6. (Overtime only) Specify the number of common and contiguous characters.

   For common characters, edit the NecessaryCommonLength value. For contiguous characters, edit the NecessaryContiguousLength value.
7. Save and close the text editor.

8 Apply the ALPR matcher settings in Server Admin, as follows:
   a) From a web browser, open Server Admin typing *http://<server>/genetec*.
   b) From the *Servers* section on the *Overview* page, select the server that hosts the Directory role.
   c) Next to the server name, click **Actions** > **Console**.



   a) Click the **Commands** tab.
   b) Clear the **User commands only** checkbox.
   c) From the list of commands, click **UpdateAutoVuGlobalSettings**.

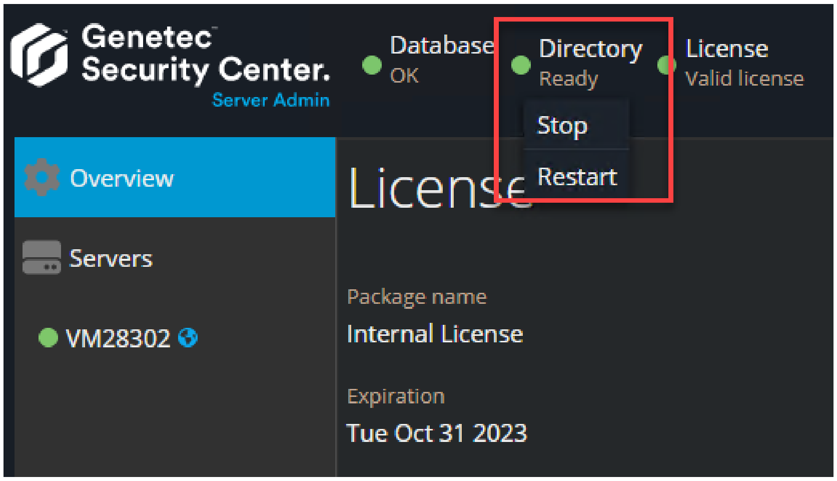


d) Close Server Admin.

9 Restart the Security Center Directory role, as follows:

a) From a web browser, open Server Admin typing http://<server>/genetec.

b) Click **Directory** and select **Restart**.



c) After the Directory restarts, close Server Admin.

ALPR matcher settings are now configured and applied to all the ALPR Manager roles on your system. Genetec Patroller™ units are updated the next time they connect to Security Center wirelessly, or when you manually transfer Patroller settings using a USB key.

After you finish

Verify that your ALPR Manager roles have been updated by looking at the *MatcherSettings.xml* file in their corresponding root folders (*C:\Genetec\AutoVu\RootFolder\ManualTransfer\General*). You can also tell by the XML file's *Date modified* field that it has been updated.

Related Topics

MatcherSettings.xml file on page 976

Modifying the auto-complete suggestions for filters in the *Reads* report

To customize the auto-complete suggestions for *Reads* report filters, you can add or delete default values in the annotation fields. For example: *Vehicle color*, *Vehicle make*, and *Vehicle type*.

What you should know

Customizing the auto-complete suggestions is useful in the following scenarios:

- If the SharpOS of your camera units is updated with new auto-complete suggestions that are currently unavailable on your Security Center system. For example, if the updated SharpOS identifies *Gold* as a *Vehicle color*, you might need to customize the list of suggested vehicle colors in Security Center to include *Gold*.
- If you use an SDK or a plugin to edit the *Sharp analytics* attributes of the reads captured. For example, you could use a plugin to edit the *Vehicle color* attribute in a read to *Silver*. In this case you might need to add *Silver* to the list of suggested vehicle colors in Security Center.

To modify auto-complete suggestions for filters:

1. From the Config Tool homepage, click **ALPR** > **General settings** > **Annotation fields**.
2. Select the *Sharp analytic* filter that you want to edit.
3. Click ✏.

   The **Edit an annotation field** window opens.
4. Click the **Edit** icon (✏) next to *Field name*.

   The **Edit annotation field suggestions** window opens.
5. To add a suggestion: Enter a value, and click ➕.

   To add multiple suggestions, enter values separated by a comma, and click ➕.
6. To delete a suggestion: Select a value, and click ✖.
7. Click **OK**.
8. Click **Cancel**.

The *Reads* report now includes your custom auto-complete filter suggestion.

44

Hotlists

This section includes the following topics:

About hotlists

A hotlist is a list of wanted vehicles, where each vehicle is identified by a license plate number, the issuing state, and the reason why the vehicle is wanted (stolen, wanted felon, Amber alert, VIP, and so on). Optional vehicle information might include the model, the color, and the vehicle identification number (VIN).

Hotlists are used by both the AutoVu™ Genetec Patroller™ and the AutoVu ALPR Manager role to check against license plates captured by ALPR units to identify vehicles of interest.

The hotlist entity is a type of hit rule. A hit rule is a method used by AutoVu to identify vehicles of interest. Other types of hit rules include *overtime*, *permit*, and *permit restriction*. When a plate read matches a hit rule, it is called a hit. When a plate read matches a plate on a hotlist, it is called a hotlist hit.

Creating hotlists

To use a hotlist in Security Center, you must create the hotlist, map it to its source text file, and configure it for your enforcement scenario.

Before you begin

Create the hotlist source as a *.txt* or *.csv* text file.

What you should know

- Hotlists can be used with any type of AutoVu™ fixed or mobile system.
- The source text file must be located on a drive that is accessible from the computer hosting the ALPR Manager.

To create a hotlist:

1. From the Config Tool home page, click **ALPR** > **Hotlists**, and then click **Hotlist** (+).

   The *Creating a hotlist* wizard opens.
2. Click the **Basic information** tab, type a name for the hotlist in the **Entity name** field, and click **Next**.

   You can enter an optional entity description.
3. Set the priority of the hotlist using the **Priority** slider.

   Zero (0) is the highest priority setting and 100 is the lowest. If a plate read matches more than one hotlist, the hotlist with the highest priority is displayed first in the list of hotlist matches.
4. Enter the **Hotlist path** on the computer where the hotlist source text file is located.

   If you start typing a path to a network drive, you might have to enter a username and password to access the network drive.

   NOTE: The Windows credentials you enter must have read/write access to the hotlist file.
5. If the attribute fields in the source text file vary in length, turn on the **Use delimiters** option, and enter the type of character (delimiter) used to separate each field.

   By default, the option is turned on, and the delimiter specified is a semi-colon (;). If your source text file is made up of fixed length fields, turn off the **Use delimiters** option. Security Center supports the following delimiters:

   - Colon (:)
   - Comma (,)
   - Semi-colon (;)
   - Tab (type “Tab”)

   IMPORTANT: If your source list file uses tab as a delimiter, only use one tab space. Do not use more than one Tab space to align columns in your file, or Security Center might be unable to parse the hotlist.
6. (Optional) To prohibit users from editing this hotlist in Security Desk, turn off the **Visible in editor** option.

   To edit a hotlist in Security Desk, users require the *Hotlist and permit editor* privilege.
7. Configure the hotlist **Attributes** options and click **Next**.

8 On the *ALPR Manager assignment* page, choose an ALPR Manager, and then click **Next**.

   - **All ALPR Managers**: All ALPR Managers, and any entities configured to inherit hotlists from them, synchronize the new hotlist.

     NOTE: Future ALPR Managers do not automatically synchronize the new hotlist.
   - **Specific ALPR Managers**: Only the selected ALPR Managers, and the entities that inherit hotlists from them, synchronize the new hotlist.

     NOTE: Entities created in the future that are configured to inherit hotlists from one of the selected ALPR Managers also synchronize the hotlist.
   - **Assign later**: No existing ALPR Managers or associated entities synchronize the new hotlist.

9 On the *Unit specific assignment* page, select the specific patrol vehicles and Sharp units that will synchronize the new hotlist, and click **Next**.

10 (Optional) If your hotlist has custom fields, enter the appropriate values on the *Custom fields* page and click **Next**.

   The *Custom fields* page only appears if there are custom fields in your hotlist.

11 In the *Creation summary* window, verify that your hotlist information is correct and click **Next**.

   In the *Entity creation outcome* window, you receive a notification indicating whether or not your operation is successful.

12 (Optional) Edit or create a second hotlist:

   - **Edit this hotlist**: Open the *Hotlist and permit editor* task so you can edit the hotlist if you have the *Hotlist and permit editor* privilege.
   - **Create a hotlist based on this hotlist**: Create a new hotlist that uses the same settings as the hotlist you just created. You only need to specify the **Entity name**, **Entity description**, and **Hotlist path**.

13 Click **Close**.

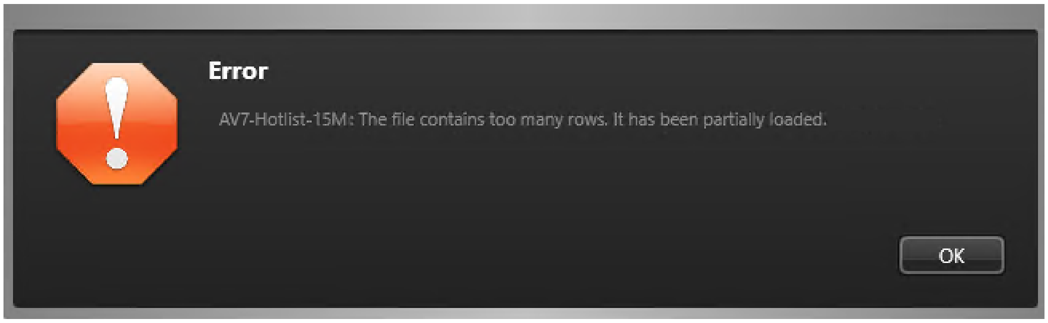
The hotlist entity is configured and enabled in Security Center.

Editing hotlists

From the *Hotlist and permit editor* task, you can add, remove, or edit entries in your hotlists.

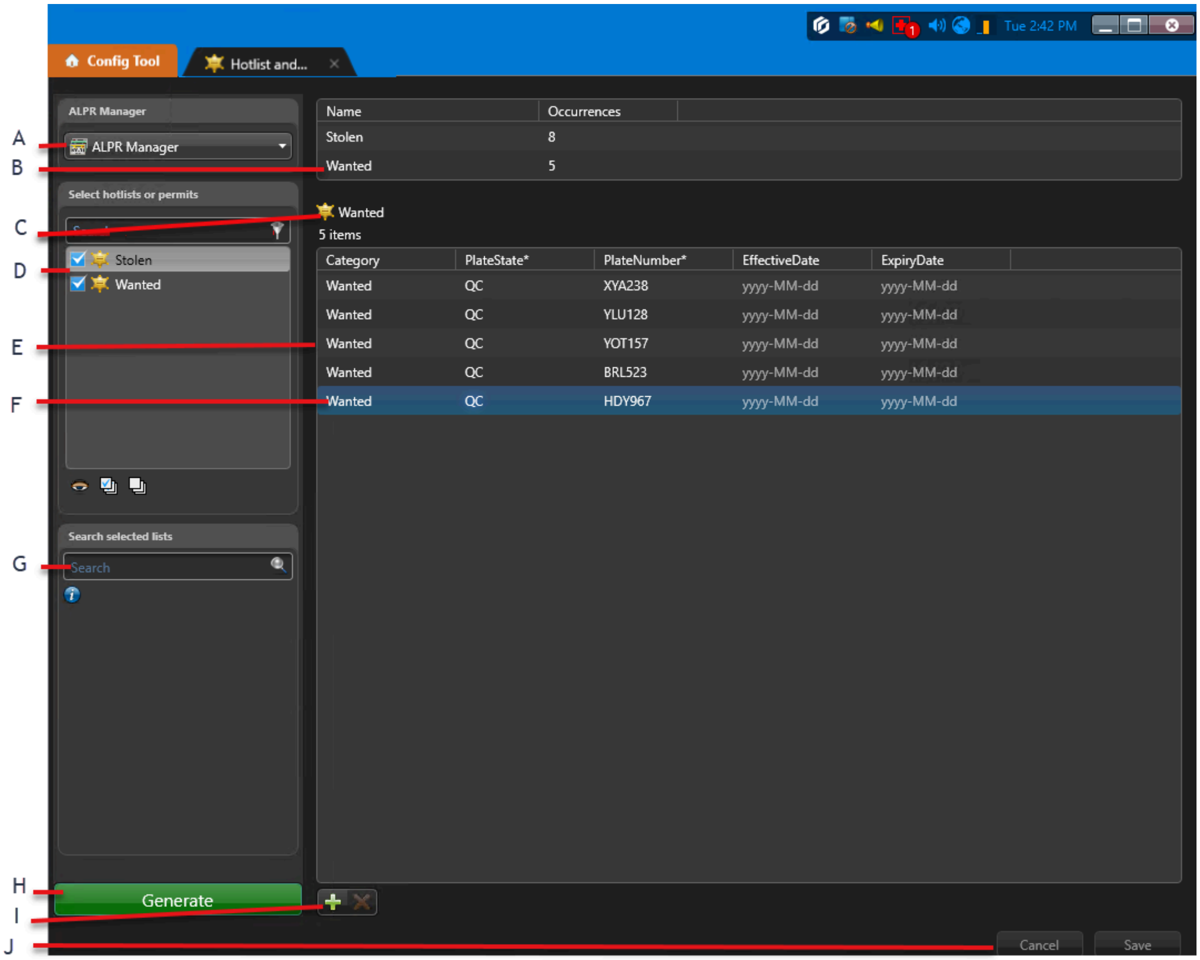
What you should know

- When you edit a hotlist in Config Tool, the linked source .txt file or .csv file is automatically updated. Likewise, if you edit the source file, the Config Tool hotlist is automatically updated.
- To edit a hotlist, you must have the *Add entries*, *Delete entries*, and *Modify entries* privileges for hotlists and permit lists.
- If a hotlist has more than 100000 records, an error message is displayed to inform that the hotlist is only partially loaded.



Error

AV7-Hotlist-15M: The file contains too many rows. It has been partially loaded.



Name	Occurrences
Stolen	8
Wanted	5

Wanted
5 items

Category	PlateState*	PlateNumber*	EffectiveDate	ExpiryDate
Wanted	QC	XYA238	yyyy-MM-dd	yyyy-MM-dd
Wanted	QC	YLU128	yyyy-MM-dd	yyyy-MM-dd
Wanted	QC	YOT157	yyyy-MM-dd	yyyy-MM-dd
Wanted	QC	BRL523	yyyy-MM-dd	yyyy-MM-dd
Wanted	QC	HDY967	yyyy-MM-dd	yyyy-MM-dd

A	List of ALPR Managers.
B	Summary pane displaying selected hotlists and permits.
C	Name of the hotlist selected in the summary pane.
D	Available hotlists and permits.
E	Details pane displaying all entries of the hotlist selected in the summary pane.
F	An entry in your hotlist. You can modify or delete entries in a hotlist or permit list.
G	Search for a keyword across selected hotlists or permit lists. You can search for a specific date, plate state, plate number, and so on.
H	Generate selected hotlists or permit lists.
I	Add or delete the selected row from the list.
J	Save or cancel your changes.

NOTE: To display hotlists through advanced search, you can click and apply the required filters. For more information, see Searching for entities using the search tool on page 80.

To edit a hotlist:

1 Open the *Hotlist and permit editor* task.

TIP: You can open the task by navigating to **ALPR** > **Hotlists** then clicking **Edit hotlist** (✎).

2 Select required hotlists or permits and click **Generate**.

In the main pane, the following information is displayed:

- Summary pane: Lists selected hotlists along with the number of entries in each hotlist.
- Details pane: Shows entries of the hotlist highlighted in summary pane.

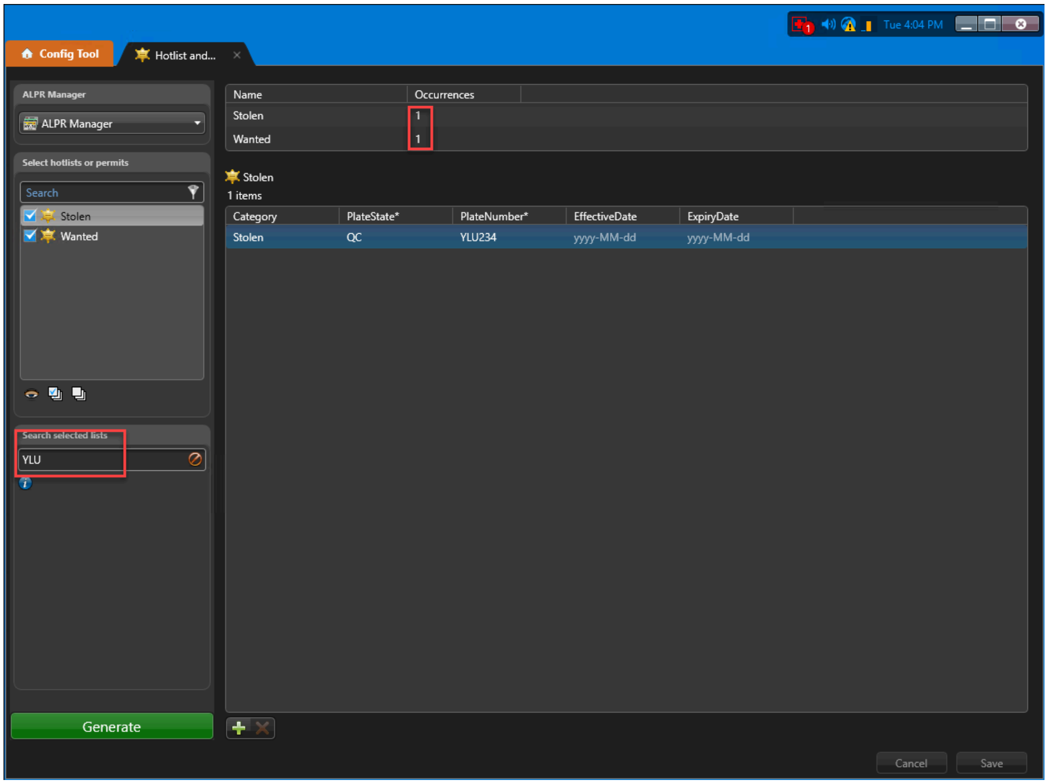
NOTE: The summary pane is displayed only if multiple hotlists are selected.

3 (Optional) Under the *Search selected lists* section, enter the value you want to search for in the **search box**. You can search for any value, for example, a specific license plate in both stolen and wanted hotlist.

NOTE: The search returns any matching strings in any of the hotlist columns. For example, if you search for *December (12)* in a numeric format, a license plate XYZ**12**3 is also displayed in the results.

The hotlist and permit task is updated as follows:

- Summary pane: Lists selected hotlists along with the frequency of the search phrase in each hotlist.
- Details pane: Shows all entries of the search phrase present in the hotlist highlighted in summary pane.



Name	Occurrences
Stolen	1
Wanted	1

Stolen

1 items

Category	PlateState*	PlateNumber*	EffectiveDate	ExpiryDate
Stolen	QC	YLU234	yyyy-MM-dd	yyyy-MM-dd

Search selected lists: YLU

4 From the *Hotlist and permit editor* task, you can:

- Add (✚) or remove (✖) vehicle entries.
- Edit vehicle entries within a hotlist by double clicking on the desired cell.
- Right-click entries to copy, cut, and paste between hotlists.

  NOTE: You can only move entries within the same *Hotlist and permit editor* task. If you have two tasks open, you cannot paste between them.

5 Click **Save**.

The hotlist and source file are updated and the changes are applied for new license plate reads in Security Center.

Selecting which hotlists and permits a patrol vehicle monitors

For hotlists and permit lists to be monitored by patrol vehicles, they must be activated and managed by at least one ALPR Manager.

What you should know

- The ALPR Manager sends the active hotlists and permit lists to the patrol vehicles it manages.
- The ALPR Manager matches the hotlists against the reads collected from Sharp cameras to produce hits.
- When you create a new hotlist or permit list, they are active for all ALPR Managers by default.
- Only patrol vehicles configured for parking enforcement require permits.
- You can associate permits to individual patrol vehicles. You can associate hotlists to individual patrol vehicles and Sharp units.

To select which hotlists and permit lists to monitor:

1. From the Config Tool home page, click **System** > **Roles**, and then click the ALPR Manager you want to configure.
2. Click the **Properties** tab.
3. Under **File association**, select the hotlists and permits you want the ALPR Manager to manage.
4. Click **Apply**.

Installing the Hotlist Permit File Updater plugin

For AutoVu™ Managed Services (AMS) systems that are hosted on Microsoft's Azure cloud platform, installing the *Hotlist Permit File Updater* plugin lets you push updated hotlists and permits to the cloud where they can then be downloaded on patrol vehicles.

What you should know

AMS allows you to quickly deploy an automatic license plate recognition (ALPR) system by reducing the need for on-site IT infrastructure and support. With AMS, your ALPR system is hosted in the cloud and experts from Genetec Inc. configure and maintain it.

To install and configure the Hotlist Permit File Updater plugin:

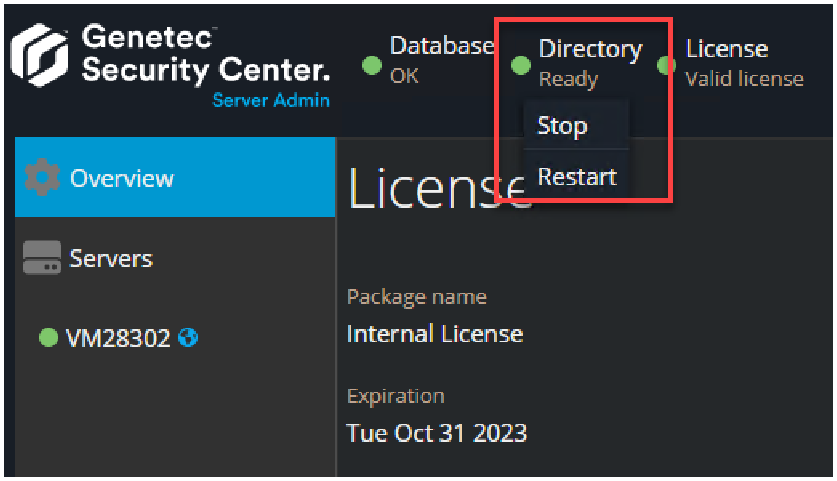
1 Download the Hotlist Permit Updater package, which is available at http://downloadcenter.genetec.com/products/AutoVu/Tools/HotlistPermitUpdater.zip.

2 To install the plugin, open the Hotlist Permit Updater package and double click the *Genetec.CS.HotListPermitFileUpdater.Setup* MSI file and follow the instructions in the installer.

3 Restart the Security Center Directory role, as follows:

a) From a web browser, open Server Admin typing http://<server>/genetec.

b) Click **Directory** and select **Restart**.



License

Package name
Internal License

Expiration
Tue Oct 31 2023

c) After the Directory restarts, close Server Admin.

4 Create the required custom events.

a) From the Config Tool, open the *System* task, click the **General settings** view, and go to the *Events* page.

b) Click **Add an item** (➕).

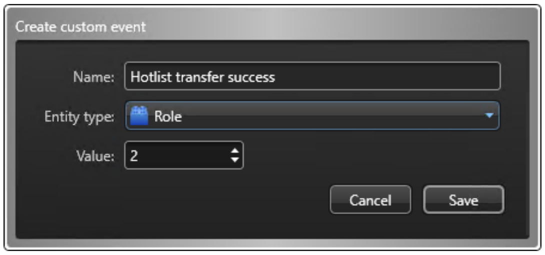
c) In the **Create custom event** dialog box, enter the **Name** *Hotlist transfer success*.

d) From the **Entity type** list, select **Role**.

e) In the **Value** field, type a unique number to identify this custom event from other custom events.

NOTE: These values are not related to the logical IDs of entities.

f) Click **Save** > **Apply**.



Create custom event

Name: Hotlist transfer success

Entity type: Role

Value: 2

g) Using these steps, create two additional events:

- *Hotlist transfer failure*
- *Hotlist start transfer trigger*

5 Install the *Raise custom event* macro so that Security Center can trigger the custom events.

a) From the Config Tool home page, open the *System* task, and click the **Macros** view.

b) Click **Macro** (✚), and name the new macro *Raise custom event*.

c) Click the **Properties** tab.

d) Click **Import from file**, navigate to the *RaiseCustomEventMacro* TXT file that is included in the package, and click **Open**.

The TXT file contains the following script:

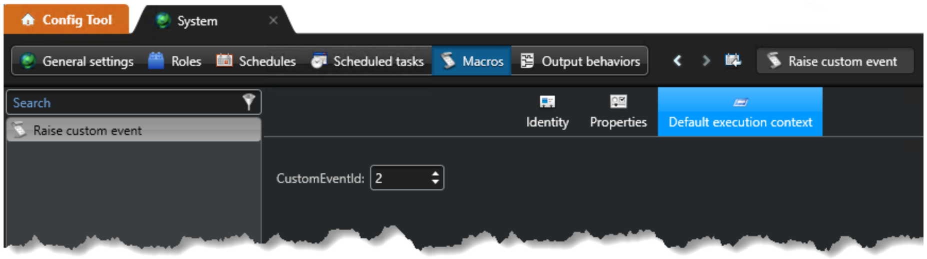
```
// ==========================================================================
// Copyright (C) 2013 by Genetec, Inc.
// All rights reserved.
// May be used only in accordance with a valid Source Code License Agreement.
// ==========================================================================
using Genetec.Sdk;
using Genetec.Sdk.Entities;
using Genetec.Sdk.Entities.CustomEvents;
using Genetec.Sdk.Queries;
using Genetec.Sdk.Scripting;
using Genetec.Sdk.Diagnostics.Logging.Core;
using System;
using System.Collections.Generic;
using System.Data;
using System.IO.Ports;
using System.Linq;
using System.Text;
using System.Threading;
namespace RaiseCustomEvent
{
    public class RaiseCustomEvent : UserMacro
    {
        public int CustomEventId { get; set; }
        public RaiseCustomEvent()
        {
            CustomEventId = 0;
        }
        public override void Execute()
        {
            try
            {
                if (CustomEventId > 0)
                {
                    Sdk.ActionManager.RaiseCustomEvent(new
 CustomEventId(CustomEventId),
                       SdkGuids.SystemConfiguration);
                }
            }
            catch (Exception)
            {
            }
        }
        protected override void CleanUp()
        {
        }
    }
}
```

a) Click **Apply** to save the macro.

b) Click the **Default execution context** tab.

c) In the *Custom event ID* field, enter the **Value** that you configured for the *Hotlist start transfer trigger* event.

d) Click **Apply**.



CustomEventId: 2

6 Create a scheduled task to start the file transfer.

a) From the Config Tool home page, open the *System* task, and click the **Scheduled tasks** view.

b) Click **Scheduled task** (+).

A new scheduled task entity is added in the entity list.

c) Name the task *Trigger hotlist update*.

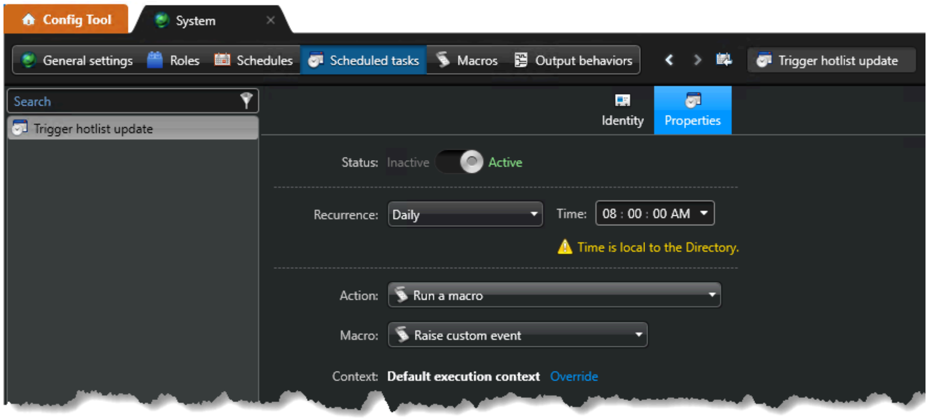
d) Click the **Properties** tab, and set the **Status** option to **Active**.

e) Set the **Recurrence** of the task, for example, daily at 8:00 am.

f) From the **Actions** list, select *Run a macro*.

g) From the **Macro** list, select the *Raise custom event* macro you created.

h) Click **Apply**.



Status: Inactive Active

Recurrence: Daily

Time: 08 : 00 : 00 AM

⚠ Time is local to the Directory.

Action: Run a macro

Macro: Raise custom event

Context: Default execution context

7 Install the *Hotlist permit file updater* macro.

a) From the Config Tool home page, open the *Plugins* task.

b) Click **Add an entity** (+) and select **Plugin**.

c) From the *Creating a role* wizard, install the *Hotlist Permit File Updater* plugin.

d) The Hotlist Permit File Updater is added to the plugins list. Select it and click the **Properties** tab.

e) Configure the plugin to use the HTTP, FTP, or SFTP transfer method

HTTP or FTP:

- Enter the remote URL where the file to download is located. Enter the credentials if needed. If the source is not secured using a username and password, leave the fields blank.

SFTP:

- **Host:** Enter the host using the following formatting:
  - sftp://(hostname or IP):(port)
  - sftp://(hostname or IP) If you do not specify a port, the default port 22 is used.
  - (hostname or IP) If you do not specify a protocol, the host name uses SFTP.
- **File path:** Enter the file path of the hotlist or permit.

  NOTE: The file path is relative to the home directory of the connected user on the SFTP server.
- **Connection mode:** Select the connection mode according to the SFTP site configuration and enter the **Username**, **Password**, and **Certificate path** according to your selection.

  NOTE:
  - The certificate must be located on the server on which the plugin is running and not the computer on which Config Tool is used.
  - The path must also reflect the location of the file on the server.
  - The certificate file should contain a private key in an OpenSSH format.
  - SSH-2 keys are supported. SSH-1 keys are unsafe and are not supported by the OpesSSh format.

f) From the **Hotlist/Permit** list, select the hotlist or permit you want to push to the patrol vehicles.

g) From the **Success event** list, select the *Hotlist transfer success* event you created.

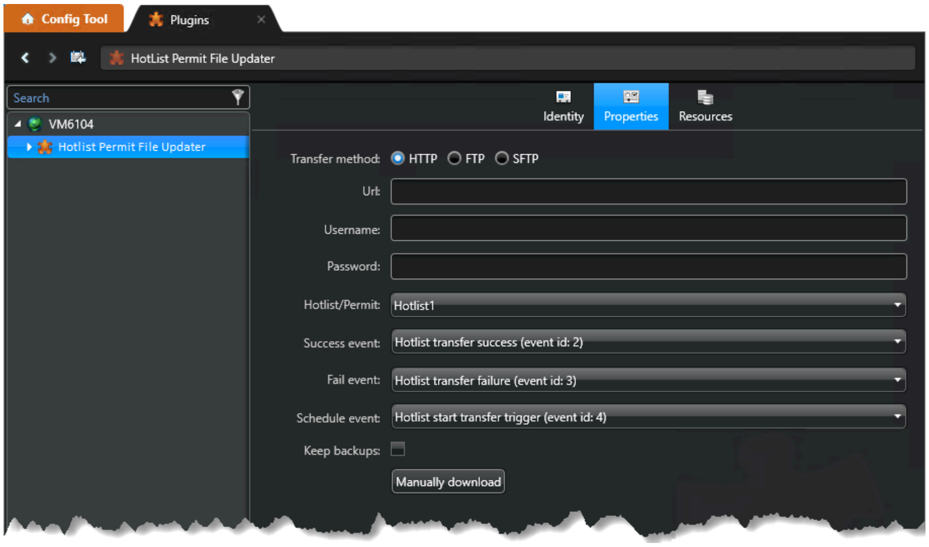
h) From the **Fail event** list, select the *Hotlist transfer failure* event you created.

i) From the **Schedule event** list, select the *Hotlist start transfer trigger* you created.

j) If you select **Keep backups**, the system creates a backup of the current hotlist or permit file before downloading the new one. The file name uses the original name + the current date and time + the .bak extension, for example, *hotlist2.tbl hotlist2.tbl 11-22-2017 11h10m55.bak*.

NOTE: To trigger the download immediately, click **Manually download**.

k) Click **Apply**.



Transfer method: ● HTTP ○ FTP ○ SFTP

Url:

Username:

Password:

Hotlist/Permit: Hotlist1

Success event: Hotlist transfer success (event id: 2)

Fail event: Hotlist transfer failure (event id: 3)

Schedule event: Hotlist start transfer trigger (event id: 4)

Keep backups: □

Filtering out invalid characters from hotlists and permit lists

When a hotlist or permit is created or modified, you can specify the character set that applies to the license plates in the list based on a selected language, and what the ALPR Manager does if it detects a list with invalid characters (non-alphanumeric characters).

What you should know

To view detailed information about how many invalid entries were deleted or modified, you can also save the logs of the filtering process.

To filter out plates when modifying hotlists and permit lists:

1. From the Config Tool home page, click **System** > **Roles**, and then click the ALPR Manager you want to configure.
2. Click the **Properties** tab.
3. Under **Plate filtering**, select the types of characters to filter on from the **Character set** list (Latin, Arabic, Japanese, Cyrillic, or Thai).
4. In the **Invalid plate number** section, select one of the following options to specify how the ALPR Manager handles invalid records:
   - **Modify record:** Modify any plate entries in memory with invalid characters such as spaces, dashes, ampersands and so on. For example, the plate number “ABC#%3” becomes “ABC3”.
   - **Remove record:** Remove from memory any plate entry with invalid characters. The plate number does not raise hits, even if it is in the list.

   NOTE: Regardless of the option selected, the original text file or CSV file does not get modified.
5. To log the filtering process, select the **Log filtering** option.

   The plate filtering logs will be saved in the AutoVu™ root folder: *C:\Genetec\AutoVu\RootFolder*.

   NOTE: There is no size limit for the log. It needs to be maintained, otherwise, the logs can occupy gigabytes of disk space.
6. Click **Apply**.

Adding privacy settings to license plate reads and hits

You can configure Genetec Patroller™ to obscure plate numbers, or to exclude plate, context, or wheel images from reads and hits that are received in Security Center, so that the information is not stored in the ALPR Manager database.

What you should know

Obscuring license plate numbers or excluding data from reads or hits allows you to comply with privacy laws in your region.

If you need to send an email with ALPR data to a specific recipient, then you can override the privacy settings for individual hotlists.

To add privacy settings to reads and hits:

1 From the Config Tool home page, click **ALPR** > **General settings** > **Applications**.

2 Under **Privacy**, turn **ON** the data types that you want to hide from reads and hits:

- **License plate, context, or wheel images:** Images are not sent to Security Center or included in offloaded data.
- **License plate:** Replaces the text string of the license plate number with asterisks (*) when sent to Security Center or in the offloaded data.

3 Click **Apply**.

Adding privacy settings to hotlists

To obscure license plate numbers, or exclude plate, context, or wheel images from reads and hits that are received in Security Center from a specific hotlist, you can set the hotlist as private.

Before you begin

You must obtain a special DLL file from Genetec Inc. For more information, contact your Genetec Inc. representative.

What you should know

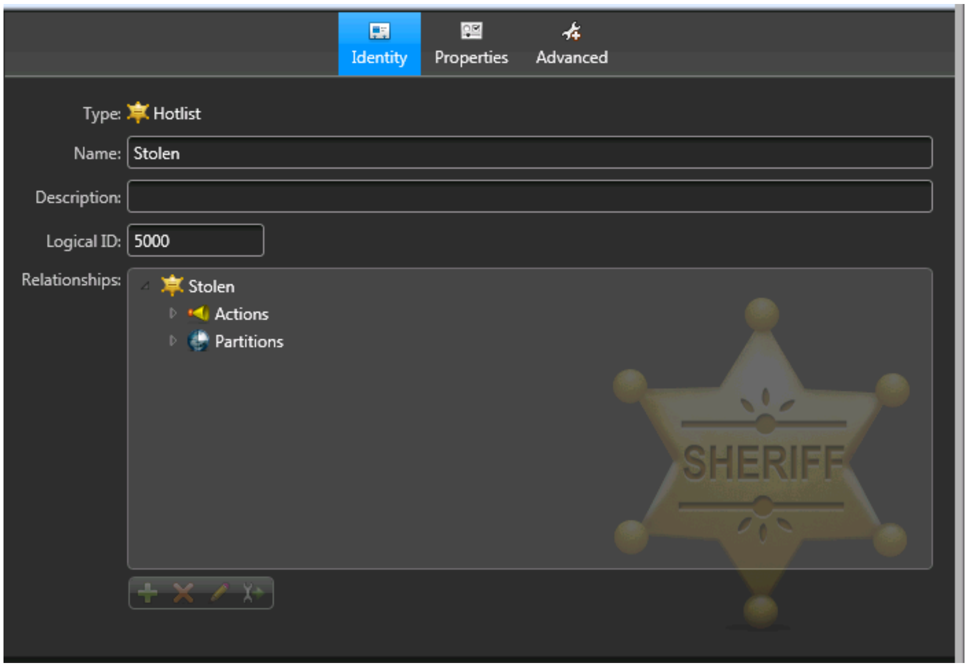
If you add privacy settings to a hotlist, Security Center keeps the ALPR data (for example, plate numbers, GPS coordinates, date/time, and so on), but disassociates that data from the hotlist that generated the hit. For example, if Genetec Patroller™ generates a hit from a hotlist called "StateWideFelons", you can keep all the ALPR data on that hit, but you won't be able to see that the matched license plate was on the "StateWideFelons" hotlist.

The privacy settings of specific hotlists take precedence over the global privacy settings configured at the ALPR Manager level. However, it is best practice to turn off all the privacy settings at the ALPR Manager level to avoid conflicts.

To add privacy settings to reads and hits:

1. Copy the DLL file you received from Genetec Inc. to the Security Center root folder (for example, *C:\Program Files\Genetec Security Center 5.11*).
2. Restart the Directory role from Server Admin, as follows:
   a) Open Internet Explorer.
   b) In the address bar, type *http://server IP address:port/Genetec* and press **Enter**.
   c) Log on to Server Admin.
   d) Under **Directory status**, click **Restart**.
3. From the Config Tool home page, click **ALPR** > **General settings** > **Applications**.
4. Under **Privacy**, turn **OFF** all the settings.
5. Click **Apply**.
6. From the home page, click **ALPR** > **Hotlists.**

7 Select the hotlist that you want to make private, and then click the **Identity** tab.



Type: Hotlist

Name: Stolen

Description:

Logical ID: 5000

8 In the **Logical ID** field, enter the value *5000*.

This marks the hotlist, and tells Security Center to make the ALPR data private.

9 Click **Apply**.

After you finish

Repeat for as many hotlists as you want.

Allowing users to edit hotlists and permits

When you are configuring properties of a hotlist or permit, you can select whether users are allowed to edit the list using the *Hotlist and permit editor* task in Security Desk.

What you should know

To edit a hotlist or permit list in Security Desk, users must have the *Hotlist and permit editor* privilege.

IMPORTANT: Please note the following about the Hotlist and permit editor:

- Only the first 100,000 rows of a list are loaded into the Hotlist and permit editor.
- If an error occurs while the hotlist is being loaded, the loading process is canceled and an error message is displayed. However, you will not lose any of the data loaded before the error occurred, and you can still edit the data loaded into the editor.

To allow users to edit hotlists and permits:

1. From the Config Tool home page, do one of the following:
   - Click **ALPR** > **Permits**, and select the permit to configure.
   - Click **ALPR** > **Hotlists**, and select the hotlist to configure.
2. Click the **Properties** tab.
3. Switch the **Visible in editor** option to **ON**, and click **Apply**.

Receiving notifications when hotlist hits occur

You can configure Security Center to send you an email notification when hotlist hits occur.

Before you begin

To make sure that the email notification is sent, do the following:

- Configure the mail server in the Server Admin - Overview page.
- Make sure the **Email notification** option is **ON** in the ALPR Manager - Properties tab.

What you should know

You can configure Security Center to send an email notification when either of the following occurs:

- When any license plate on a hotlist generates a hit.
- When an individual license plate on a hotlist generates a hit. You can specify a different email address for as many individual plates on a hotlist as you want.

The email contains the hit information (matched plate number, Genetec Patroller™ name, user, hotlist name, and priority) in the message body, and optional image attachments.

To receive notifications when a hotlist hit occurs:

1 From the Config Tool home page, click **ALPR** > **Hotlists**.

2 Select the hotlist you want to configure, and click the **Advanced** tab.

3 To add email addresses in **Email addresses** field:

   a) Click Add (✚).

   b) In the pop up window, enter the email address you want to notify.

      NOTE: If you are entering more than one email address, separate them with a comma.

   c) Click **OK**.

      NOTE: Duplicate email addresses are not added.

4 (Optional) To delete an email addresses from **Email addresses** list, select the email address and click Remove (✖).

   NOTE: You can only delete email addresses one at a time.

5 Click **Apply**.

   When any license plate in the selected hotlist generates a hit, a notification email is sent to the address you specified.

To receive notifications when a license plate generates a hit:

1 Add an email attribute to the hotlist as follows:

   a) From the Config Tool home page, click **ALPR** > **Hotlists**.

   b) Select the hotlist you want to configure, and click the **Properties** tab.

   c) Under **Attributes**, add a new email-related attribute (for example, *Email*) so that Security Center knows to look for email addresses in the hotlist's source file.

      NOTE: If you have multiple ALPR Manager roles enabled, the email attribute name must be the same for all ALPR Manager roles.

   d) Click **Apply**.

      Security Center will now look for email addresses in the hotlist source file.

2 Turn on **Email notification** and configure the related settings as follows:
   a) From the Config Tool home page, click **System** > **Roles**.
   b) Select the ALPR Manager you want to configure, click the **Properties** tab, and then click **Email notification**.
   c) In the **Email attribute name** field, type the same attribute name you created in the first step.
   d) (Optional) Under **Email attachments**, specify what information you want the email to contain.

      For example, you might want to send only the license plate text string without any images to keep the email's file size small.
   e) (Optional) In the **Log emails in** field, select where to store the email notification logs.

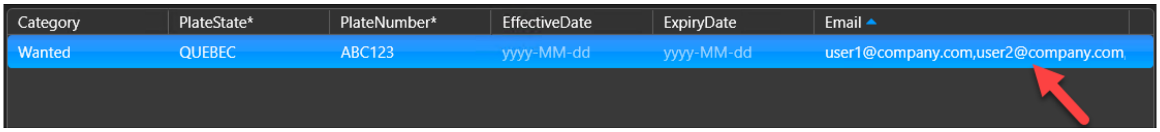
      The logs will be saved in the AutoVu™ root folder: *C:\Genetec\AutoVu\RootFolder*, and will help you keep track of who received email notifications.
   f) Click **Apply**.

      The ALPR Manager now knows that some hotlists contain email addresses for individual license plate entries.

3 Add email addresses in the hotlist source file.

   NOTE: Because you added the *Email* attribute to the hotlist entity, you can now use the *Hotlist and permit editor* to add email addresses. You can also add them directly to the source file if you prefer.
   a) From the Config Tool home page, click **Hotlist and permit editor**.

      NOTE: The **Visible in editor** option must be turned on to edit the hotlist.
   b) Select the hotlist you want to configure, then click **Load**.
   c) Click the email label.



Category	PlateState*	PlateNumber*	EffectiveDate	ExpiryDate	Email ▲
Wanted	QUEBEC	ABC123	yyyy-MM-dd	yyyy-MM-dd	user1@company.com,user2@company.com,

   d) In the pop up window, enter the email address you want to notify.

      NOTE: If you are entering more than one email address, separate them with a comma.
   e) Click Add (✚).
   f) (Optional) To delete email addresses from the list, select the email address and click Remove (✖).

      NOTE: You can only delete email addresses one at a time.
   g) Click **OK**.

      NOTE: Duplicate email addresses are not added.
   h) Click **Save**.

If a license plate with an email address generates a hit, an email is sent to the specified recipient.

Related Topics

Server Admin - Overview page on page 99
Allowing users to edit hotlists and permits on page 1000

Receiving *Match* and *No match* events in Security Desk

To receive *Match* and *No match* license plate events in Security Desk, you need to turn on hotlist matching. Sharp units can then match license plates against active hotlists and permit lists.

Before you begin

The hotlist or permit list must be active and managed by an ALPR Manager so that the events are monitored.

What you should know

When hotlist matching is enabled, you can configure event-to-actions in Security Desk, based on the following types of events:

- *Match* **event:** A license plate read by the Sharp is on a hotlist.
- *No match* **event:** A license plate read by the Sharp is not found on a specific hotlist.

Typically, *No match* events are used in access control scenarios. For example, you can associate a hotlist to a specific Sharp unit that monitors access to a parking lot or similar location. In this scenario, a Security Center event-to-action for a *License plate hit* event grants the vehicle access, such as opening a gate or raises a barrier. In the same scenario, an event-to-action for a *No match* event could trigger an alarm or send an email to security personnel.

To receive *Match* and *No match* events in Security Desk:

1. From the Config Tool homepage, click **System** > **Roles**.
2. Select the ALPR Manager that you want to configure, and then click the **Properties** tab.
3. Turn on the **Matching** option.
4. (Optional) To generate *No match* events when a Sharp unit reads a license plate that is not part of a hotlist or permit list, turn on the **Generate "No match" events** option.
5. Click **Apply**.

Wildcard hotlists

Wildcard hotlists contain entries with only partial license plate numbers. They can be used in situations where witnesses did not see or cannot remember the complete license plate number. This allows the officer to potentially intercept wanted vehicles that may not have been detected using standard hotlists.

A wildcard hotlist includes entries that have either one or two asterisks (*) in the license plate number field. The asterisks are the wildcards you use when you don’t know the character. Only the plate number field accepts wildcard characters. If the asterisk is found in any other field (for example, state or province), it is considered as a normal character.

Note the following about wildcard hotlists:

- If you activate wildcards on a hotlist, Genetec Patroller™ ignores all hotlist entries that do not contain a wildcard, or that have more than two wildcard characters.
- It is the number of wildcards in the *PlateNumber* field, and not the location of the wildcard character, that determines how many mismatched characters are allowed before a match can occur.
- The position of the wildcards cannot be enforced because, typically, when witnesses report a partial plate number, they do not remember the position of the characters they missed. The sequence of the normal characters in the *PlateNumber* is respected, such that the three patterns “S*K3*7”, “**SK37”, and “SK37**” are equivalent.

  If a wildcard hotlist contains the license plate entry S*K3*7:

  - Plate reads **N**SK3**5**7 and **A**S**D**K37 *will* generate a hit because both reads have no more than two mismatched characters (in bold) and the sequence “SK37” is respected.
  - Plate read SUKA357, *will not* generate a hit because it contains three mismatched characters (in red).
  - Plate read SKU573 read will not generate a hit because the sequence of characters SK37 is not found in the read.

BEST PRACTICE:

- Do not use more than one wildcard hotlist per Patroller.
- Use only one wildcard hotlist per ALPR Manager.
- Limit the number of wildcard entries in a hotlist to 100 plates.

Activating wildcard hotlists

To read partial license plates, you must set a hotlist as a wildcard hotlist.

Before you begin

The hotlist must be active and managed by an ALPR Manager.

To activate wildcard hotlists:

1 From the Config Tool home page, click **ALPR** > **Hotlists**, and then click the hotlist you want to configure.

2 Click the **Advanced** tab, and turn the **Use wildcards** option to **ON**.

3 Click **Apply**.

Related Topics

Wildcard hotlists on page 1004

Default hotlist and permit attributes

The following hotlist and permit attributes are created by default in Security Center:

- **Category (Mandatory):** The name of the parking permit. This field in the permit list's source text file *must* match the permit entity name exactly for the entry to be downloaded to Genetec Patroller™. If you have multiple categories in the same source file, you can use the same permit list for different permit entities in your system.

  For example, here is a simple permit list with three different permit categories (*Students*, *Faculty*, and *Maintenance)*. You can use this same permit list for three different permit entities (a *Students* permit entity, a *Faculty* permit entity, and a *Maintenance* permit entity) Each entity can point to the same source text file. Security Center extracts the license plates (and related information) whose category is the same as the name of the permit entity.

Category field	Students	QC;DEF228;2012-01-31;2012-05-31;PermitID_1
	Faculty	QC;345ABG;2012-01-31;2012-07-25;PermitID_2
	Maintenance	QC;244KVF;2012-01-31;2012-03-31;PermitID_3

- **PlateState (Optional):** Issuing state (or province, or country) of the license plate.
- **PlateNumber (Mandatory):** The license plate number.
- **EffectiveDate (Optional):** Date from which the permit on the list is valid.
- **ExpiryDate (Optional):** Date after which the permit is no longer valid.
- **PermitID (Optional -** *Shared permit enforcement, typically University Parking Enforcement and some City enforcement applications***):** Used when multiple entries in a permit list share the same permit (for example, car pool permits). Can be used to identify the number of the permit issued to the vehicle whose license plate is identified in *PlateNumber*. In the case of shared permits, normally up to four separate vehicles would all have the same permit number.

  A violation results in a *Shared Permit* hit in Patroller.

Related Topics

About permits on page 1137

Configuring hotlist and permit attributes

You must configure the attributes of a hotlist or permit in Security Center the way it is written in its source text file, so Genetec Patroller™ can parse the information in the list.

What you should know

- Hotlist and permit list text file must include the *Category*, and *PlateNumber* fields (attributes). These are mandatory fields, and they cannot be deleted.
- There cannot be any spaces within an attribute name.
- If you add additional attributes to a hotlist, they are automatically added as annotation fields when a hit occurs for the hotlist. For more information on annotation fields, see Adding user custom fields to license plate reads and hits on page 1110.

To configure hotlist or permit attributes:

1. From the Config Tool home page, do one of the following:

   If you are configuring attributes from the **Creating a hotlist** or **Creating a permit** wizard, skip ahead to Step 3.

   - Click **ALPR** > **Permits**, and select the permit to configure.
   - Click **ALPR** > **Hotlists**, and select the hotlist to configure.

2. Click the **Properties** tab.
3. Under the **Attributes** section, do one of the following:
   - To configure a default attribute, select it in the list, and click **Edit the item** (✏).
   - To add a new attribute, click **Add an item** (➕).
4. If you are adding a new attribute, type a **Name** for the attribute.

   The name can contain spaces.

5. If you want to use a default value for the field, type in the **Value** option.

   The default value is interpreted differently depending on whether delimiters are used or not.

   - If delimiters are used and you add a default value for this field, the populated field in the source file is overwritten.
   - If delimiters are not used and the field is empty in the source file, the default value you add here is used for the field. However, if the field is populated in the source file, it will not be overwritten.

6. If you are adding a new attribute and it is mandatory in the source file, turn on the **Is mandatory** option.

   Example: If you add a mandatory attribute called *CarColor*, the column for *CarColor* in the source file must have text in it.

7. To show additional attribute fields, click ⊕.
8. If the source file uses fixed length data fields instead of delimiters, switch the **Fixed length** option to **ON**, set the **Start** character position of the attribute in the file, and its **Length**.

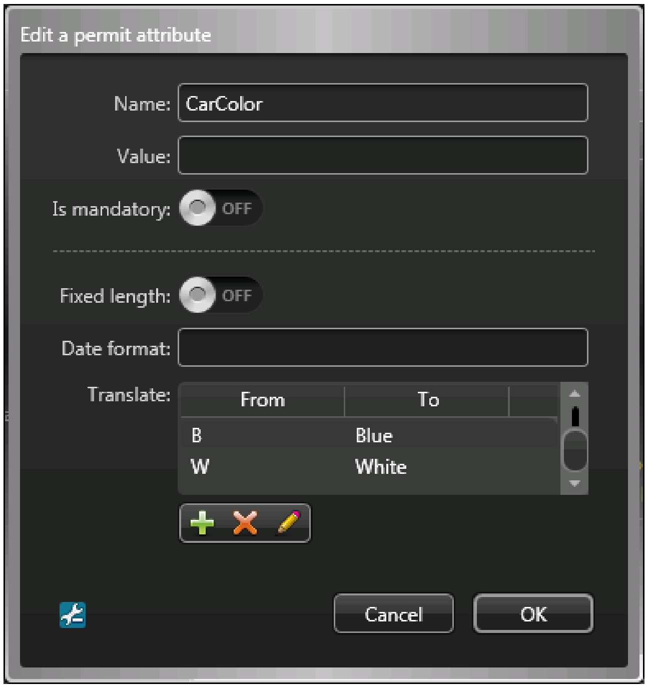
   The position of the first character in the source file is zero (0).

9. If the field contains a date or time value in the source file, specify a **Date format**.

   All standard date and time format strings used in Windows are accepted. If nothing is specified, the default time format is “yyyy-MM-dd”.

10 If you want to transform the values read from the data file, click **Add an item** (➕) under **Translate**, select a **From** and **To** value, and click **OK**.

Example: In the following example, the new field is CarColor and B will be translated to Blue and W will be translated to White.



Edit a permit attribute

Name: CarColor

Value:

Is mandatory: OFF

Fixed length: OFF

Date format:

Translate:

From	To
B	Blue
W	White

11 Click **OK**.

12 To delete an attribute that you are not using in the source file, select it in the list, and click **Delete** (✖).

Example: If the permits on your list don’t expire, you can delete the *ExpiryDate* attribute.

The attribute fields from your hotlist and permit list source text files should now match the attributes in the entity’s **Properties** tab. Patroller can now download the information from the list.

Example

The following source file uses variable field length data, and a semicolon (;) as a delimiter. It uses the following attributes: *Category*, *PlateState*, *PlateNumber*, *EffectiveDate*, *ExpiryDate*, and *PermitID*.

```
MyPermit;QC;DEF228;2012-01-31;2012-05-31;PermitID_1
MyPermit;QC;345ABG;2012-01-31;2012-07-25;PermitID_2
MyPermit;QC;067MMK;2012-03-31;2012-09-11;PermitID_1
MyPermit;QC;244KVF;2012-01-31;2012-03-31;PermitID_3
```

Related Topics

Default hotlist and permit attributes on page 1006

Configuring past-read matching on the ALPR Manager

When a hotlist is updated, the system can search the license plate reads in the ALPR Manager database to see if the new hotlist entries have been previously read.

Before you begin

Create a hotlist that will be used to trigger past-read matching.

What you should know

- You can trigger past read matching using a hot action, a scheduled task, or an event-to-action.
- In the Security Desk *Hits* report, hits that are generated using past-read matching are indicated in the *Post matched* column.
- If your system includes patrol vehicles, you can run past-read matching in Patroller. For more information, see the *Genetec Patroller™ Administrator Guide*.

To configure past-read matching on the ALPR Manager:

1 Associate the hotlists you want to manage with the ALPR Manager.

  NOTE: In later steps, you will select specific hotlists from this list on which to perform past-read matching.

  a) From the Config Tool home page, click **System** > **Roles**, and then click the ALPR Manager you want to configure.
  b) Click the **Properties** tab.
  c) Under **File association**, select the hotlists and permits you want the ALPR Manager to manage.
  d) Click **Apply**.

2 Enable past-read matching on the ALPR Manager role.

  a) Click the **Properties** tab.
  b) Turn the **Matching** option **ON**.
  c) (Optional) To generate *No match* events when a license plate is read by a Sharp and the plate is not part of a hotlist or permit list, turn the **Generate “No match” events** option to **ON**.

3 The **Past-read matching** section lists all of the hotlists that you have associated with the ALPR Manager role. Select the hotlists for which you want to enable past-read matching.

  NOTE: Federated hotlists are not supported by past-read matching and are therefore not displayed in the list.

4 In the **Search back time field**, set the time interval over which past-read matching takes place.

  NOTE: Performing past-read matching on many or large hotlists and using a long search back time can affect system performance.

5 Click **Apply**.

6 Trigger past-read matching using the following methods:

  - Create a scheduled task that uses the *Trigger past-read matching* action.
  - Create an event-to-action that uses the *Hotlist changed* event and the *Trigger past-read matching* action.
  - In Security Desk, create a hot action that uses the *Trigger past-read matching* action. For more information on creating hot actions, see the *Security Center User Guide*.

Related Topics

Scheduling a task on page 221

Creating event-to-actions on page 212

Using a hotlist when the ALPR Manager role is hosted on an expansion server

If the ALPR Manager role is hosted on a different server than the Directory role, both servers must have access to the hotlist file. The servers can either share the same hotlist file, or you can save an empty hotlist file on the Directory server.

What you should know

You can choose one of the following methods to manage your hotlist.

Sharing the hotlist file on a network drive that is accessible by both servers:

1 Save the hotlist TXT file on a network drive that is accessible from the ALPR Manager server and the Directory server.

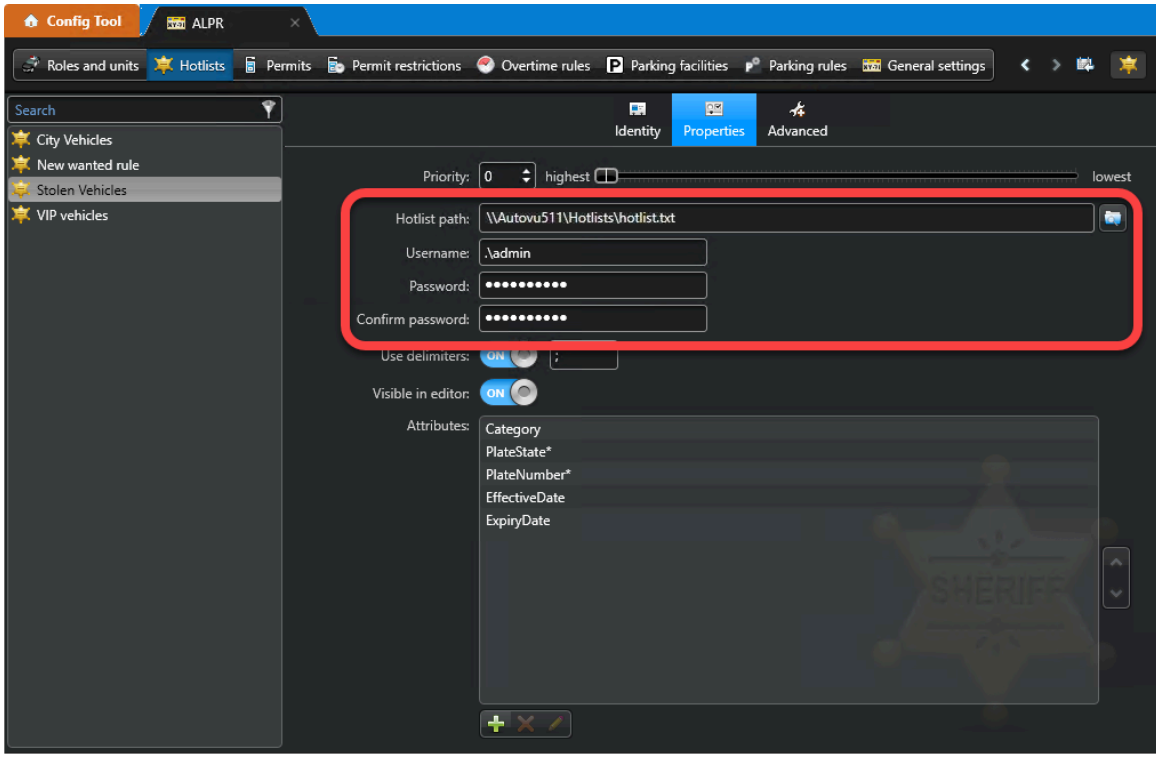
2 Share the directory containing the hotlist file. The directory must be accessible by both servers.

3 In the Security Center hotlist configuration, enter the path to the file as follows: *\\PCNAME\Directory\file.txt*.

NOTE: You can enter the path when creating the hotlist, or you can modify the path in the *Properties* tab of an existing hotlist entity.

4 Enter the credentials for the drive hosting the hotlist file.

5 Click **Apply**.



Priority: 0 highest lowest

Hotlist path: \\Autovu511\Hotlists\hotlist.txt

Username: .\admin

Password: •••••••••••

Confirm password: •••••••••••

Use delimiters: ON ;

Visible in editor: ON

Attributes: Category
PlateState*
PlateNumber*
EffectiveDate
ExpiryDate

Creating an empty hotlist:

1 Save the hotlist TXT file on the ALPR Manager server.

2 Save an empty TXT file with the same name on the Directory server.

IMPORTANT: The empty file must be in the same path location on both servers. For example, if the hotlist is in *C:\Hotlists* on the ALPR manager server, then the empty file on the Directory server must also be in *C:\Hotlists*.

Configuring advanced hotlist settings

The **Advanced** tab is where you configure hotlist properties such as the color of a hotlist hit and the sound file that plays when a hotlist hit occurs. These properties are not required for all hotlists, but allow you to customize hotlists for specific scenarios.

Before you begin

Create the hotlist.

To configure advanced hotlist settings:

1. From the Config Tool home page, click **ALPR** > **Hotlists**, and select the hotlist you want to configure.
2. Click the **Advanced** tab.
3. Beside **Color**, click the colored block and assign a new color to the permit.

   The map symbol that marks the location of the hotlist hit in Security Desk and Genetec Patroller™ will appear in that color, as well as in the *Hotlist Hit* and *Review Hits* screen in Patroller.
4. Turn on **Use wildcards** to activate wildcard hotlists.
5. Turn on **Covert** if you want to set the hotlist to a covert hotlist. When you choose this setting, Patroller users are not alerted when a hit occurs. Only users with sufficient privileges can view covert hits in Security Desk
6. Enter an **Email address** that receives a notification when the hotlist you're configuring generates a hit.
7. Enter the path for the **Sound file** Patroller plays when a hotlist hit occurs. If you leave this field blank, Patroller plays its default sounds. The path (you must include the filename) indicates the file's location on the Patroller in-vehicle computer.
8. Turn on **Override privacy for emails** if you want to bypass any privacy settings you applied at the Directory level, and send an email with real ALPR data to the email address you specified for this particular hotlist.
9. Turn on **Disable periodic transfer** if you only want permit changes to be downloaded to Patroller when the user logs on to the application. This option requires a wireless connection between Patroller and Security Center.

   Turn on **Enable transfer modification** if you want to transfer hotlist modifications to Patroller as soon as they occur. For example, you can use this option on a hotlist to force Patroller to query for changes more frequently than the periodic transfer period (which applies to all hotlists). This can be useful for Amber alerts because they can be added to a specific hotlist and sent to a Patroller almost immediately. This option requires a continuous wireless connection between Patroller and Security Center.

45

AutoVu third-party data exporter

This section includes the following topics:

About the AutoVu Third-party Data Exporter

The AutoVu™ Third-party Data Exporter is a feature that uses either an HTTPS or a SFTP connection protocol to securely export ALPR events, for example reads and hits, to external endpoints. The feature supports multiple file formats, such as XML, JSON, and others, to export the data.

Examples of exported reads and hits

- For examples of JSON files, see Examples of JSON files for the AutoVu third-party data exporter on page 1318.
- For examples of XML files, see Examples of XML files for the AutoVu third-party data exporter on page 1326.

License options for AutoVu Third-party Data Exporter

The data formats supported and the number of extra external endpoints vary depending on your license. By default, you can export an XML file of the ALPR events to a single external endpoint. The following table lists the supported data formats and the number of endpoints configurable per license option:

License option	Data format supported	Endpoints supported
None	XML	1
AU-PI-T2MEAEXPORT [1]	JSON2, XML	1
GSC-AV-MS-PI-T2MEAEXPORT [1, 2]	JSON2, XML	1
AU-PI-3RDPARTYEXPORTER-1X	JSON, JSON2, JSONLAP, UTMC, XML	1
GSC-AV-MS-PI-3RDPRTYEXPRT-1X	JSON, JSON2, JSONLAP, UTMC, XML	1
GSC-AV-PI-3RDPARTYEXPORTER-1X	JSON, JSON2, JSONLAP, UTMC, XML	1
AU-PI-3RDPARTYEXPORTER-3X	JSON, JSON2, JSONLAP, UTMC, XML	3
GSC-AV-MS-PI-3RDPRTYEXPRT-3X	JSON, JSON2, JSONLAP, UTMC, XML	3
GSC-AV-PI-3RDPARTYEXPORTER-3X	JSON, JSON2, JSONLAP, UTMC, XML	3

[1] Typically used with the T2 Systems Mobile Enforcement Application.

[2] Typically used with AutoVu Managed Services (AMS) systems.

Limitations

The following limitations apply:

- If a Genetec Patroller™ unit raises a covert hotlist hit, the event is exported twice.
- If you use XML or JSON file formats to export events, only the events generated by the Patroller contain a value in the address field.
- The feature exports at a rate of 20 events per second with an HTTPS connection, and 10 events per second with SFTP. If the total events per second exceed these rates, it is recommended to set the *Queueing protocol* to **High volume**.

- If a Patroller unit has more than 2000 events to offload, it is recommended to do one of the following:
  - Use an HTTPS connection to export the events.
  - Set the *Queueing protocol* to **High volume**.
- The license counter for the endpoints does not automatically update after adding the endpoints to the system.

  Workaround: Restart the Config tool to refresh the license counter.
- The feature does not currently export any AutoVu™ Free-Flow related events.
- The maximum number of endpoints per ALPR role is nine.

Related Topics

Examples of XML files for the AutoVu third-party data exporter on page 1326

Examples of JSON files for the AutoVu third-party data exporter on page 1318

Configuring the HTTPS endpoint to export read and hit events

You must configure the ALPR manager role to export a license plate read or hit event automatically to the required HTTPS endpoint.

Before you begin

- Ensure that your Security Center license has a valid certificate for the AutoVu™ third-party data exporter plugin integration. For more information about licenses, see "About AutoVu third-party data exporter" in the *Security Center Administrator Guide*.
- To configure a secure connection, you must have all the required information from the corresponding third-party API.
- Ensure that the server firewall rule is updated with the port number specified by the third-party API.
- To set the *Queueing protocol* to **High volume**, ensure that the system uses **RabbitMQ**. For more information, see High-volume data export using RabbitMQ on page 1019.

  NOTE: If you already have a **RabbitMQ** installed for another Genetec™ application, you can use the same credentials and TLS certificates to export high volumes of data.

To export reads and hits to external third-party systems:

1 From the Config Tool homepage, click **System** > **Roles**, and then click the ALPR Manager you want to configure.

2 Click the **Properties** tab and enable the **Data Exporter** option.

3 Select the required *Queueing protocol* from the drop down menu.

  - **Standard:** This is the default mode.
  - **High volume:** Select this mode if you need to export a high volume of events.

    NOTE: In the *Communication settings* pop-up window, enter the details configured in the **RabbitMQ** installation.

4 Click ➕ and select the required secure connection type from the list.

5 In the *Parameters* section, configure the following:

  - **Endpoint name:** Enter a relevant name for the required third-party server.
  - **Server URL:** Enter the IP address of the third-party server. You can also add URL parameters that are required, for example, `https://server:5001/api/json?params1=test1&params2=test2`.

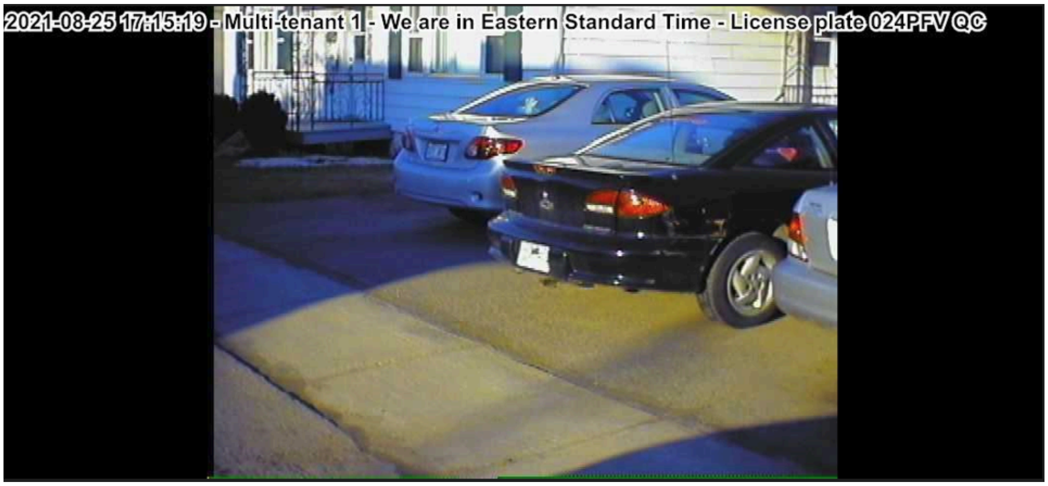
    NOTE: The default port for the server URL is 443. To override the default value, add the required port to the server URL. For example, to use port 5001, enter the IP address as `https://server:5001/api/`.
  - **Export format:** Select the format in which the data needs to be exported.

- XML: Export reads and hits in XML format.
- JSON: Export reads and hits in JSON format.
- UTMC: Export reads in UTMC format supported in Europe.
- JSON2: Export hits to a T2 ticketing system.
- JSONLAP: Export reads in a JSON format supported by Brazil municipalities.

6 (Optional) If the *Export format* selected in step 4 is **XML** or **JSON** or **JSON2**, configure the following settings in the *File format-specific* section:

- **Customer ID:** Enter the value provided by the customer.

  NOTE: This section is displayed only if *Export format* selected is **JSON2**.
- **What to export:** Select the events that you want to export.
- **Export settings:** Choose the export settings as required.
  - **Export images:** Select this option to export the images along with the read or hit.
  - **Enforced hits only:** Select this option to export enforced hits.
  - **Add watermarks to context images:** Select this option to add watermark to context images. To better suit your requirements, you can customize the variables in the following ways.
    - Modify the variables. For example, you can add **{timezone}** to the template.
    - Arrange the order of the variables. For example, you can add **{timezone}** at the start of the template.
    - Add words to provide more information. For example, you can add **We are in** before {timezone} to provide more context about the timezone.


2021-08-25 17:15:19 - Multi-tenant 1 - We are in Eastern Standard Time - License plate 024PFV QC

  - **Date format:** Select how you want the date to appear in exported license plate reads. The following formats are available:
    - MM/dd/yyyy
    - MM-dd-yyyy
    - dd/MM/yyyy
    - dd-MM-yyyy
    - yyyy/MM/dd
    - yyyy-MM-dd
- **Critical:** Select the events that you want to resend after an export operation fails.
  - **Reads:** Select this option to resend any reads.
  - **Hits:** Select this option to resend any hits.

  NOTE: The AutoVu third-party data exporter retries until the event is successfully exported or a long list of events need to be resent.

7 (Optional) If the *Export format* selected in step 4 is **JSONLAP**, configure the following settings in the *File format-specific* section:
   - **Company code:** Enter the value provided by third-party API.
   - **Contract code:** Enter the value provided by third-party API.

8 In the **Authorization** section, configure the following settings:
   NOTE: This section is displayed only if *Connection type* selected is **Https**.
   - **Authorization mode:** Choose the authorization mode as required.
     - **None:** Select this option if the third-party system does not require any specific authorization method.
     - **Certificate:** Select this mode if the third-party system uses **TLS** certificate.
     - **PasswordGrant:** Select this mode if the third-party system uses **PasswordGrant** token.
     - **Client Credentials:** Select this mode if the third-party system uses **Client Credentials** token.
   - **Client certificate:** Enter or browse the path to the TLS certificate provided by third-party API.
     NOTE: This parameter is displayed only if *Certificate* authorization mode is selected.
   - **Token URL:** Enter the value provided by third-party API.
   - **Client ID:** Enter the value provided by third-party API.
   - **Client secret:** Enter the value provided by third-party API.
   - **Username:** Enter the value provided by third-party API.
   - **Password:** Enter the value provided by third-party API.
   - **Scope:** Enter the value provided by third-party API.
     NOTE: If no value is provided, the field can be left empty.

9 Click **Apply**.

Configuring the SFTP endpoint to export read and hit events

You must configure the ALPR manager role to automatically export a license plate read or hit event to the required SFTP endpoint.

Before you begin

- Ensure that your Security Center license has a valid certificate for the AutoVu™ third-party data exporter plugin integration. For more information about licenses, see "About AutoVu third-party data exporter" in the *Security Center Administrator Guide*.
- To configure a secure connection, you must have all the required information from the corresponding third-party API.
- Ensure that the server firewall rule is updated with the port number specified by the third-party API.
- To set the *Queueing protocol* to **High volume**, ensure that the system uses **RabbitMQ**. For more information, see High-volume data export using RabbitMQ on page 1019.
  NOTE: If you already have a **RabbitMQ** installed for another Genetec™ application, you can use the same credentials and TLS certificates to export high volumes of data.

To export reads and hits to external third-party systems:

1 From the Config Tool home page, click **System** > **Roles**, and then click the ALPR Manager you want to configure.

2 Click the **Properties** tab and enable the **Data Exporter** option.

3 Click + and select the required secure connection type from the list.
   - **Standard:** This is the default mode.
   - **High volume:** Select this mode if you need to export a high volume of events.

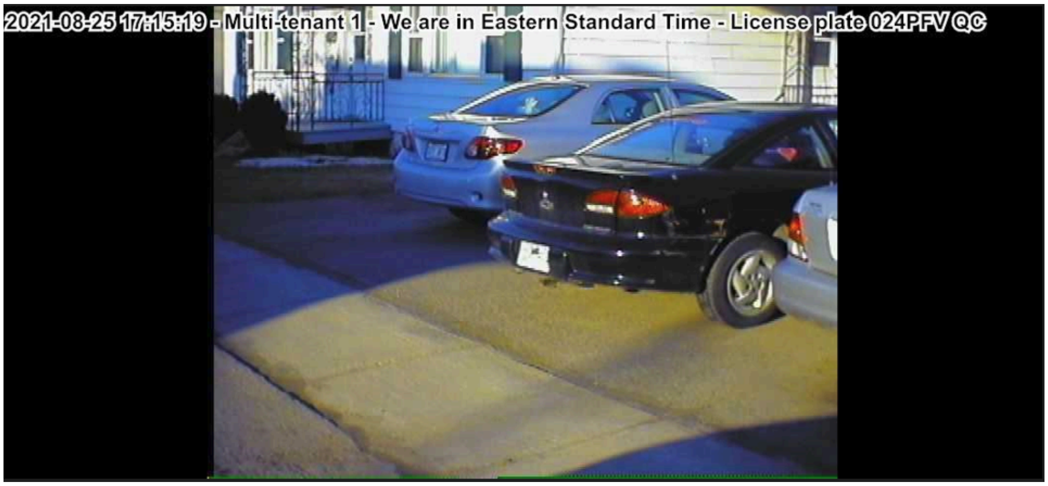
NOTE: In the *Communication settings* pop up window, enter the details configured in the **RabbitMQ** installation.

4. In the *Parameters* section, configure the following:
   - **Endpoint name:** Enter a relevant name for the required third-party server.
   - **Destination folder:** Enter the path of the destination folder on the third-party server.
   - **File name template:** (Optional) Enter a relevant value for the ExportData field. For example, if you are exporting all hit events, you can change the template from ExportData_{type}_{date}_{time} to Hits_{type}_{date}_{time}.

     NOTE: At the time of export, the system generates file names based on the template displayed. The placeholders such as type, date, and time are automatically replaced with the corresponding real time values.
   - **Export format:** Select the format in which the data needs to be exported.
     - XML: Export reads and hits in XML format.
     - JSON: Export reads and hits in JSON format.
     - UTMC: Export reads in UTMC format supported in Europe.
     - JSON2: Export hits to a T2 ticketing system.
     - JSONLAP: Export reads in a JSON format supported by Brazil municipalities.

5. (Optional) If the *Export format* selected in step 4 is **XML** or **JSON** or **JSON2**, configure the following settings in the *File format-specific* section:
   - *Customer ID*: Enter the value provided by the customer.

     NOTE: This section is displayed only if *Export format* selected is **JSON2**.
   - *What to export*: Select the events you want to export.
   - **Export settings:** Choose the export settings as required.
     - **Export images:** Select this option to export the images along with the read or hit.
     - **Enforced hits only:** Select this option to export enforced hits.
     - **Add watermarks to context images:** Select this option to add watermark to context images. To better suit your requirements, you can customize the variables in the following ways.
       - Modify the variables. For example, you can add **{timezone}** to the template.
       - Arrange the order of the variables. For example, you can add **{timezone}** at the start of the template.
       - Add words to provide more information. For example, you can add **We are in** before {timezone} to provide additional context about the timezone.


2021-08-25 17:15:19 - Multi-tenant 1 - We are in Eastern Standard Time - License plate 024PFV QC

     - **Date format:** Select how you want the date to appear in exported license plate reads. The following formats are available:

        - MM/dd/yyyy
        - MM-dd-yyyy
        - dd/MM/yyyy
        - dd-MM-yyyy
        - yyyy/MM/dd
        - yyyy-MM-dd
    - **Critical:** Select the events you want to resend after an export operation fails.
        - **Reads:** Select this option to resend any reads.
        - **Hits:** Select this option to resend any hits.

      NOTE: The AutoVu third-party data exporter will retry until the event is successfully exported or more than 1000 events need to be resent.

6 (Optional) If the *Export format* selected in step 4 is **JSONLAP**, configure the following settings in the *File format-specific* section:

- *Company code***:** Enter the value provided by third-party API.
- *Contract code***:** Enter the value provided by third-party API.

7 (Optional) In the **Connection settings** section, configure the following settings:

NOTE: This section is displayed only if *Connection type* selected is **Sftp**.

- **Hostname or IP:** Enter the hostname or IP address of the destination.
- **Port:** Enter the port number of the destination address.
- **Username:** Enter the value provided by third-party API.
- **Password:** Enter the value provided by third-party API.
- **SSH Key:** Enter the value provided by third-party API.

  NOTE: If no value is provided, the field can be left empty.
- **SSH passphrase:** Enter the value provided by third-party API.

  NOTE: If no value is provided, the field can be left empty.

8 Click **Apply**.

High-volume data export using RabbitMQ

If you select the **High Volume** option in the Third-Party Data Exporter configuration, you must also connect to an instance of RabbitMQ queuing software. RabbitMQ is a message broker that routes data using a messaging queue. It can either be hosted on the same network or it can be a cloud version.

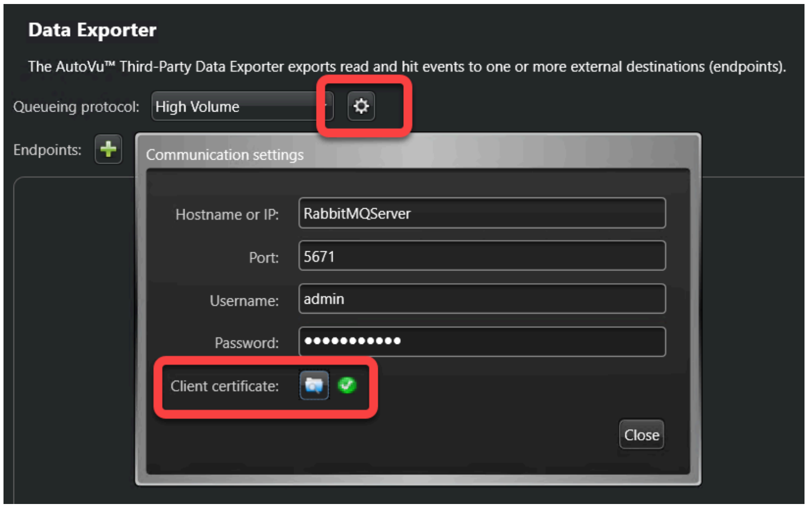
To enable the high-volume queuing, navigate to **System** > **Roles** > **ALPR Manager** > **Data Exporter**, and set the **Queuing Protocol** to **High Volume**.

RabbitMQ on a local network

You can install RabbitMQ on a server on your local network, however, you must consider the following:

- The RabbitMQ installation can be long and complex compared to the cloud offering option.
- The RabbitMQ instance needs to be monitored and updated regularly to make sure that no security issues are discovered over time.
- RabbitMQ requires disk space to store the data that is waiting to be exported to the endpoint.

If you are using a local instance of RabbitMQ, HTTPS mode must be configured, and the TLS certificate used for the HTTPS must be used in the *Communication settings*.



Data Exporter

The AutoVu™ Third-Party Data Exporter exports read and hit events to one or more external destinations (endpoints).

Queueing protocol: High Volume

Endpoints:

Communication settings

Hostname or IP: RabbitMQServer

Port: 5671

Username: admin

Password: ●●●●●●●●●●●●

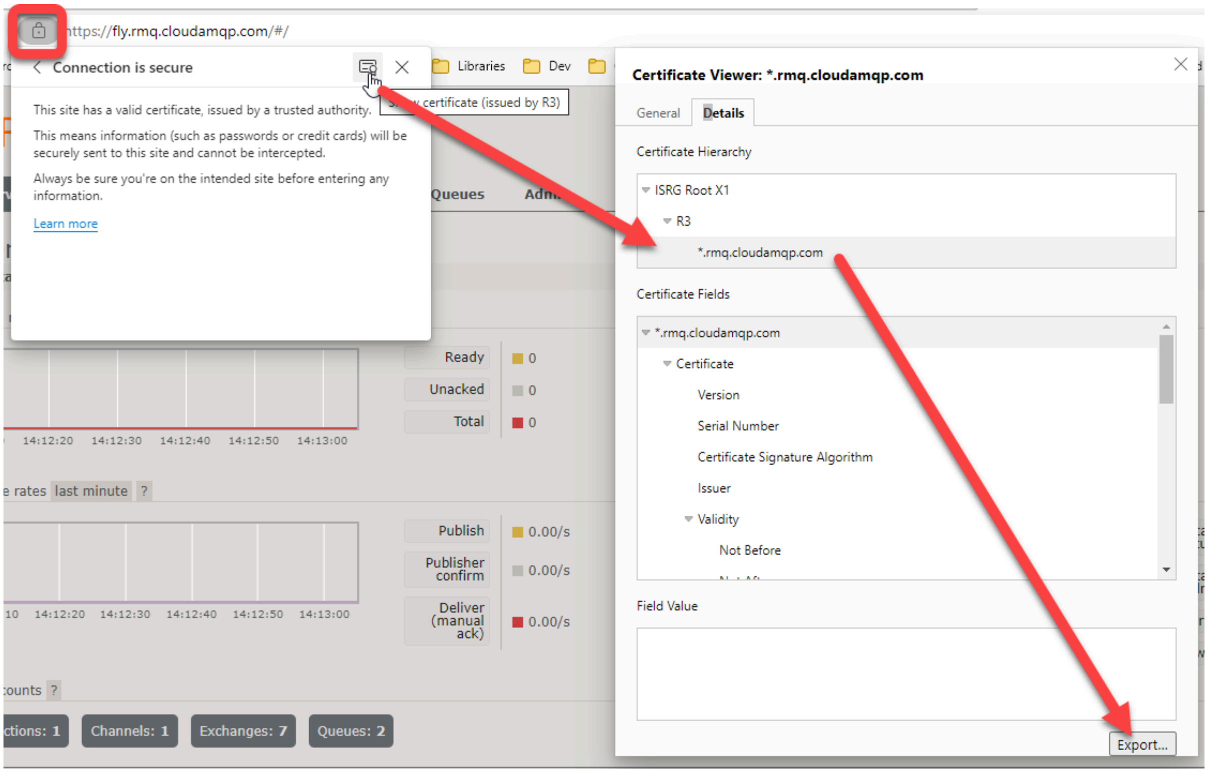
Client certificate:

Cloud offering of RabbitMQ

As an alternative to the local RabbitMQ, you can use a cloud offering of RabbitMQ. This solution is more expensive because of the disk space requirements, but it is also more secure and more resilient. The RabbitMQ instance is usually created within minutes by the service provider, and is highly available.

IMPORTANT: There is currently a potential communication problem between the cloud version of RabbitMQ and Windows Server 2022. If Security Center is installed on a Windows Server 2022, the Third-Party Data Exporter might not be able to connect to a cloud instance of RabbitMQ.

If you are using a cloud instance of RabbitMQ, you must either request the TLS certificate from the service provider, or use a browser to download it directly, for example, from the RabbitMQ manager.



https://fly.rmq.cloudamqp.com/#/

Connection is secure

This site has a valid certificate, issued by a trusted authority.

This means information (such as passwords or credit cards) will be securely sent to this site and cannot be intercepted.

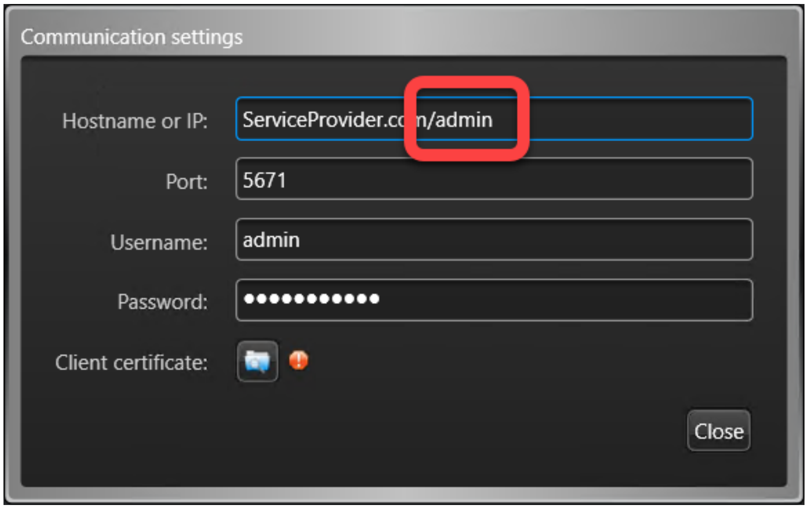
Always be sure you're on the intended site before entering any information.

Learn more

Certificate Viewer: *.rmq.cloudamqp.com

The TLS certificate must be used in the *Communication settings* as shown in the *RabbitMQ on a local network* section.

RabbitMQ uses virtual hosts to manage the access to queues and for administration. Some cloud service providers keep the default (/) for their own use as administrators. In that case, you can specify a virtual host in the Data Exporter. The **Username** is usually used as the virtual host.



Communication settings

Hostname or IP: ServiceProvider.com/admin

Port: 5671

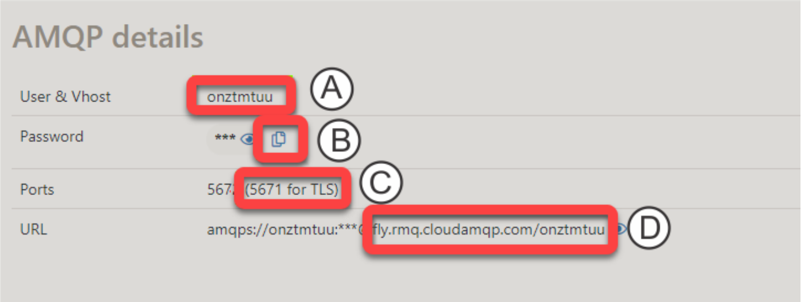
Username: admin

Password: ●●●●●●●●●●●●

Client certificate:

Example

The Third-Party Data Exporter was tested using the CloudAMQP service provider. All of the necessary information is provided on their management portal:



AMQP details

User & Vhost: onztmtuu

Password: ***

Ports: 567 (5671 for TLS)

URL: amqps://onztmtuu:***@ fly.rmq.cloudamqp.com/onztmtuu

	Description
A	Username
B	Password
C	Port to use for the connection
D	Hostname and virtual host

46

AutoVu fixed systems

This section includes the following topics:

Preparing to deploy a fixed SharpV ALPR system

To make sure that your fixed AutoVu™ deployment goes smoothly, you must perform a series of pre-configuration steps.

The following steps describe a typical AutoVu deployment. Depending on your specific installation requirements, your process might be different.

NOTE: Settings that are pre-configured during your installation are not listed in this task. For example, when you install Security Center, the ALPR Manager root folder is automatically created on your computer at the location *C:\Genetec\AutoVu\RootFolder*.

Security Center

Step	Task	Where to find more information
1	Install Security Center Server software on your *main server*.	- Installing Security Center in the *Security Center Installation and Upgrade Guide*.
2	(Optional) Install Security Center Server software on *expansion servers*.	- Adding expansion servers in the *Security Center Installation and Upgrade Guide*.
3	(Optional) Add an additional server to act as *secondary server* for the ALPR Manager to set up failover.	- Setting up role failover on page 164.
4	Install Security Center Client software on at least one workstation.	- Installing Security Center client software in the *Security Center Installation and Upgrade Guide*.

SharpV

Step	Task	Where to find more information
1	Install the SharpV camera.	- SharpV fixed deployment overview in the *SharpV Deployment Guide*.
2	Update the SharpV system to the latest SharpOS version.	- Updating a Sharp unit in the *SharpV Deployment Guide*.
3	Configure the SharpV system in the Sharp Portal.	- Logging on to the Sharp Portal in the *SharpV Administrator Guide*.

Deployment overview for your fixed AutoVu system

To integrate different ALPR capabilities to Security Center, you can deploy a fixed AutoVu™ system using SharpV cameras.

The following steps describe a typical AutoVu deployment. Depending on your specific installation requirements, your process might be different.

Step	Task	Where to find more information
1	Complete the pre-configuration steps.	• Preparing to deploy a fixed SharpV ALPR system on page 1023.
2	Use the Admin account in Config Tool to connect your system.	• Logging on to Security Center through Config Tool on page 7.
3	Configure the ALPR Manager server and database settings.	• Configuring the ALPR Manager role on page 961.
4	Configure the Archiver role in Security Center.	• Setting up the Archiver role for ALPR on page 963.
5	Add the SharpV camera to the ALPR Manager role so that Security Center can receive license plate reads.	• Adding a SharpV camera to the ALPR Manager on page 1029.
6	(Optional) If you want to store video from the SharpV camera, add it to the Archiver role. **NOTE:** The ALPR Manager always sends ALPR images to the Archiver for storage.	• Adding a SharpV camera to the Archiver on page 1044.
7	(Optional) Specify the SharpV location and time zone.	• Setting geographical locations of entities on page 79.
8	(Optional) Create and configure hotlist entities.	• Creating hotlists on page 985.
9	(Optional) If you are using license plates as credentials for access control, then configure the system to grant or deny access to a parking area or other facility.	• Configuring access control using vehicle license plate credentials on page 1050.

Connecting SharpV cameras to the ALPR Manager role

To receive automoatic license plate recognition (ALPR) data in Security Center with a fixed AutoVu™ system, you must configure the ALPR Manager role so that it can connect to the Sharp camera.

Before you begin

- You must know the IP address of the computer that is hosting the ALPR Manager role.
- If you change any of the ports used to detect Sharp cameras, make sure you also update the firewall rule.

  IMPORTANT:

  - Each ALPR Manager must use a unique discovery port.
  - When setting the discovery port, do not use port 5050 because it is reserved for the logger service.

What you should know

There might be more than one way of adding a Sharp camera, depending on the SharpOS version and the network topology. Use the methods described here if the Sharp and Security Center are on the same subnet. If the Sharp and Security Center are not on the same subnet, or if they must communicate across the Internet where the network topology includes NATs, you might have to use a different connection method. For more information, see SharpV camera connections to the ALPR Manager role on page 1027.

To connect a SharpV camera running SharpOS 12.7 and later:

1. From the Config Tool home page, click **System** > **Roles**, and then select the ALPR Manager you want to configure.
2. Click the **Properties** tab, and then click the **LPM protocol** setting.
3. Confirm the **Listening port** to be used when adding Sharp cameras. If you change the port, click **Apply** to confirm the change.
   - **LPM protocol - Listening port:** Port used to listen for connection requests coming from SharpV cameras and Genetec Patroller™. After the connection is established, the ALPR Manager can receive updates from the Sharp it manages. The default listening port is 10001.
4. Click the **Live** setting and under **Send on read (SharpV only)**, configure the following:
   - **License plate image:** Include the high resolution close-up image of the license plate along with the plate read data.
   - **Context image:** Include the wide angle context image of the vehicle along with the plate read data.

   These images are displayed in Security Desk when monitoring ALPR events.

   NOTE: This Live setting also applies when using the LPM protocol.

To connect a SharpV camera running SharpOS 12.6 and earlier:

1. From the Config Tool home page, click **System** > **Roles**, and then select the ALPR Manager you want to configure.
2. Click the **Properties** tab, and then click the **Live** setting.
3. Under **Network**, configure the following ports:
   - **Listening port:** Port used to listen for connection requests coming from SharpV cameras and Genetec Patroller™. After the connection is established, the ALPR Manager can receive updates from the Sharp it manages. The default listening port is 8731.
   - **Sharp discovery port:** Port used by the ALPR Manager to find fixed Sharp units on the network.

4 Under **Send on read (SharpV cameras only)**, configure the following:
   - **License plate image:** Include the high resolution close-up image of the license plate along with the plate read data.
   - **Context image:** Include the wide angle context image of the vehicle along with the plate read data.

   These images are displayed in Security Desk when monitoring ALPR events.

   NOTE: This Live setting also applies when using the LPM protocol.

After you finish

- Make sure the Sharp discovery port matches the port number in the Sharp Portal. For more information, see the *Sharp Administrator Guide*.
- To ensure that plate reads have the correct timestamp, configure the time zone of the fixed Sharp units.
- To plot the ALPR events (reads and hits) associated with the Sharp units on the *map* in Security Desk, configure the geographical location of the Sharp units.

SharpV camera connections to the ALPR Manager role

If you want to send ALPR data from a SharpV camera to Security Center, you must first enroll the camera in the Security Center *ALPR* task under *Roles and units*.

When connecting to Security Center 5.8 or later, the SharpV uses the LPM protocol to manage the connection (when manually added). If the LPM protocol is not enabled on the SharpV, other connection methods are available.

For information on configuring ALPR Managers for fixed AutoVu system, see About the ALPR Manager role on page 959.

Adding a camera using the LPM protocol

This is the preferred method for adding a Sharp to the ALPR Manager. The LPM protocol provides a secure and reliable connection.

Connection Method	When to use this method	Requirements
Manually add the camera in Security Center: You can add the camera to the ALPR Manager in Config Tool's *ALPR* task.	If your camera can be upgraded to SharpOS 12.7 or higher, this is the recommended method. For compatibility information, see Product compatibility for AutoVu Automatic License Plate Recognition (ALPR).	• SharpOS 12.7 or higher with LPM protocol enabled • Security Center 5.8 or higher • You must know the IP address and the username and password used to access the Sharp Portal .

Adding a camera that does not use the LPM protocol

For cameras where the SharpOS version is earlier than 12.7, the easiest way to add a Sharp camera in Security Center is to configure the ALPR Manager to discover the camera. If this connection method is not possible, you can add the camera manually in Security Center or in the camera's web portal.

NOTE: If you are connecting a SharpV camera, it is recommended that you upgrade it to SharpOS 12.7 or higher, and enable the secure and reliable LPM protocol connection.

Connection Method	When to use this method	Requirements
Configure the ALPR Manager to discover the camera: You can configure the ALPR Manager's *Discovery port* to find the camera on the subnet.	This is the preferred method if the camera and Security Center are on the same subnet.	To use this method, you must set the same *Discovery port* in the ALPR Manager's *Properties* tab and in the camera's web portal. The camera and Security Center must be on the same subnet.

Connection Method	When to use this method	Requirements
Manually add the camera in Security Center: You can add the camera to the ALPR Manager in Config Tool's *A* task.	Use this method when the camera and Security Center are on different subnets within the same LAN. You can use this method if the *Discovery port* is not available, however the *Discovery port* can be changed in Security Center and in the camera's web portal. **NOTE:** • You cannot use this method if communication must go across the Internet. • If the camera is behind a NAT, you must configure port forwarding.	To use this method, you must know the IP address, port (80 or 443), and its control port (default 8001). The camera and Security Center must be on the same network.
Add a Sharp from the camera's web portal: You can force a connection from the camera's web portal when you select the *Security Center* extension and select **Connect to Security Center**. For assistance, contact your Genetec™ representative.	Use this method if the camera and Security Center must communicate across the Internet and where the network topology includes NATs. **NOTE:** If the camera is behind a NAT, you must configure port forwarding.	To use this method, you must enter the *Hostname* or *IP address* and *port* (listening port) of the Security Center computer.

Adding a SharpV camera to the ALPR Manager

To send license plate reads to Security Center, you must add the SharpV camera to an ALPR Manager.

Before you begin

- To add a camera in Security Center, you must first configure an ALPR Manager role.
- If your SharpV was shipped with SharpOS 12.7 or later and you are manually adding the SharpV to Security Center, you do not need to upgrade it to use the LPM protocol. If your SharpV camera is running an earlier SharpOS 12.x version, it is recommended that you upgrade the camera and enable the LPM protocol to take advantage of this secure and reliable connection to Security Center.

  NOTE: If a camera uses the LPM protocol to connect to Security Center, the **Active extension** in the Sharp Portal is set to *Security Center (LPM protocol)*.

What you should know

- The steps for adding the camera to the ALPR Manager depend on the SharpOS version running on the camera. For more information, see SharpV camera connections to the ALPR Manager role on page 1027.
- If the SharpOS running on the camera is 12.6 or earlier, you can still connect by configuring the Security Center, HTTP, or FTP extensions in the Sharp Portal.

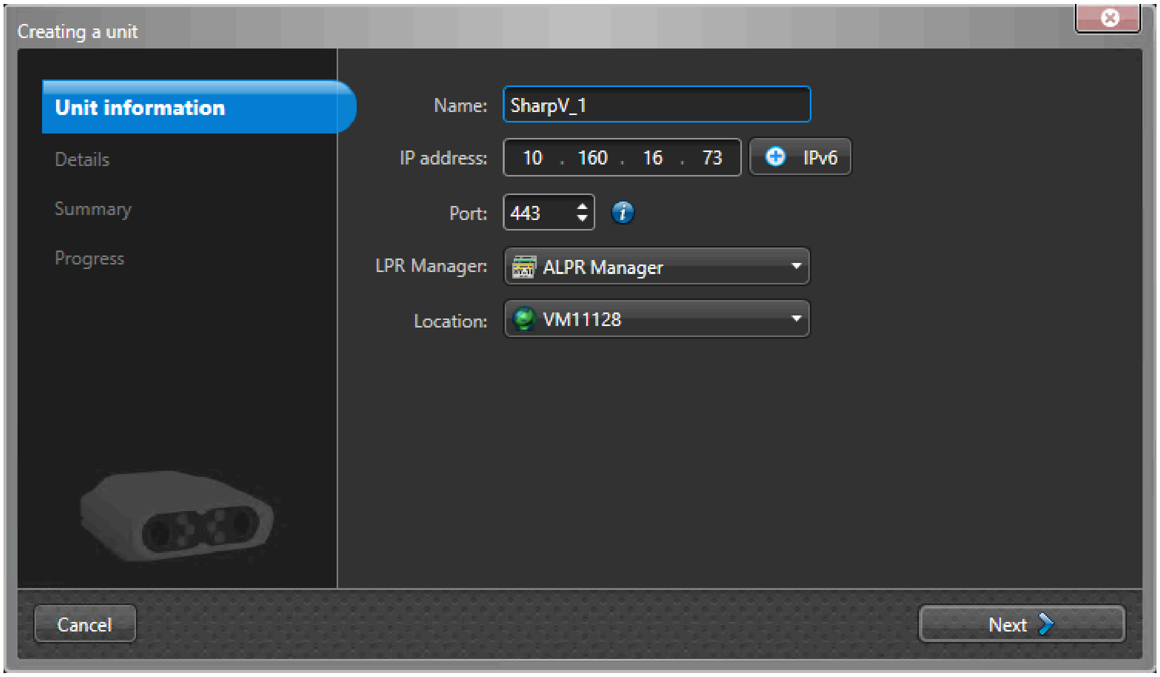
To manually add a camera running SharpOS 12.7 or later (LPM protocol):

1. From the Config Tool home page, click the *ALPR* task and select **Roles and units**.
2. Select the **ALPR Manager** role from the drop-down list.
3. Click ✚ **ALPR unit**.

   The *Creating a unit* dialog box opens.
4. Enter a **Name** for the camera.
5. Enter the camera's **IP address**.
6. This SharpOS version requires HTTPS communication. Enter **Port** 443.

   NOTE: If the camera is behind a NAT, enter the IP address of the NAT, and the port of the NAT which has been associated to port 443 of the camera.

7 From the **Location** list, assign the camera to an area entity.



Creating a unit

Name: SharpV_1

IP address: 10 . 160 . 16 . 73

Port: 443

LPR Manager: ALPR Manager

Location: VM11128

8 Click **Next**.

9 Enter the **Username** and **Password** used to log onto the Sharp Portal.

10 Click **Next**.

The system validates the credentials.

11 Review the settings and click **Create**.

To manually add a camera running SharpOS 12.6 or earlier (Legacy protocol):

1 From the Config Tool home page, click the *ALPR* task and select **Roles and units**.

2 Select the **ALPR Manager** role from the drop-down list.

3 Click ✚ **ALPR unit**.

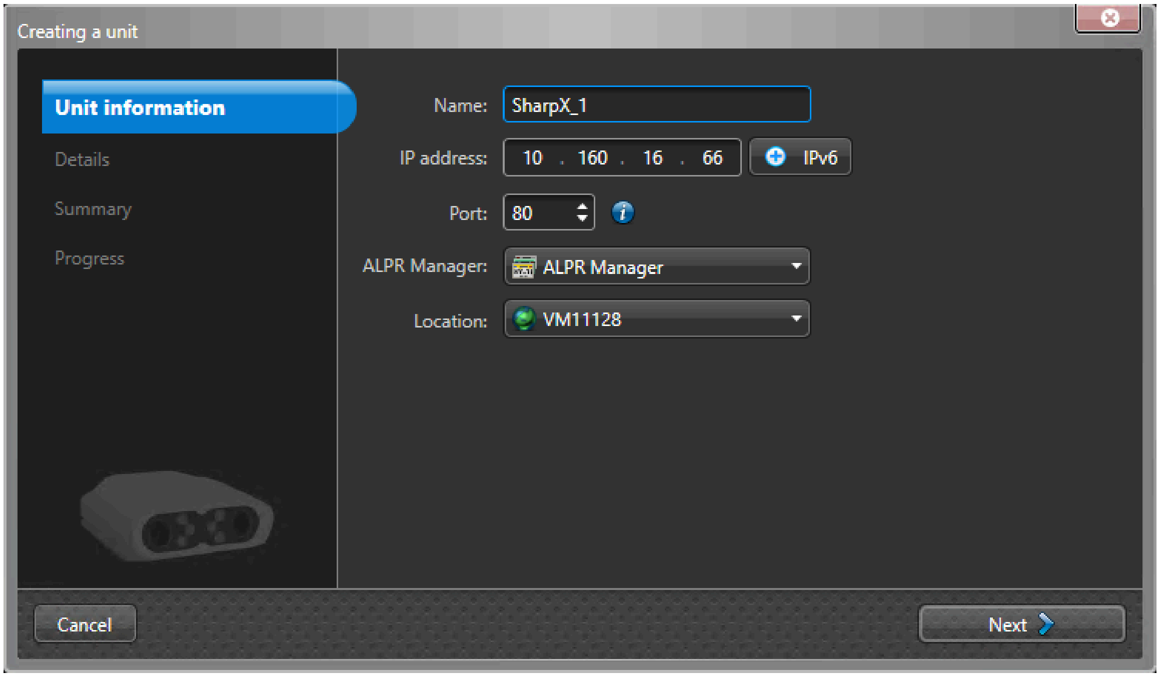
The *Creating a unit* dialog box opens.

4 Enter a **Name** for the camera.

5 Enter the Sharp unit's IPv4 **IP address**.

6 Enter **Port** 443 for HTTPS or 80 for HTTP, according to the Sharp unit's configuration.

7 From the **Location** list, assign the camera to an area entity.



Name: SharpX_1

IP address: 10 . 160 . 16 . 66

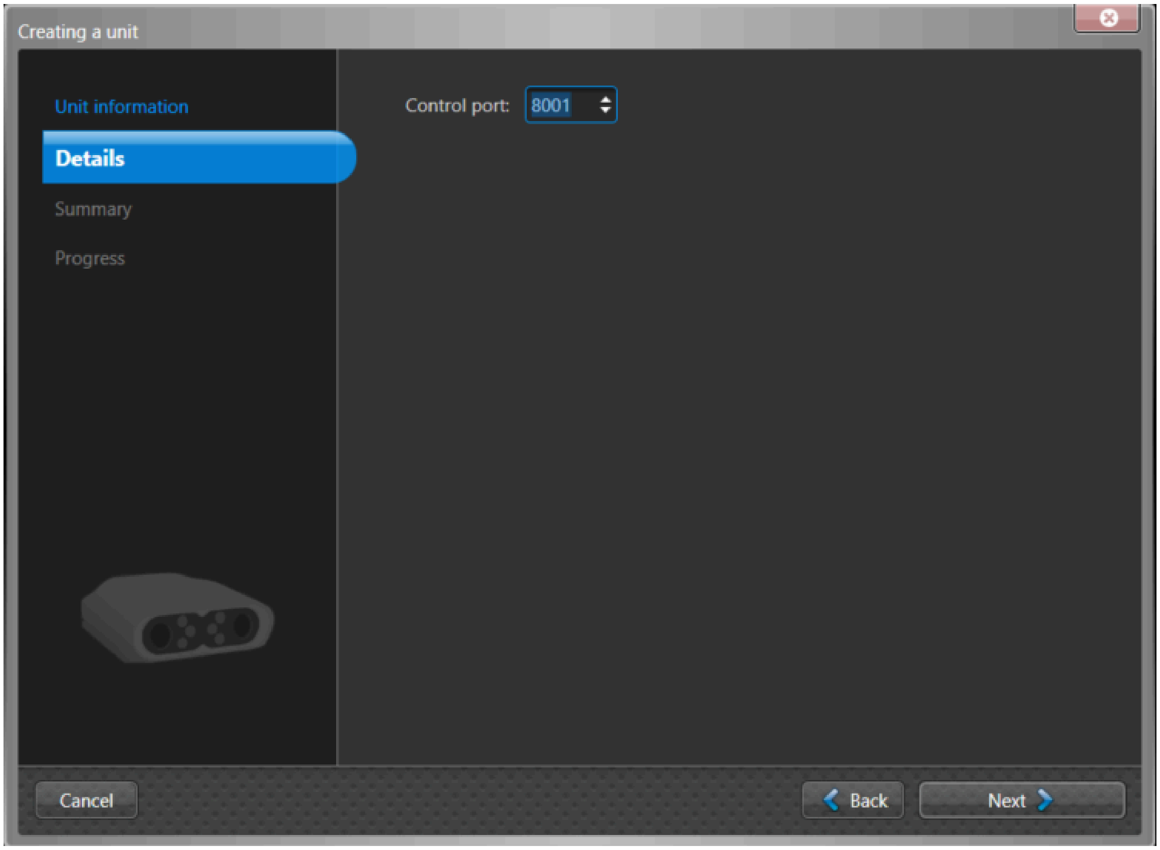
Port: 80

ALPR Manager: ALPR Manager

Location: VM11128

8 Click **Next**.

9 Enter the camera's **Control port** (default: 8001).
This information should match what is displayed in the Sharp Portal configuration page.



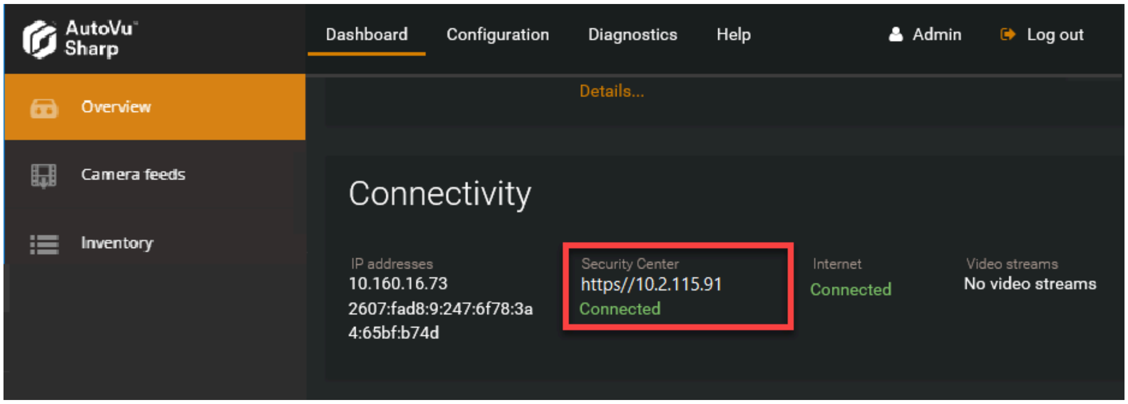
Control port: 8001

10 Click **Next**.

11 Review the settings and click **Create**.

IMPORTANT: When using the LPM protocol, the Extension in the Sharp Portal is automatically set to *None*. Do not change the extension.

- The new camera is added under the selected ALPR Manager.
- In the following image, the https:// address prefix indicates that the unit is connected to Security Center using the legacy protocol.



Connectivity

IP addresses
10.160.16.73
2607:fad8:9:247:6f78:3a4:65bf:b74d

Security Center
https//10.2.115.91
Connected

Internet
Connected

Video streams
No video streams

Related Topics

SharpV camera connections to the ALPR Manager role on page 1027

Upgrading a SharpV to use the LPM protocol on page 1036

Adding a Cloudrunner camera to the ALPR manager

To view license plate reads from Cloudrunner in Security Center, you must add the cloud cameras to the required ALPR Manager.

Before you begin

Ensure that you have a valid user access to a Cloudrunner tenant.

What you should know

You can only register one tenant to an ALPR manager role. If you have multiple tenants in your account, you need multiple ALPR manager roles to integrate the cameras from each tenant. The following Config Tool actions are not applicable for Cloudrunner cameras:

- Replacing the unit with a different Cloudrunner camera.
- Upgrading the firmware version of the unit.
- Deleting the unit when it is active(selected) to an ALPR manager role.

To add Cloudrunner cameras:

1 From the Config Tool homepage, click the *ALPR* task and select **Roles and units**.

2 Select the **ALPR Manager** you want to configure, and then click the **Properties** tab.

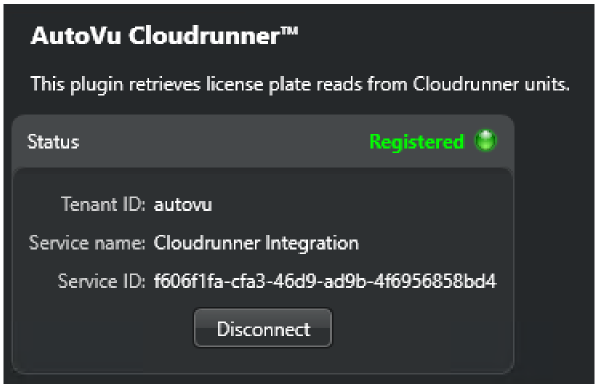
3 Select **Cloudrunner integration**.

4 Click **Register**.

5 In the pop-up window, enter your *Cloudrunner* login.

NOTE: If you have multiple tenants in your account, select the tenant whose cameras you want to add to the ALPR manager.

After the tenant is successfully connected, the *Status* is updated to *Registered* and the Cloudrunner tenant details are displayed. The following example illustrates the updated *Status* section, when a tenant is successfully registered.



AutoVu Cloudrunner™

This plugin retrieves license plate reads from Cloudrunner units.

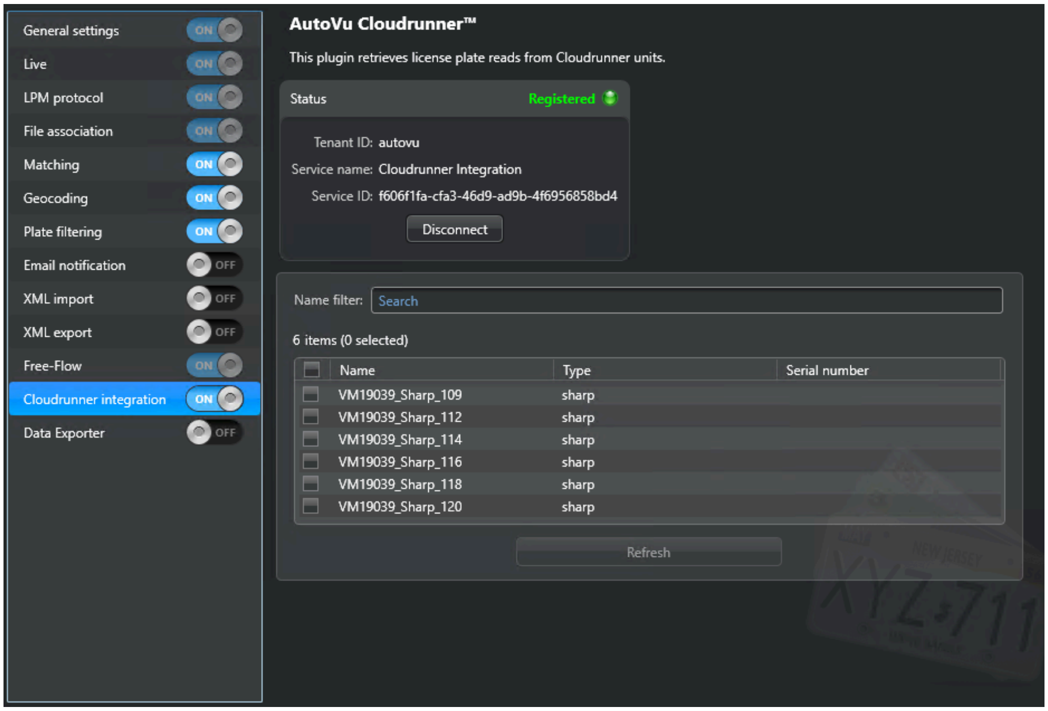
Status Registered ●

Tenant ID: autovu

Service name: Cloudrunner Integration

Service ID: f606f1fa-cfa3-46d9-ad9b-4f6956858bd4

6 From the list of cameras displayed, select the cameras whose reads you want to view.



General settings	ON
Live	ON
LPM protocol	ON
File association	ON
Matching	ON
Geocoding	ON
Plate filtering	ON
Email notification	OFF
XML import	OFF
XML export	OFF
Free-Flow	ON
Cloudrunner integration	ON
Data Exporter	OFF

AutoVu Cloudrunner™

This plugin retrieves license plate reads from Cloudrunner units.

Status: Registered

Tenant ID: autovu
Service name: Cloudrunner Integration
Service ID: f606f1fa-cfa3-46d9-ad9b-4f6956858bd4

Name filter: Search

6 items (0 selected)

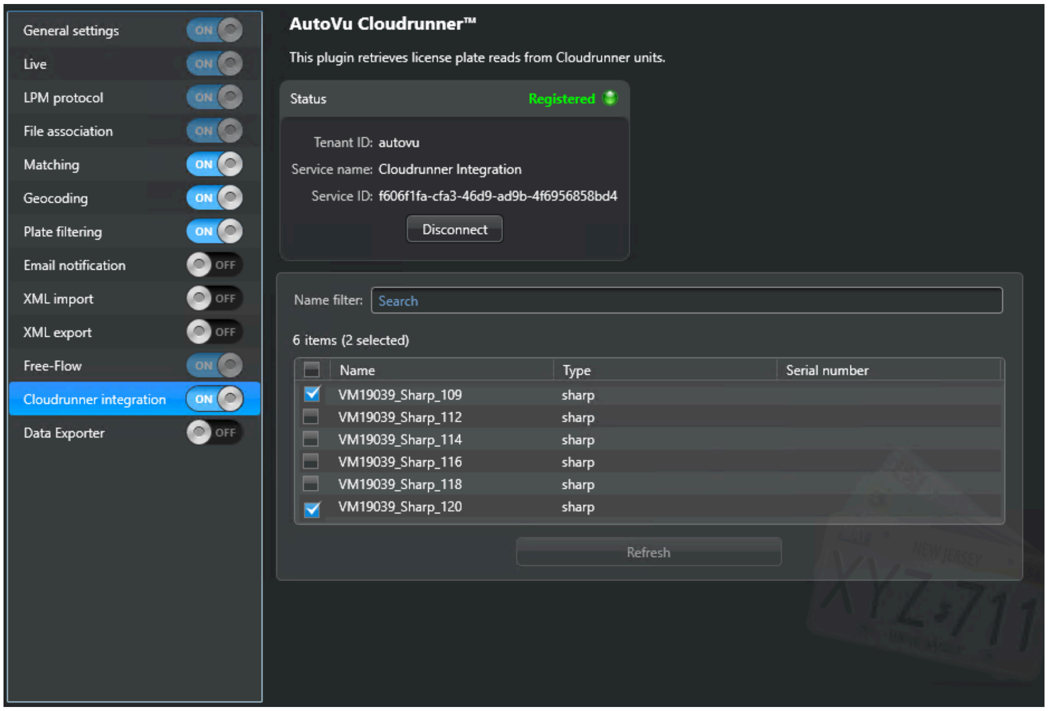
□	Name	Type	Serial number
□	VM19039_Sharp_109	sharp	
□	VM19039_Sharp_112	sharp	
□	VM19039_Sharp_114	sharp	
□	VM19039_Sharp_116	sharp	
□	VM19039_Sharp_118	sharp	
□	VM19039_Sharp_120	sharp	

NOTE: If a camera is already connected to another ALPR manager role, the camera is automatically grayed out. To move a connected camera to a different ALPR role registered to same tenant, deselect the camera from the existing ALPR role and reselect it in the other ALPR role.

7 (Optional) If you add a new camera to your Cloudrunner account, click **Refresh** to view it in the list.

8 Click **Apply**.

- The cameras are added under the selected ALPR manager role.



General settings	ON
Live	ON
LPM protocol	ON
File association	ON
Matching	ON
Geocoding	ON
Plate filtering	ON
Email notification	OFF
XML import	OFF
XML export	OFF
Free-Flow	ON
Cloudrunner integration	ON
Data Exporter	OFF

AutoVu Cloudrunner™

This plugin retrieves license plate reads from Cloudrunner units.

Status: Registered

Tenant ID: autovu
Service name: Cloudrunner Integration
Service ID: f606f1fa-cfa3-46d9-ad9b-4f6956858bd4

Name filter: Search

6 items (2 selected)

□	Name	Type	Serial number
☑	VM19039_Sharp_109	sharp	
□	VM19039_Sharp_112	sharp	
□	VM19039_Sharp_114	sharp	
□	VM19039_Sharp_116	sharp	
□	VM19039_Sharp_118	sharp	
☑	VM19039_Sharp_120	sharp	

- To view the reads from the Cloudrunner cameras, see "Investigating reported license plate reads" in the *Security Center User Guide*.

Upgrading a SharpV to use the LPM protocol

The License Plate Management (LPM) protocol provides a Sharp camera with a secure and reliable connection to Security Center. When The LPM protocol is enabled on a Sharp camera, the protocol manages the camera's connection to the ALPR Manager role.

Before you begin

- Minimum SharpOS version: 12.7

  NOTE: If your SharpV was shipped with SharpOS 12.7 or later and you are manually adding the SharpV to Security Center, you do not need to upgrade it to use the LPM protocol.
- Minimum Security Center version: 5.8

What you should know

- After you upgrade your SharpV to 12.7 or later, you can still connect to Security Center using the **Active extension:** *Security Center (Legacy)* until you upgrade to the LPM protocol.
- If the LPM protocol is enabled on the camera, Security Center can only connect to the camera using the LPM protocol.
- If a camera uses the LPM protocol to connect to Security Center, the **Active extension** in the Sharp Portal is set to *Security Center (LPM protocol)*.
- You cannot revert the LPM protocol upgrade.

To upgrade a SharpV camera to use the LPM protocol:

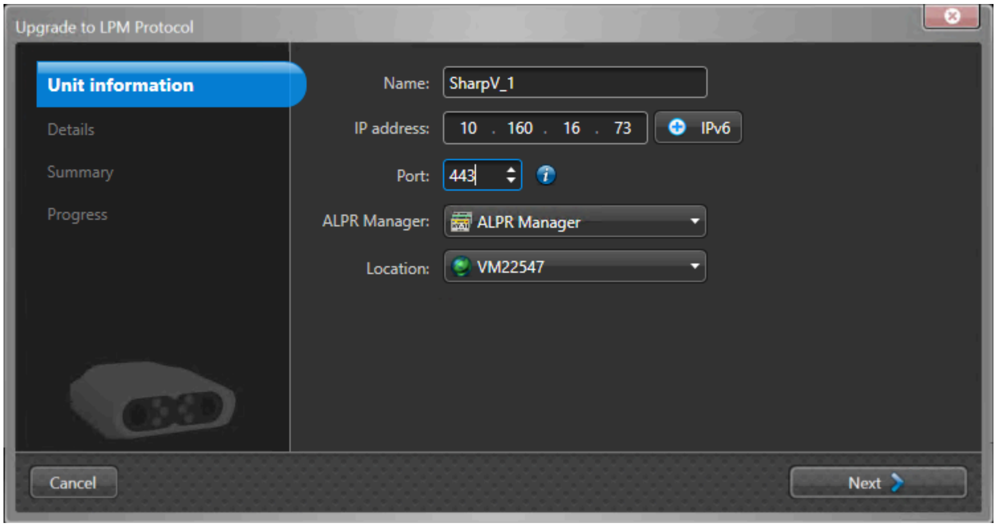
1 From the Config Tool home page, click the *ALPR* task and select **Roles and units**.

2 Select the **ALPR Manager** role from the drop-down list.

3 Expand the list of cameras under the ALPR Manager and select the SharpV camera.

4 At the bottom of the screen, click **Unit** and select **Upgrade to LPM protocol** .

The *Upgrade to LPM Protocol* window opens.



Upgrade to LPM Protocol

Name: SharpV_1

IP address: 10 . 160 . 16 . 73

Port: 443

ALPR Manager: ALPR Manager

Location: VM22547

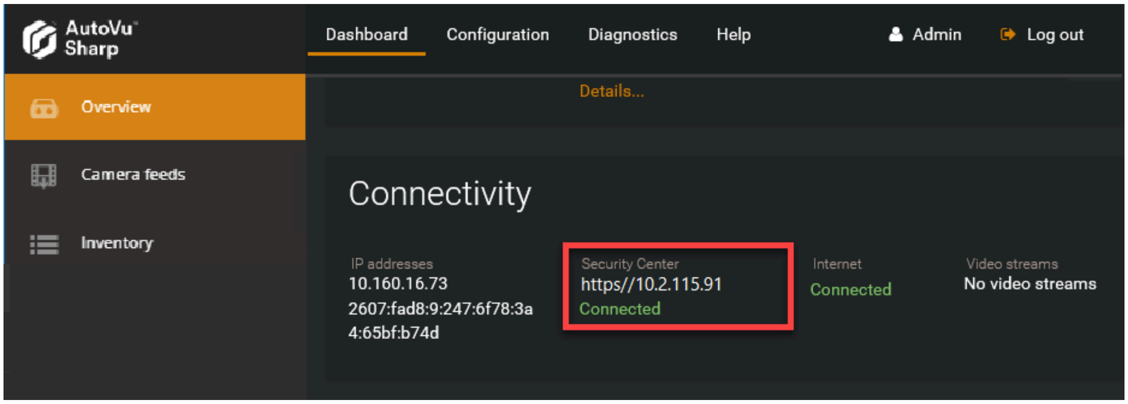
5 Enter the HTTPS **Port** of the unit (default = 443).

6 Click **Next**.

7 Enter the **Username** and **Password** used to log onto the Sharp Portal and click **Next**.

8 Review the settings and click **Upgrade**.

The Sharp Portal shows that the camera is connected to Security Center. The LPM protocol listening port (default = 10001) is appended to the IP address, indicating that the LPM protocol is managing the connection to Security Center.



Connectivity

IP addresses
10.160.16.73
2607:fad8:9:247:6f78:3a
4:65bf:b74d

Security Center
https//10.2.115.91
Connected

Internet
Connected

Video streams
No video streams

Related Topics

SharpV camera connections to the ALPR Manager role on page 1027

About port forwarding for SharpV cameras using the LPM protocol or SSH tunnel

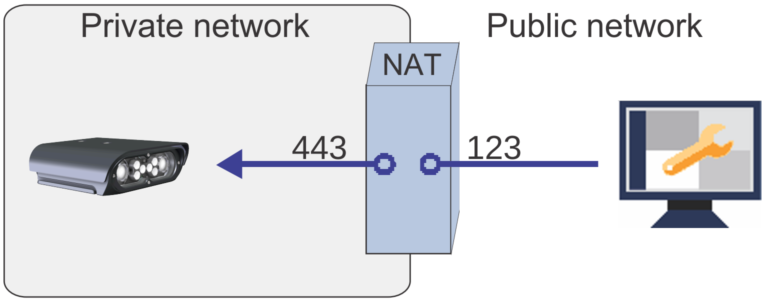
For SharpV cameras that use the LPM protocol to connect to Security Center, if either the SharpV or the ALPR Manager role is behind a *network address translation (NAT)*, additional configuration is required.

IMPORTANT: Consider the following when designing your system:

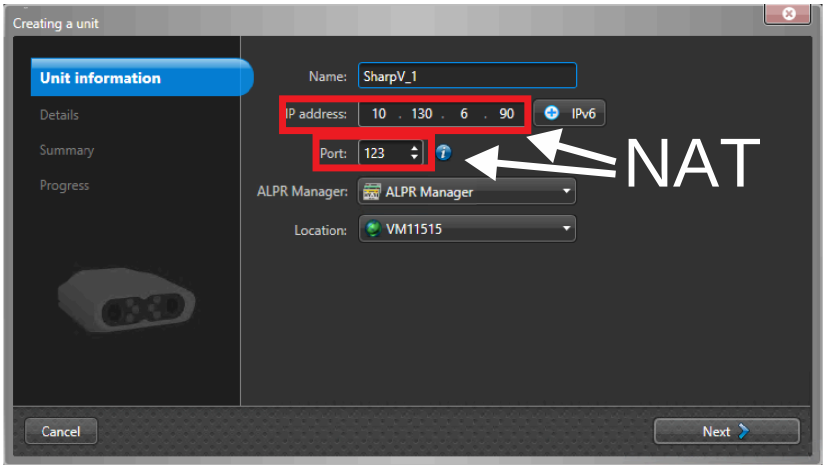
- If the SharpV camera or the ALPR Manager role are behind a NAT, it is not possible to configure a failover server.
- If you have a multi-server system where the Directory and the ALPR Manager roles are installed on different machines, it is not possible to configure NAT port forwarding for the ALPR Manager role.

The SharpV is behind a NAT

If the SharpV is behind a NAT, you must configure port forwarding to forward the port of the NAT to the IP address and port of the SharpV. For example, if port 123 is available on the NAT, configure port forwarding to point to port 443 on the SharpV.



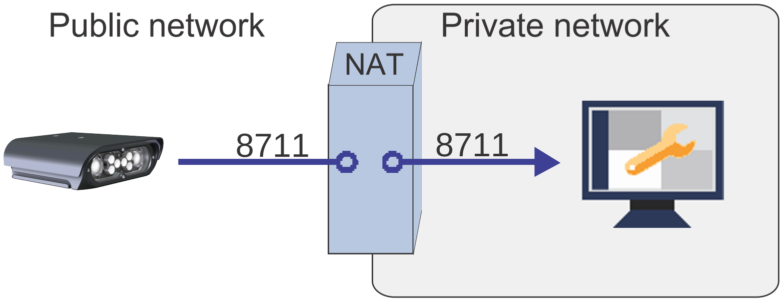
- When adding the SharpV to the ALPR Manager using the *Create a unit* wizard, enter the IP address and port of the NAT.


Creating a unit

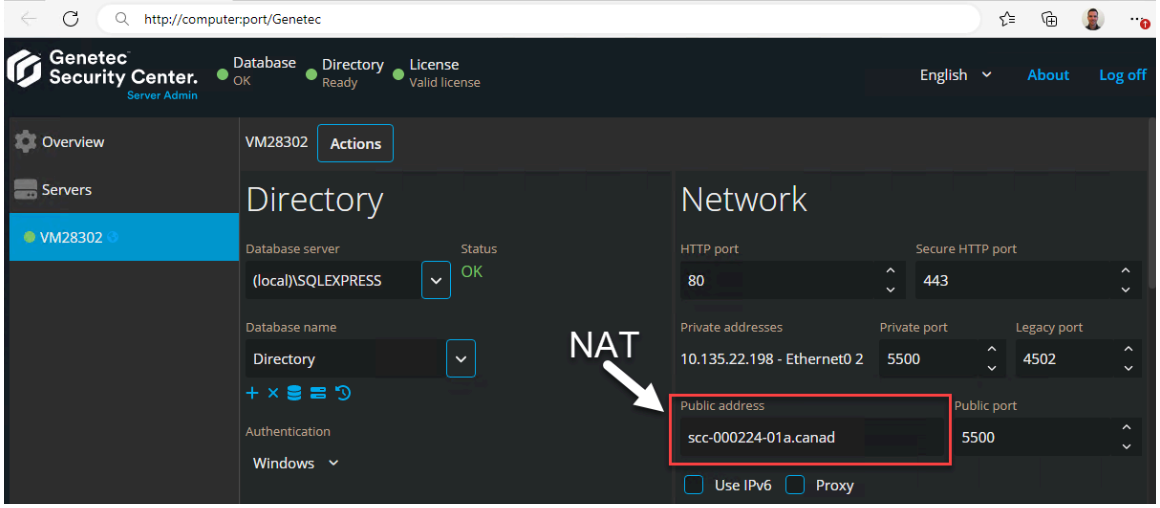
Name: SharpV_1
IP address: 10 . 130 . 6 . 90
Port: 123
ALPR Manager: ALPR Manager
Location: VM11515

The ALPR Manager role is behind a NAT

If the ALPR Manager role is behind a NAT, you must configure the ALPR Manager listening port to match the inbound port that is configured on the NAT. For example, if port 8711 is available on the NAT and the firewall rules have been configured accordingly, configure port forwarding to point to port 8711 on the ALPR Manager.



- In the Server Admin **Public address** field, enter the hostname or IP address.



VM28302

Directory

Database server: (local)\SQLEXPRESS

Status: OK

Database name: Directory

Authentication: Windows

Network

HTTP port: 80

Secure HTTP port: 443

Private addresses: 10.135.22.198 - Ethernet0 2

Private port: 5500

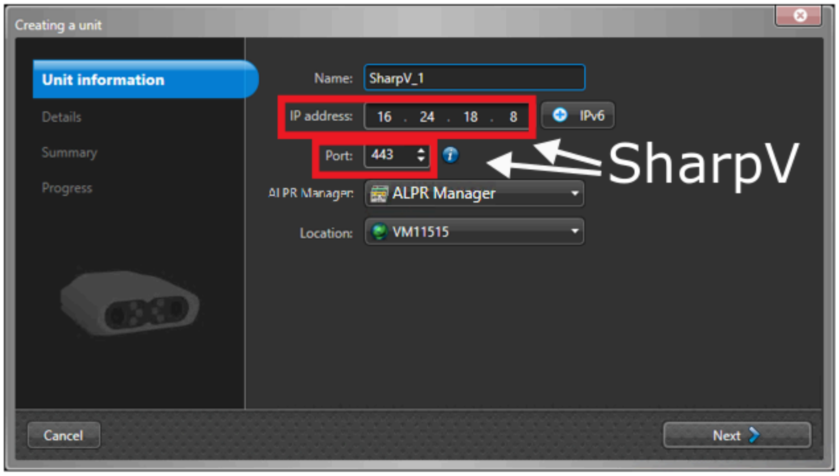
Legacy port: 4502

Public address: scc-000224-01a.canad

Public port: 5500

□ Use IPv6 □ Proxy

- When adding the SharpV to the ALPR Manager using the *Create a unit* wizard, enter the IP address and port of the SharpV.



Name: SharpV_1

IP address: 16 . 24 . 18 . 8

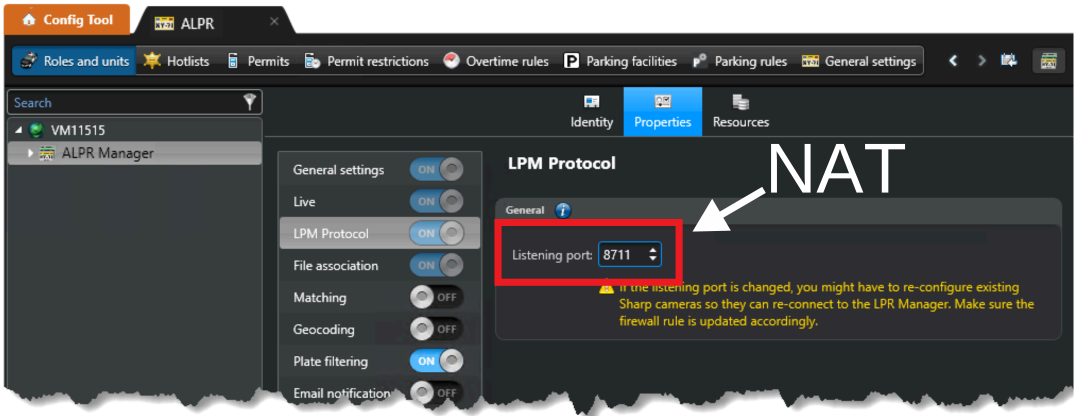
IPv6

Port: 443

ALPR Manager: ALPR Manager

Location: VM11515

- Update the port that the ALPR Manager will be listening on. In this example where the NAT is configured to use port 8711, you would change the LPM protocol **Listening port** from the default port (10001) to port 8711.



LPM Protocol

General settings	ON
Live	ON
LPM Protocol	ON
File association	ON
Matching	OFF
Geocoding	OFF
Plate filtering	ON
Email notification	OFF

Listening port: 8711

If the listening port is changed, you might have to re-configure existing Sharp cameras so they can re-connect to the LPR Manager. Make sure the firewall rule is updated accordingly.

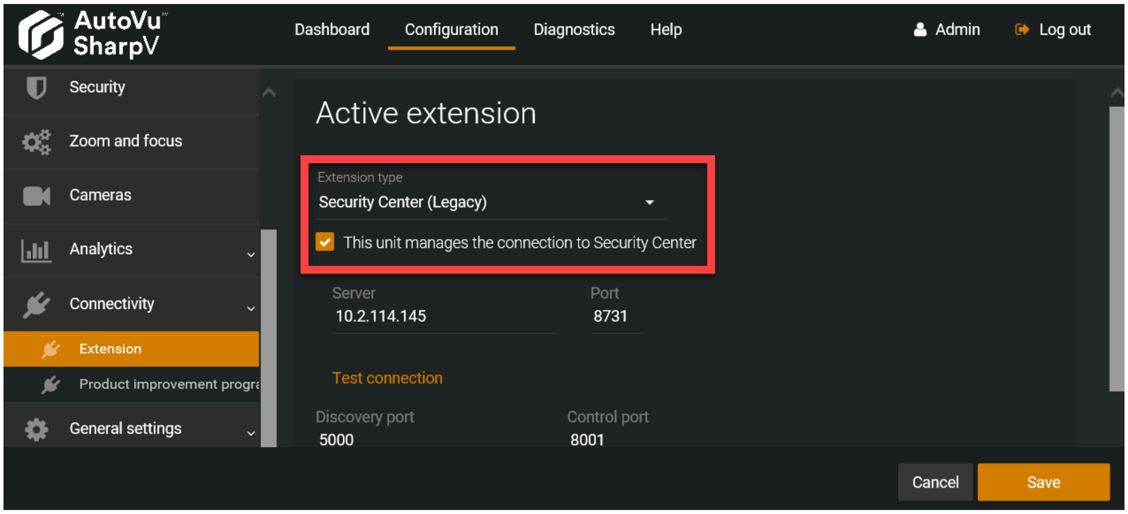
About port forwarding for SharpV cameras using the Security Center (legacy) extension

For SharpV cameras that use the Security Center (legacy) extension to connect to Security Center, if either the SharpV or the ALPR Manager role is behind a Network address translation (NAT) device, additional configuration is required.

The SharpV is behind a NAT

- **If the SharpV manages the connection:**

  In this case, the SharpV connection to Security Center is forced using the **This unit manages the connection to Security Center** setting in the Sharp Portal.



Active extension

Extension type: Security Center (Legacy)

☑ This unit manages the connection to Security Center

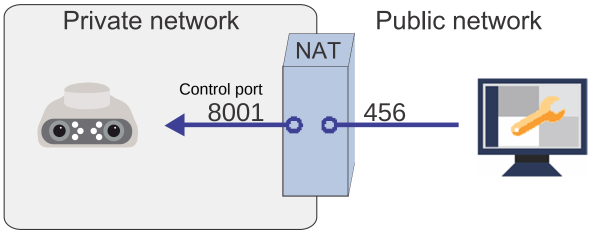
Server: 10.2.114.145

Port: 8731

Discovery port: 5000

Control port: 8001

  Configure port forwarding to forward the port of the NAT to the IP address and port 8001 (control port) of the SharpV.

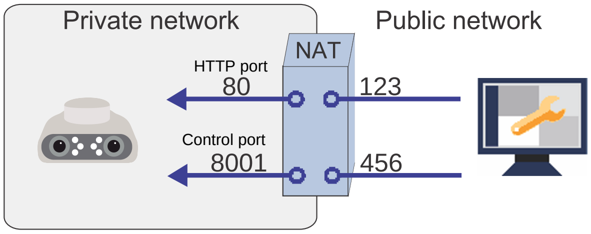


- **If the ALPR Manager role manages the connection (SharpOS 12.7 and later):**

  The SharpV does not support the legacy extension when the ALPR Manager role manages the connection.

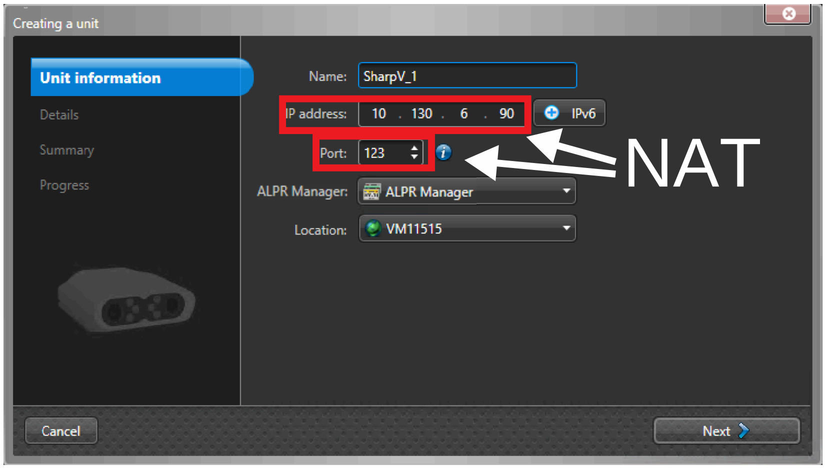
- **If the ALPR Manager role manages the connection (SharpOS 12.6 and earlier):**

  In this case, you must configure port forwarding to forward the port of the NAT to the IP address, HTTP port (80), and control port (8001) of the SharpV.



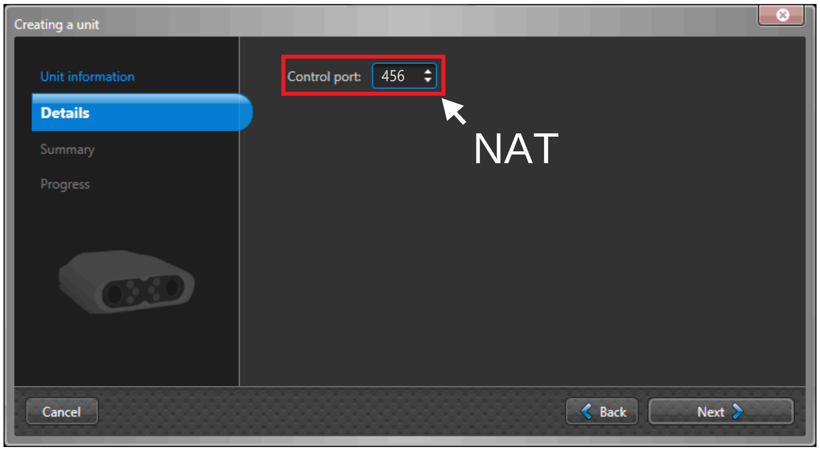
- When adding the SharpV to the ALPR Manager using the *Create a unit* wizard, enter the IP address and port of the NAT.

  NOTE: The **Port** in this screen corresponds to the port the SharpV is configured to listen to for HTTP traffic. By default, legacy SharpV cameras listen for HTTP traffic on port 80, however if you have configured the device to use HTTPS, it will be listening for HTTP traffic on port 443. In such a case, you must configure the NAT to port forward HTTP traffic to port 443 instead of port 80.



Name: SharpV_1
IP address: 10 . 130 . 6 . 90
Port: 123
ALPR Manager: ALPR Manager
Location: VM11515

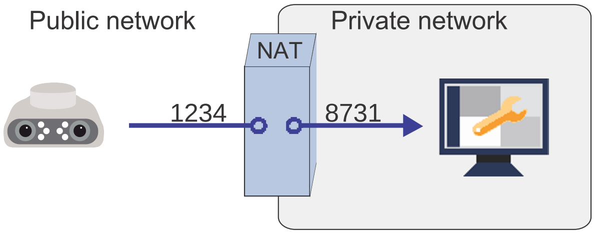
In the *Details* page, enter the port of the NAT that is configured to port forward to the control port (8001).



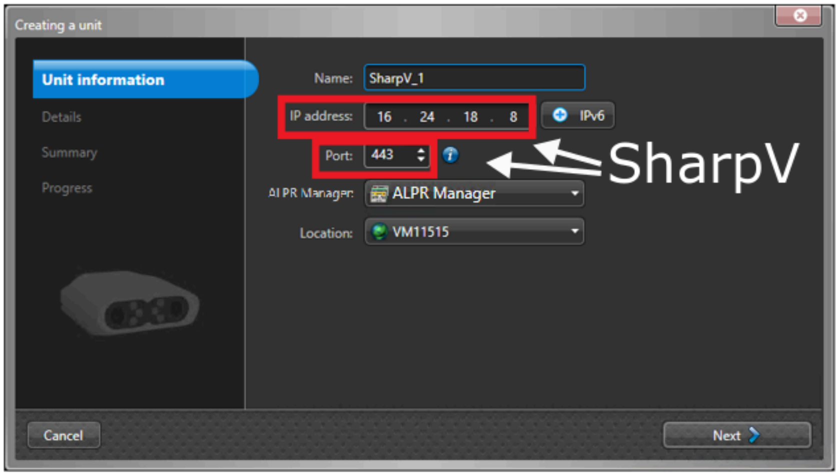
Control port: 456

The ALPR Manager role is behind a NAT

In this case, you must configure port forwarding to point to the listening port of the ALPR Manager. For example, if port 1234 is available on the NAT, configure port forwarding to point to port 8731 (listening port) on the ALPR Manager.

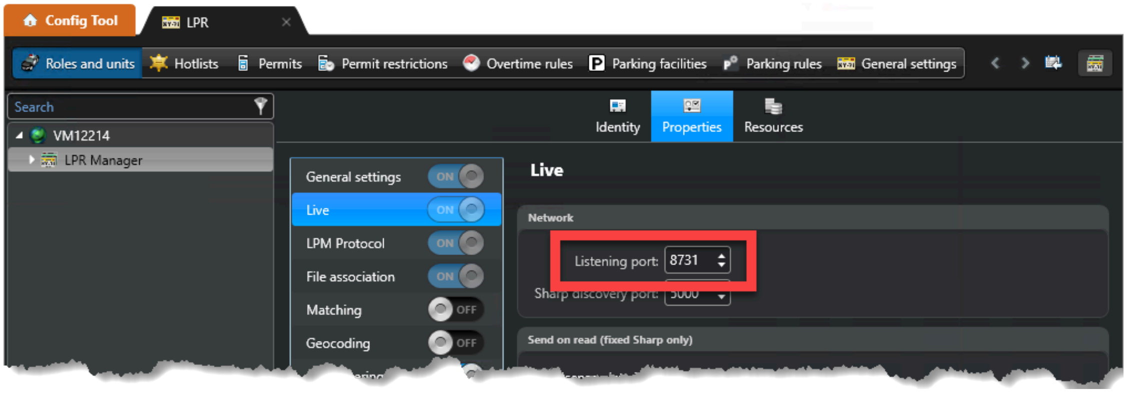


- When adding the SharpV to the ALPR Manager using the *Create a unit* wizard, enter the IP address and port of the SharpV.



Name: SharpV_1
IP address: 16 . 24 . 18 . 8
Port: 443
ALPR Manager: ALPR Manager
Location: VM11515

- The listening port is defined in the **Live** settings on the ALPR Manager's *Properties* tab.



General settings: ON
Live: ON
LPM Protocol: ON
File association: ON
Matching: OFF
Geocoding: OFF

Listening port: 8731
Sharp discovery port: 5000

Adding a SharpV camera to the Archiver

The ALPR Manager always sends ALPR images to the Archiver for storage. If you also want to store video from the SharpV, you must add the camera to the Archiver role.

Before you begin

- Set up the Archiver role for ALPR.
- Log on to the camera's web portal and change the default password.
- By default, SharpV cameras include a self-signed certificate that uses the common name of the SharpV (for example, SharpV12345). To add the SharpV to the Archiver, you must generate a new certificate (signed or self-signed) that uses the camera’s IP address instead of the common name.

What you should know

- The unit is added to the Archiver according to the encoding type configured in the Sharp Portal. For more information, see SharpOS Portal - Encoding page.

To manually add a SharpV camera to the Archiver:

1 From the Config Tool homepage, open the *Video* task and click the **Roles and units** view.

2 Click **Video unit** (✚).

The *Manual add* dialog box opens.

3 If you have multiple Archiver roles, select one to manage the unit from the **Archiver** list.

4 From the **Manufacturers** list, select **AutoVu**™.

5 From the **Product type** list, select **All**.

6 Enter the **IP address** of the video unit.

- Select **IPv4** or **IPv6** and enter the **IP address**.
- If your network supports DHCP, enter the assigned **IP address**.

  NOTE: If this address is subject to change, click **Hostname** to enter the hostname of the unit.

To add multiple units in a single operation, enter a range (⊕) of IP addresses.

7 Enter the **HTTP port** for the unit (default = 80).

NOTE: If the unit uses HTTPS, enter the HTTP port (80) here. You will enter the HTTPS port in the following steps.

8 Select the **Authentication** method for the camera.

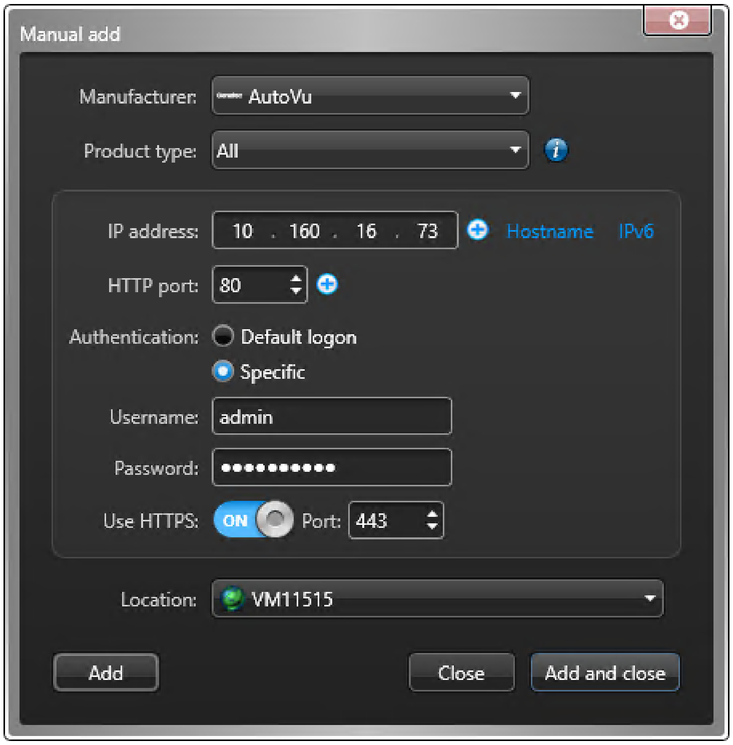
- **Default logon:** The camera uses the default logon defined for the Archiver in the *Extensions* tab. Using this method, you can define the same logon credentials for multiple cameras.

  IMPORTANT: You cannot use the default logon when adding a SharpV camera. You must use the credentials you configured when you first logged on to the SharpV portal.
- **Specific:** Enter the logon credentials for the camera. Turn on **Use HTTPS** if you have applied a certificate.

  NOTE: Sharp cameras running SharpOS 12.7 or later must use HTTPS communication.

9 From the **Location** drop-down, assign the camera to an area entity.

10 Click **Add**.



Manual add

Manufacturer: AutoVu

Product type: All

IP address: 10 . 160 . 16 . 73

HTTP port: 80

Authentication: ○ Default logon ● Specific

Username: admin

Password: ●●●●●●●●●●●

Use HTTPS: ON Port: 443

Location: VM11515

The notification tray displays the message "Adding unit started". If successful, it displays the message "Unit added successfully".

The camera is added under the selected Archiver.

Replacing SharpV units

You can replace a SharpV unit without losing any of its associated plate reads by swapping the connection parameters of the old unit with a new unit.

Before you begin

In Security Desk, run a *Reads* report and a *Hits* report on the Sharp unit you want to replace. You need these reports to verify that the data has been transferred to the new Sharp unit.

To replace a Sharp unit:

1 Add the new Sharp entity in the ALPR Manager.

NOTE: The name you use for the new entity is not important. At the end of the camera replacement procedure, the connection parameters of the entities will be switched and you will delete the entity you are adding now.

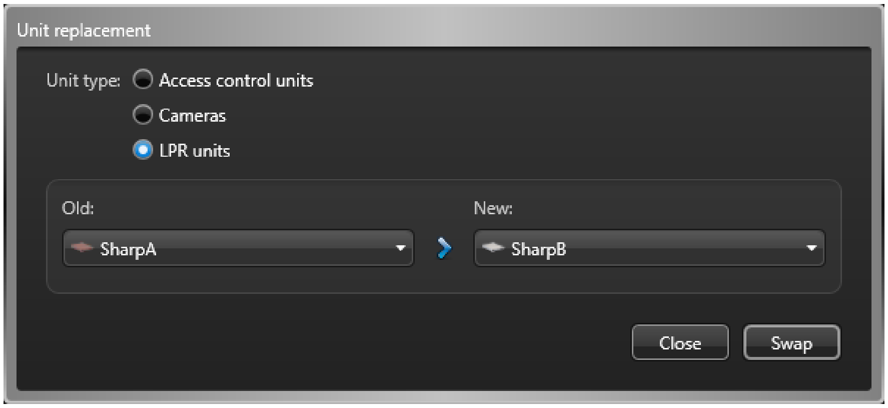
2 Copy the configuration settings of the old Sharp entity to the new Sharp entity using the Copy configuration tool.

3 Power down the old Sharp unit.

4 In Config Tool, click **Tools** > **Unit replacement**.

5 In the **Unit type** option, select **ALPR units**.

6 Select the **Old** and the **New** Sharp units.



Unit replacement

Unit type: ○ Access control units
○ Cameras
● LPR units

Old: SharpA
New: SharpB

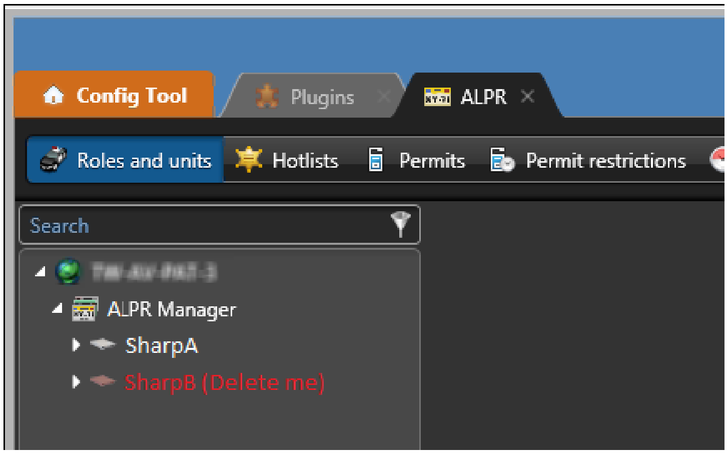
7 Click **Swap**.

When the Sharp unit has been replaced, the system displays the message: "The operation was successful". The connection parameters of the new Sharp unit are now associated with the reads and hits from the old Sharp unit.

8 Verify that the reads and hits are still associated with the old Sharp entity by running a Security Center *Reads* report and a *Hits* report. Compare these reports to the ones you ran before the swap operation to ensure that the data has been successfully transferred.

The Sharp entities have been swapped in Security Center. The old Sharp unit now has the new entity name and is displayed in the ALPR Manager with the message: "Delete me".

9 Right-click the Sharp entity and select **Delete**. In the confirmation dialog box that opens, click **Delete**.



Related Topics

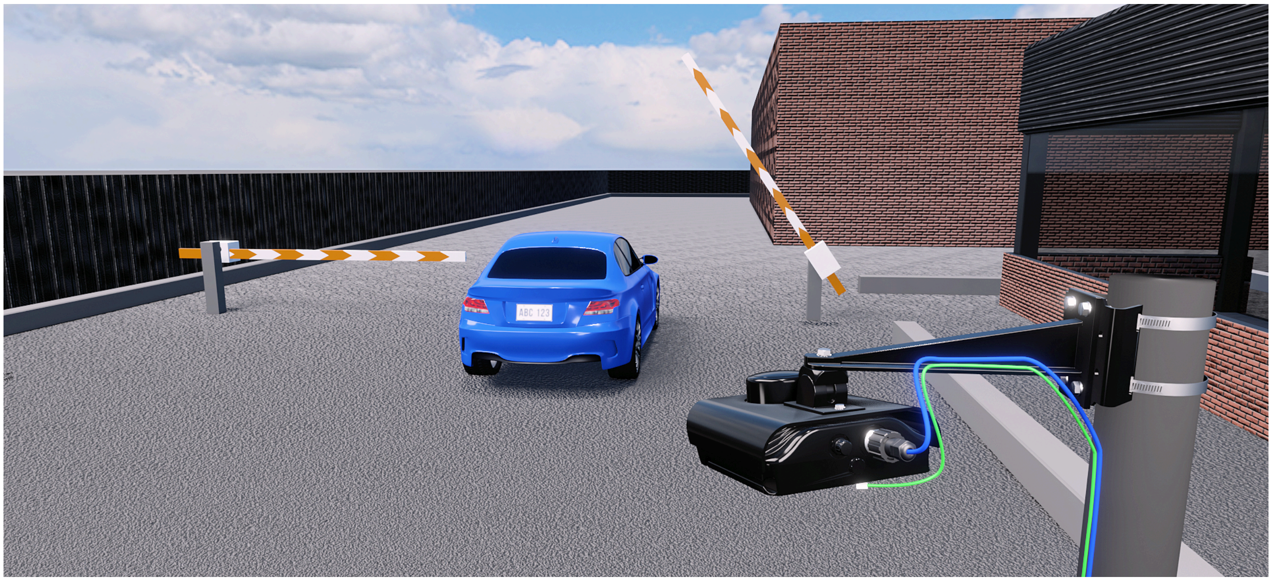
Copying configuration settings from one entity to another on page 82
Connecting SharpV cameras to the ALPR Manager role on page 1025

ALPR access control

By installing SharpV cameras at the entry to a gated parking lot, AutoVu™ License Plate Recognition technology can be used for access control by matching license plates to one or more hotlists, and then granting or denying access to vehicles at the entry point.

How ALPR access control works

In an ALPR access control scenario, you use SharpV cameras, hotlists, and Security Center event-to-actions to automate access to a parking lot or similar facility.



You begin by installing your SharpV cameras at a facility's entry points to capture the plates of vehicles attempting to enter. You then create the hotlists that contain the license plates of the vehicles which are allowed to enter, and assign them to the ALPR Manager or to individual Sharp cameras in Config Tool.

After creating and assigning your hotlists, you then create Security Center event-to-actions for the *License plate hit* and *No match* events generated by the Sharps and hotlists to grant or deny access to the vehicles.

For example, if a plate matches one or more hotlists assigned to a SharpV, Security Center triggers an action that lifts a gate or opens a garage door, while a *No match* event (plate does not match any assigned hotlist) triggers an action that sounds an alert, or sends a message to security personnel so they can question the vehicle's driver.

You can also trigger event-to-actions on hotlists of stolen vehicles, scofflaws, or other vehicles of interest. These hotlists are typically assigned to the ALPR Manager so that the event-to-action can be triggered by any of the Sharps capturing the plate.

About assigning hotlists

Hotlists are lists of vehicle license plates that can be assigned either to an ALPR Manager role, or to individual SharpV cameras.

- **Assigning a hotlist to an ALPR Manager**: When you assign a hotlist to an ALPR Manager, all SharpV cameras controlled by the ALPR Manager can match against the hotlist and trigger the event-to-action.
- **Assigning a hotlist to a Sharp camera**: When you assign a hotlist to an individual SharpV camera, only that specific SharpV camera can trigger the event-to-action. This is useful for parking facilities that have specific entry points for different groups of vehicles. For example, this allows you to assign a VIP hotlist to a SharpV camera that is installed at the entrance to the VIP parking garage.

Events used in ALPR-based access control

There are two main types of Security Center events used in an ALPR-based access control system, *License plate hit* and *No match*.

NOTE: You can also use *License Plate Read* events to trigger actions such as starting video recording for the SharpV context camera. However, only the *License plate hit* and *No match* events are described here.

- **License plate hit events:** When you turn on *Matching* for an ALPR Manager in Config Tool, Security Center tries to match the plates captured by SharpV cameras to plates on loaded hotlists. If a plate is matched to a hotlist, Security Center generates a *License plate hit* event. By creating an event-to-action that triggers on this event, Security Center can grant access to a facility by opening a gate, a garage door, and so on.
- **No match events:** You can also turn on *No match* events for an ALPR Manager in Config Tool. A *No match* event is generated when a plate is *not* matched to a hotlist. For example, you can use a *No match* event to account for guests, delivery vehicles, or other vehicles not typically registered ahead of time on a hotlist. Event-to-actions for *No match* events can either have a hotlist or a SharpV camera as the source of the event. If the hotlist is the source, it means the plate is not found on that particular hotlist. However, if the SharpV is the source, it means that the plate is not found on *any* of the hotlists assigned to the SharpV. This is a subtle but important difference you should keep in mind when configuring your system because you can have more than one hotlist assigned to a single SharpV.

  No match events are not generated against hotlists assigned to the ALPR Manager because they would apply to all the Sharps controlled by the role. For example, if you have a hotlist of stolen vehicles assigned to the ALPR Manager, any plate read not on that list would generate a *No match* event. Since the majority of the plates read by the SharpV will not be stolen vehicles, *No match* events would be generated for nearly every plate read.

ALPR access control overview:

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

Configuring access control using vehicle license plate credentials

If a SharpV ALPR camera is mounted so that it can read the license plates of vehicles stopped a garage door or parking lot gate, you can configure Security Center to grant or deny a vehicle access based on its license plate number.

Before you begin

- Learn about ALPR access control on page 1048.
- Get a fixed AutoVu™ system up and running.

What you should know

- To capture license plate numbers, the system can use AutoVu SharpV cameras, or cameras supported by the Flexreader™ plugin. For more details, see the *AutoVu Flexreader User Guide*.
- You can deploy an ALPR-based access control solution in a variety of ways. The example of a university campus is used to show you how you can customize a solution that is specific to your deployment.

  In the hypothetical university campus, the following rules apply:

  - **Faculty:** Can park in Lot A and Lot B.
  - **Students:** Can park in Lot B.
  - **Management:** Can park in Lot C.
  - **Maintenance:** Can park in Lot B on weekdays from 6:00 pm to 10:00 pm.
  - **Guests:** Can park in any lot with approval from security.
  - **Scofflaws:** Cannot park anywhere on campus, and security must be alerted if seen.

To set up access rules for parking facilities:

1. Name the Sharp entities.

   Security Center automatically detects all Sharp cameras connected to the network, but you should name each camera according to its function or location. In our example, use the names *Sharp Lot A*, *Sharp Lot B*, and *Sharp Lot C*.

   NOTE: Configuration is simpler when all Sharp cameras are on the same ALPR Manager. However, if the Sharp cameras are on multiple ALPR Managers, you must assign your hotlists accordingly.
2. Turn on hotlist matching for the ALPR Manager controlling your Sharp cameras.
3. Create and configure your hotlists.

   Name each hotlist according to its contents. In the university campus example, use the names *Faculty*, *Students*, *Management*, *Maintenance*, and *Scofflaws.*

   NOTE: In the university example, *Guests* represent anyone that shows up unannounced. Therefore, they are they are not included on any hotlist.
4. Create a schedule.

   For example, if you want the *Maintenance* staff to only have access to your parking lot between 6:00 pm and 10:00 pm, you must create a schedule in Security Center that reflects that. You'll use this schedule later when you create your event-to-actions.

5 Assign your hotlists to Sharp cameras and the ALPR Manager as follows:
   - *Faculty* to *Sharp Lot A* and to *Sharp Lot B*.
   - *Students* to *Sharp Lot B*.
   - *Management* to *Sharp Lot C*.
   - *Scofflaws* and *Maintenance* to the ALPR Manager.

   NOTE: The *Maintenance* hotlist must be assigned to the ALPR Manager because it depends on a schedule. All hotlists that you combine with schedules must be assigned to the ALPR Manager.

6 (Optional) If you have only one ALPR Manager on your system, unassign the *Faculty*, *Students*, and *Management* hotlists from the ALPR Manager.

   When you have only one ALPR Manager, new hotlists are assigned to that ALPR Manager by default (new hotlists are left unassigned if you have multiple ALPR Managers). When you assign a hotlist to a Sharp, Security Center does not automatically unassign it from the ALPR Manager; you must do it manually. Otherwise you will get duplicate match events from the other Sharp cameras.

   Example: If you assign the *Students* hotlist to *Sharp Lot B*, but forget to unassign it from the ALPR Manager, a plate read from that list by *Sharp Lot B* will also trigger matches on *Sharp Lot A* and *Sharp Lot C*.

7 Configure event-to-actions for the *Sharp Lot A*, *Sharp Lot B*, and *Sharp Lot C* cameras.

8 Configure event-to-actions for the *Scofflaws* and *Maintenance* hotlists.

Access to the parking lot is now automated for permitted vehicles, and actions are taken when unknown or scofflaw vehicles are detected.

Creating event-to-actions for ALPR events or hotlist events

To make sure that some vehicles are granted access to the parking facility, and that other actions are taken for unknown or scofflaw vehicles, you must create event-to-actions that are triggered based on *License plate hit* and *No match* events generated by Sharp cameras.

What you should know

- When you assign a hotlist to an ALPR Manager, all SharpV cameras controlled by the ALPR Manager can match against the hotlist and trigger the event-to-action. When you assign a hotlist to an individual SharpV camera, only that specific SharpV camera can trigger the event-to-action.

To create event-to-actions for Sharp-related events:

1 Open the *System* task, and click the **General settings** view.

2 Go to the *Actions* page.

3 From the **Domain** list, select **ALPR**.

4 Click **Add an item** (➕).

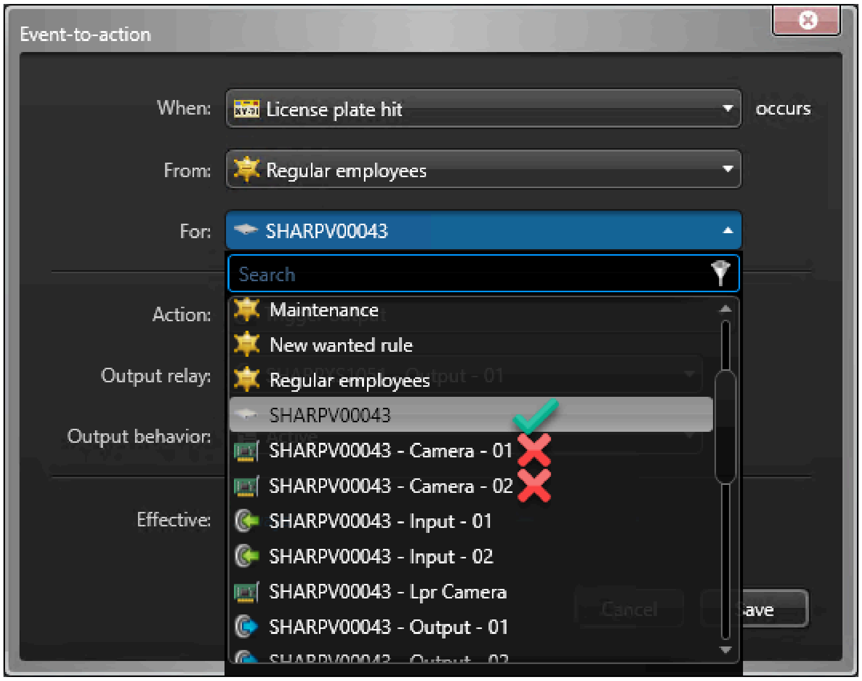
5 From the **When** list in the *Event-to-action* dialog box, select the event type *License plate hit* or *No match*.

6 From the **From** list, select a hotlist.

   The **From** and **For** fields can contain either a hotlist or a Sharp camera, and you do not need to fill both fields. For example, to create an event-to-action that is triggered when a hit is detected for your *regular employees* hotlist, no matter what camera it is detected on, select the *regular employees* hotlist in either the **From** or **For** field and select **Clear selection** for the other field so that it appears as *Any entity*.

7 From the **For** list, select the Sharp camera to which you want to assign the hotlist.

NOTE: Select the Sharp video unit, not the individual cameras (for example, *Camera - 01*) under the unit.



Event-to-action

When: License plate hit occurs

From: Regular employees

For: SHARPV00043

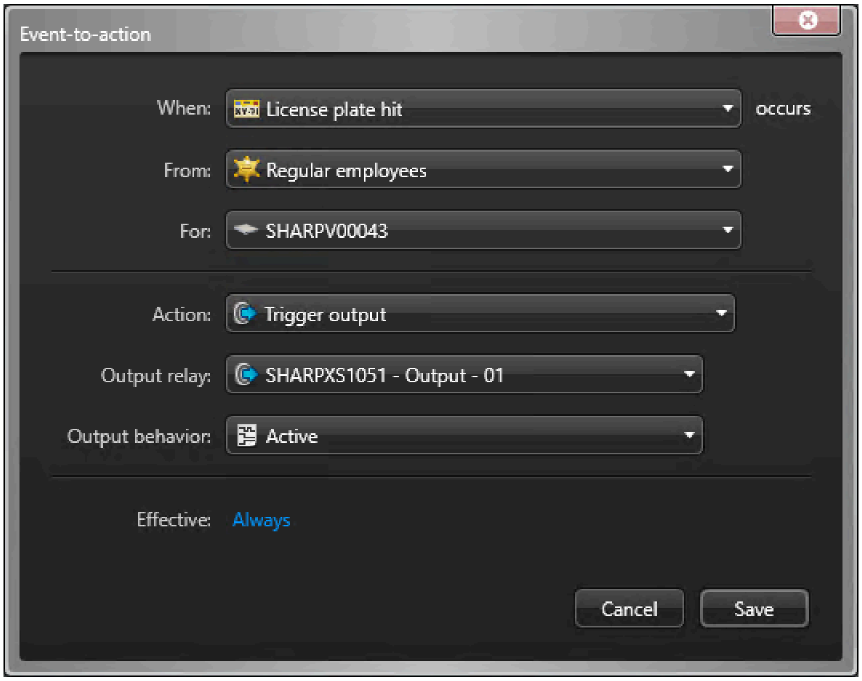
8 Select the **Action** and attributes for each type of event.

- For *License plate hit* events, select **Trigger output**, and then select the **Output relay** and **Output behavior** required to grant access to the parking lot (for example, open a gate).
- For *No match* events, select the action you want Security Center to take. For example, you can send a message to a particular Security Center user, or use another *Trigger output* action to activate a security intercom at the gate.

9 In the **Effective** option, click **Always**, and select a schedule when this event-to-action is active.

If the event occurs outside of the defined schedule, the action is not triggered.

10 Click **Save**.



Event-to-action

When: License plate hit occurs

From: Regular employees

For: SHARPV00043

Action: Trigger output

Output relay: SHARPXS1051 - Output - 01

Output behavior: Active

Effective: Always

Related Topics

ALPR access control on page 1048
Creating event-to-actions on page 212

47

Free-Flow

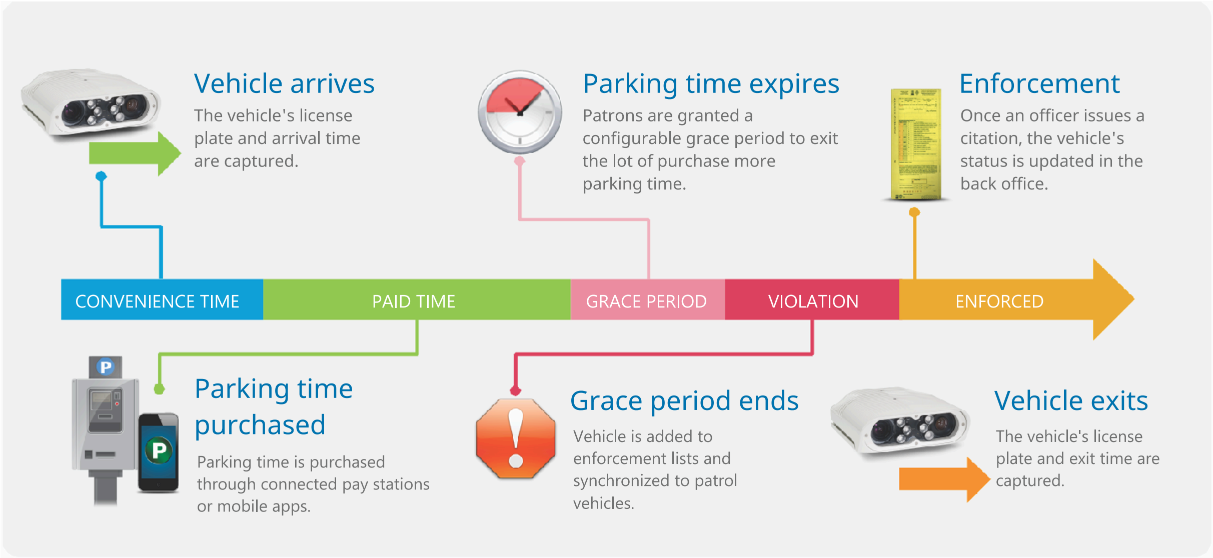
This section includes the following topics:

About Free-Flow

In parking facilities where the entrance and exit are monitored by Sharp ALPR units, the AutoVu™ Free-Flow feature in Security Center increases parking enforcement efficiency by providing a real-time inventory of parking violations.

Using the Free-Flow feature, you can manage *transient parking*, where vehicle owners pay for hourly parking, and *contract permit parking* for employee, student, or residential parking. The system records the license plates of vehicles entering and exiting the parking zone and compares them to the list of permit holders and payments received through Pay-by-Plate Sync enabled pay stations and mobile parking apps. Vehicles parked beyond their purchased time are automatically marked as violations awaiting enforcement.

If parking attendants are responsible for manually issuing citations, then based on the information provided by the Free-Flow system, you can increase operational efficiency by dispatching attendants to the parking facilities that contain the highest number of violations.


Vehicle arrives
The vehicle's license plate and arrival time are captured.
Parking time expires
Patrons are granted a configurable grace period to exit the lot of purchase more parking time.
Enforcement
Once an officer issues a citation, the vehicle's status is updated in the back office.
CONVENIENCE TIME
PAID TIME
GRACE PERIOD
VIOLATION
ENFORCED
P
P
Parking time purchased
Parking time is purchased through connected pay stations or mobile apps.
Grace period ends
Vehicle is added to enforcement lists and synchronized to patrol vehicles.
Vehicle exits
The vehicle's license plate and exit time are captured.

Free-Flow lets you do the following:

- Using the Pay-by-Plate Sync plugin, Free-Flow can also integrate with third-party parking permit providers. You can consolidate multiple third-party license plate-enabled parking (LEP) systems into a single parking solution. Vehicle owners then have the option to pay for metered parking and to extend their parking time before they are in violation.
- You can merge Pay-by-Plate Sync's dynamic permits with Security Center static permits. This allows you to define weekly or monthly permits in addition to using permits from third-party providers.
- The system can generate an XML file of violations that your ticketing management system can use.
- You can generate violation reports in PDF, CSV, and Excel formats, as well as on-screen reports. If your parking installation includes a Genetec Patroller™ unit (the in-vehicle application), the system can generate a hotlist of vehicles in violation to be used for mobile enforcement.
- If you need to manage parking lots where parking spots are leased to tenants, you can install the Free-Flow plugin.
  - For more information on the Free-Flow plugin, see the *AutoVu™ Free-Flow Plugin Guide*.
  - For more information on configuring multi-tenant parking, see Configuring Free-Flow multiple tenants with additional transient parking on page 1069.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

About parking sessions

The AutoVu™ Free-Flow feature in Security Center uses parking sessions to track each vehicle's stay in a parking zone.

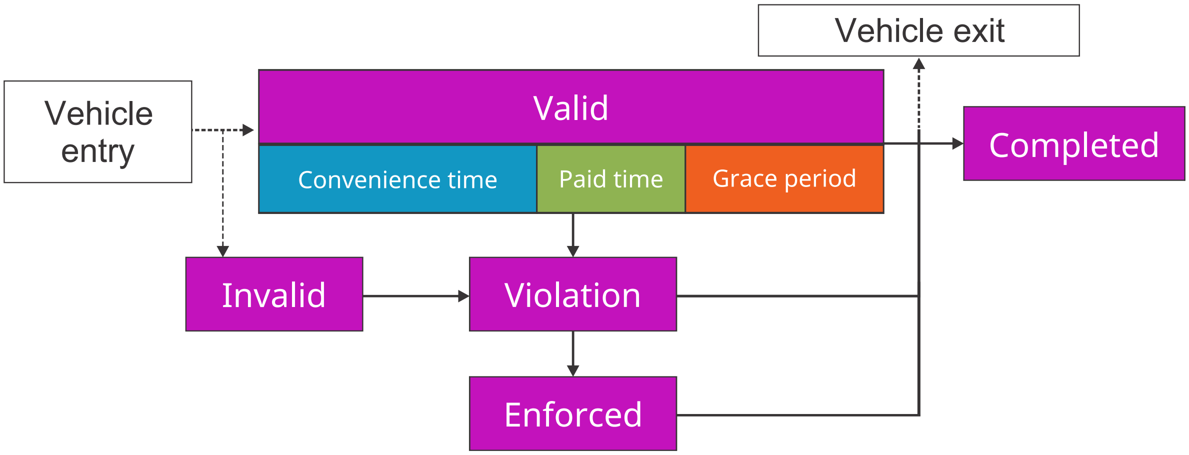
The following terms are important when setting up Free-Flow parking zones:

- **Convenience time:** The convenience time is a configurable leeway time before a vehicle starts to be charged after entering the parking zone. For example, if you need to set up a 2-hour free parking period before paid time or parking enforcement takes effect, you would set the convenience time for 2 hours. For parking lots where parking enforcement begins immediately, you would still need to set a short convenience time to allow vehicle owners time to find a parking spot and purchase parking time before parking enforcement begins.
- **Default expiration delay:** The default expiration delay is used for permits supplied by Pay-by-Plate Sync that do not include an expiration. In this case, AutoVu™ Free-Flow checks with the parking permit provider to see if the permit is still valid. Increasing this value reduces the frequency of the permit checks. For example, if the parking lot charges for parking in increments of 15 minutes, and you also set the default expiration delay to 15 minutes, the system validates the permit with the parking provider every 15 minutes.
- **Grace period:** You can add a grace period to a parking session for purposes of lenient enforcement. Following the expiration of the vehicle’s paid time or convenience time, the grace period gives extra time before a parking session is flagged as a *Violation*.
- **Maximum session time:** Setting a maximum session time helps to improve parking lot occupancy statistics. When a vehicle exceeds the maximum session time, it is assumed that the vehicle's plate was not read at the exit and the vehicle is no longer in the parking zone. The parking session appears in reports generated from the *Parking sessions* task with the *State reason: Maximum session time exceeded*.
- **Paid time:** The paid time stage of a parking session begins when the *convenience time* expires. Vehicle owners can purchase parking time through a pay station or mobile app, and the payment system can be provided by integrated third-party parking permit providers.
- **Parking rule:** A parking rule defines how and when a parking session is either considered to be valid or in violation.
- **Parking session states:** A vehicle's parking session is divided into four states: *Valid* (including convenience time, paid time, and grace period), *Violation*, *Enforced*, and *Completed*. When a vehicle parks in a parking zone, its parking session progresses through the parking session states based on the timing that is configured for the parking rule, the validity of the paid time, and whether the vehicle's parking session incurs a violation.
- **Parking zone:** The parking zones that you define in Security Center represent off-street parking lots where the entrances and exits are monitored by Sharp cameras.
- **Parking zone capacity:** The parking zone capacity is the maximum number of vehicles that can be parked in a parking zone.
- **Parking zone capacity threshold:** The parking zone capacity threshold setting determines at what point a *capacity threshold reached* event is generated. For example, if you lower the threshold to 90%, the system generates an event when the parking zone reaches 90% capacity.

Parking session states

A vehicle's parking session is divided into states, to show the progression of the owner's parking visit. If you need to monitor and investigate parking zones, or if you configure parking zones and rules, it is important to understand how a parking session progresses through these states.

When a vehicle parks in a parking zone, the states that a parking sessions moves through depends on whether there is a parking violation. The following diagram shows the possible states of a parking session:



- **Valid:** A parking session moves to the *valid* state because:
  - The vehicle's license plate is read at the parking zone entry.

    NOTE: Depending on how the parking rule is configured, the *valid* state can include *convenience time*, *paid time*, and a *grace period*.
- **Violation:** A parking session moves to the *violation* state because:
  - The valid time expires. This can include a combination of the *convenience time*, *paid time*, and *grace period* that are configured for the parking rule.
- **Enforced:** A parking session moves to the *enforced* state because:
  - The violation can be automatically updated by Genetec Patroller™ or manually updated by the Security Desk operator.
- **Completed:** A parking session moves to the *completed* state because:
  - The vehicle exits the parking zone. The parking session state is *completed* no matter what state it is in when the vehicle exits the parking zone.
  - The parking zone's inventory is updated.
  - The vehicle re-enters the parking zone. This can indicate that in the vehicle's previous parking session, the plate was not read at the parking zone exit.
  - The vehicle exceeded the *maximum session time* that is defined for the parking zone.

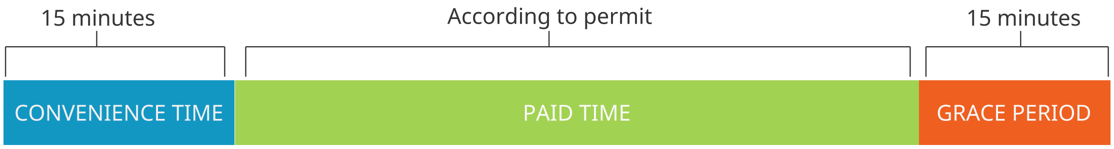
Common parking scenarios for Free-Flow

Using the AutoVu™ Free-Flow feature in Security Center, you can customize the system to meet the requirements of your parking rules.

The following examples show how Free-Flow can be used to fit common parking scenarios.

Transient parking

In the *transient parking* scenario, when a vehicle enters the parking lot, the owner must immediately purchase parking time.

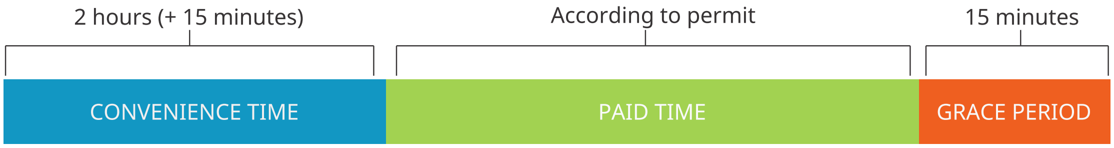


About this scenario:

- A short *convenience time* can be added to allow the vehicle owner time to find a parking spot and purchase parking time.
- If the owner has not purchased parking time by the end of the 15 minute convenience time and the 15 minute grace period, the parking session is flagged as a *Violation*.
- If the owner purchases parking time but exceeds the time purchased and the grace period, the vehicle is flagged as a *violation*.

Transient parking with a free parking period

In the transient parking scenario, vehicles can park without a permit for the first 2 hours. If the vehicle owner plans to park the vehicle in the lot for more than 2 hours, parking time must be purchased.

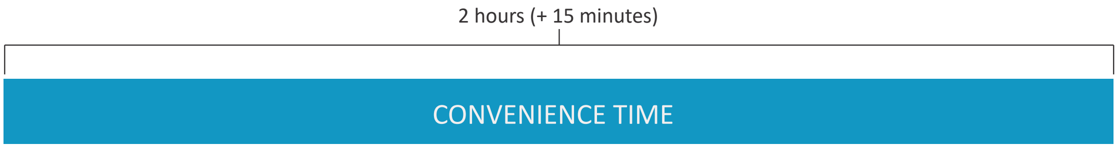


About this scenario:

- The convenience time is configured for 2 hours.
- If the owner has not purchased parking time by the end of the 2 hour convenience time and the 15 minute grace period, the parking session is flagged as a *violation*.
- If the owner purchases parking time but exceeds the time purchased and the grace period, the vehicle is flagged as a *violation*.

Overtime parking

In an *overtime* scenario, any vehicle can park for a maximum of 2 hours. Drivers cannot purchase additional parking time.

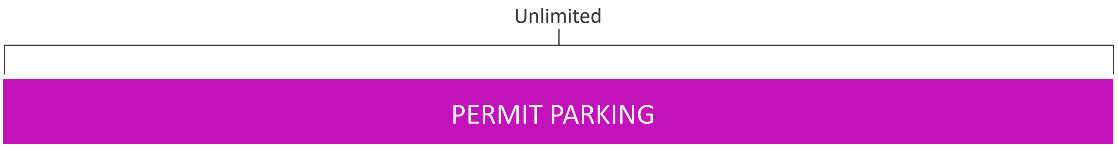


About this scenario:

- The convenience time is configured for two hours.
- If the owner parks the car for more than the 2 hour convenience time and the 15 minute grace period, the parking session is flagged as a *Violation*.

Contract permit parking

In the *contract permit parking* scenario, only drivers with monthly permits can park in the parking zone. A Security Center permit is used to grant vehicles access to the parking zone.

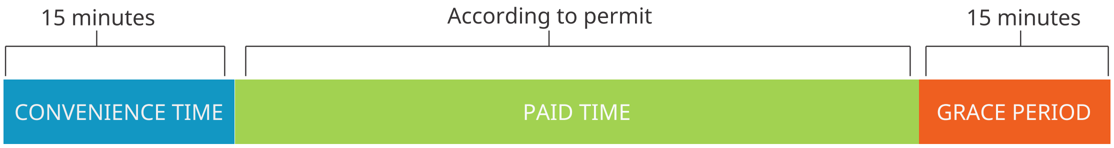


About this scenario:

- Because there is no paid time, the parking rule includes only the default minimum of 1 minute, and no grace period is configured.
- Using this configuration, you can track how long each vehicle stays in the parking zone.

Static permit and transient parking

In this scenario, a permit is used to grant vehicles access to the parking zone, and when an unknown vehicle enters the parking lot, the driver must immediately purchase parking time.



About this scenario:

- The transient parking is configured as in the example *Transient parking with a free parking period*.
- For parking sessions that use a Pay-by-Plate Sync static permit, the static permit follows the same convenience time and grace period that are configured for the transient permit parking rule, however, as they do not apply to static permits, the permit will not go into violation as long as the permit is valid.
- If the parking lot is configured to use permit restrictions, the system checks the validity of the parking sessions when the restriction takes affect.
- If the parking lot is configured to use permits that do not include a restriction, the system validates the parking sessions every fifteen minutes (default) as defined by the parking rule's **Default expiration delay** setting.

Parking zone events

During a vehicle's parking session, several events and sub-events are triggered based on the parking rules that are applied to the parking zone.

- **Events:** Administrators can use events to create event-to-actions for the parking zone. For example, you can configure an event-to-action that sends an email or triggers an alarm when a *violation detected* event is generated.
- **Sub-events:** Sub-events appear in the Security Desk *Parking zone activities* report. You can filter the report for specific sub-events, but you cannot include sub-events in an event-to-action.

The following events and sub-events are available:

Events	Sub-events
Capacity threshold reached	Not applicable
Convenience time started	Not applicable
Grace period started	• Convenience time expired • Paid time invalid
Inventory reset	Not applicable
Paid time started	• Paid time valid • Unable to validate paid time
Session completed	• Inventory reset • Maximum session time exceeded • Unknown vehicle exited • Vehicle exited • Vehicle re-entered • Read edited • Rule deleted
Session started	• Unknown vehicle exited • Vehicle entered
Validating paid time	• Convenience time expired • Paid time expired • Read edited
Violation detected	• Convenience time expired • Grace period expired • Paid time invalid • Shared permit match
Violation enforced	Not applicable

Linking permits using the Free-Flow plugin

By linking permits in specific ways in the AutoVu™ Free-Flow plugin, you can set up the system to use Pay-by-Plate Sync with static or dynamic permits, or you can also group permits so that they appear as one entity on the dashboard.

Static permits with Pay-by-Plate Sync

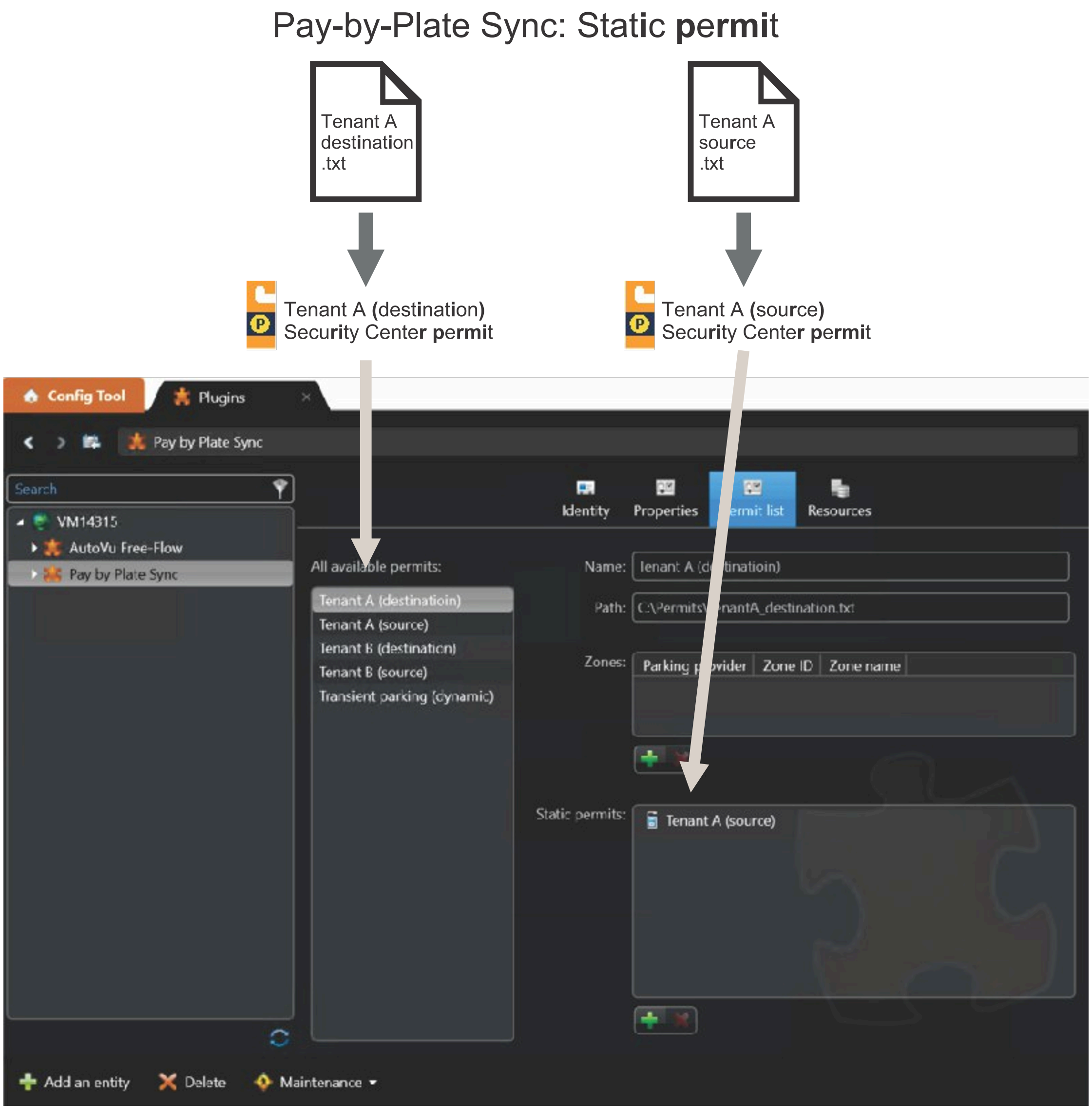
In a system that uses the Pay-by-Plate Sync plugin, a static permit holds a list of vehicle license plates that is not updated by a third-party permit provider. For example, a list of employee vehicles that are authorized to park in the lot are manually maintained as a static list.

To create a tenant that uses a static permit list, you must create two Security Center permits: a *source* permit, and a *destination* permit.

TIP: Name the Security Center permits according to their use as *source* or *destination* permits. This can help you to avoid assigning the wrong Security Center permits when you link them in Pay-by-Plate Sync. If you assign the wrong permits, you might overwrite your source plate list.

The *source* and *destination* Security Center permits are then linked through the Pay-by-Plate Sync plugin.

In the following Pay-by-Plate Sync example, the *destination* permit is selected from the **All available permits** list, and the *source* permit is added as the **Static permit**.



All available permits:

- Tenant A (destinatioin)
- Tenant A (source)
- Tenant B (destination)
- Tenant B (source)
- Transient parking (dynamic)

Name: Tenant A (destinatioin)

Path: C:\Permits\TenantA_destination.txt

Zones:

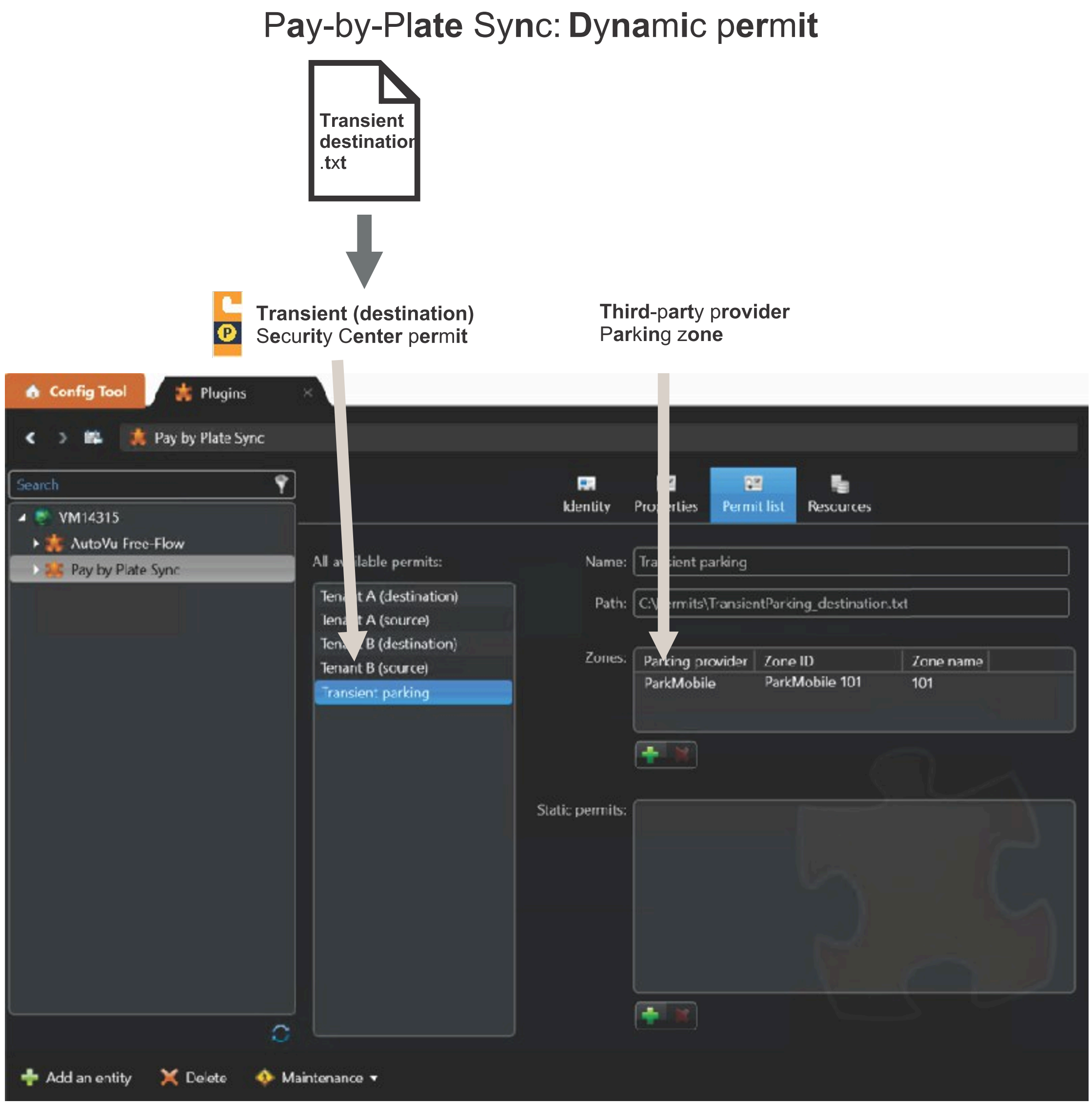
Parking provider	Zone ID	Zone name

Static permits: Tenant A (source)

Dynamic permits with Pay-by-Plate Sync

In a system that uses the Pay-by-Plate Sync plugin, a dynamic permit holds a list of vehicles that is updated by a third-party permit provider. For example, in a system where vehicle owners pay for parking at a kiosk or using a mobile phone app, the list of vehicles are dynamically managed by a third-party permit provider.

To create a dynamic permit, you must create a Security Center *destination* permit and link it to the permit provider zone in Pay-by-Plate Sync.



All available permits:
- Tenant A (destination)
- Tenant A (source)
- Tenant B (destination)
- Tenant B (source)
- Transient parking

Name: Transient parking

Path: C:\Permits\TransientParking_destination.txt

Zones:

Parking provider	Zone ID	Zone name
ParkMobile	ParkMobile 101	101

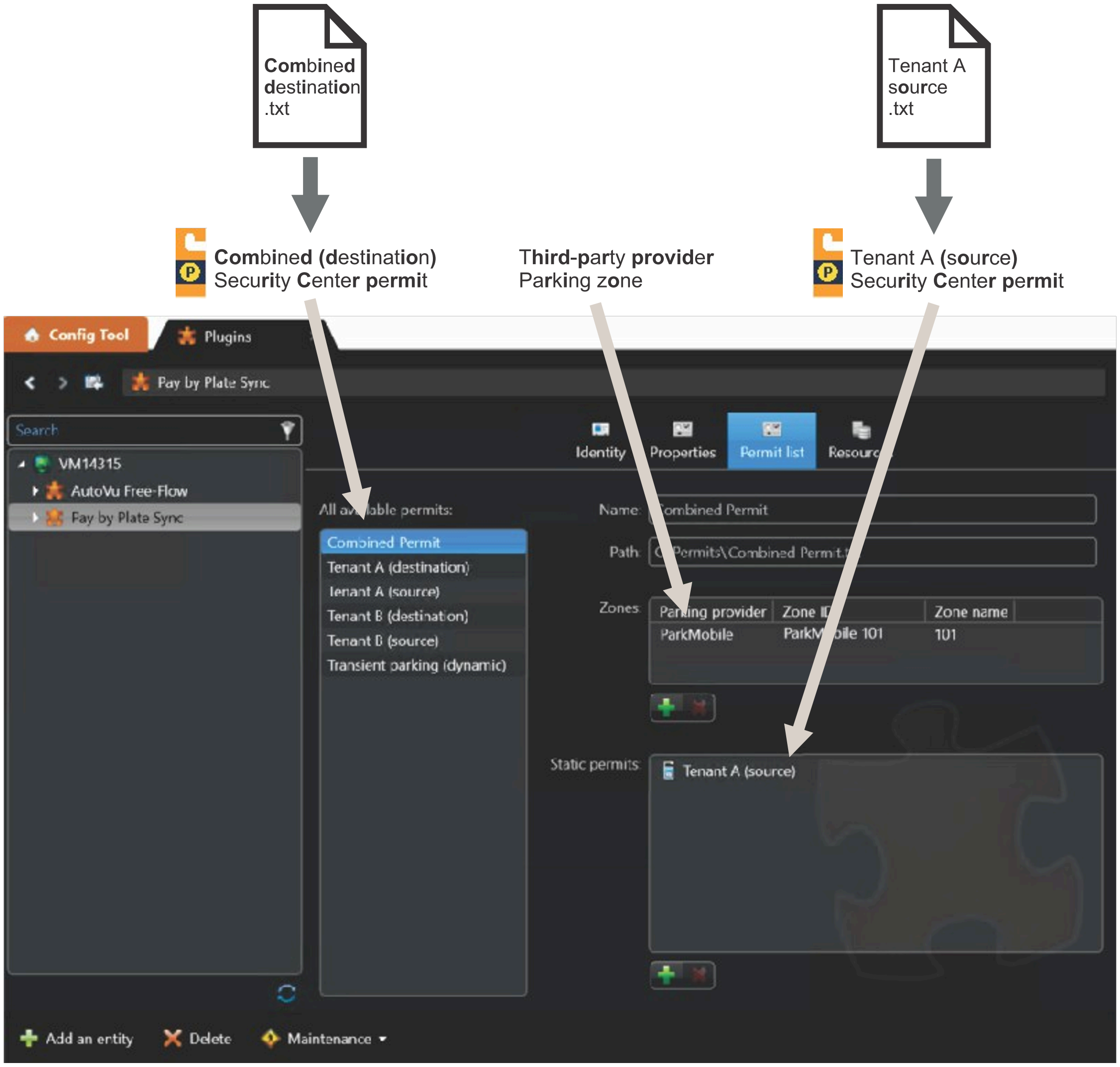
Static permits:

Grouping permits

In certain situations, you might want a group of permits to appear together as one entity in the *Dashboard* page of the AutoVu™ portal. In an example where a law firm (tenant) has two static permit lists for employee plates and VIP plates, you can group the permits in Pay-by-Plate Sync so that their statistics appear together as *Law firm* in the dashboard.

In the following example, a static permit and a dynamic permit are linked in Pay-by-Plate Sync.

Pay-by-Plate Sync: **Combined permit**



Name: Combined Permit

Path: C Permits\Combined Permit.t

Zones:

Parking provider	Zone ID	Zone name
ParkMobile	ParkMobile 101	101

Static permits: Tenant A (source)

Configuring Free-Flow for transient parking

You can configure an AutoVu™ Free-Flow system to manage transient parking at a parking facility. In this scenario, the owner installs kiosks and drivers must purchase parking time as soon as their vehicles enter the parking lot.

Before you begin

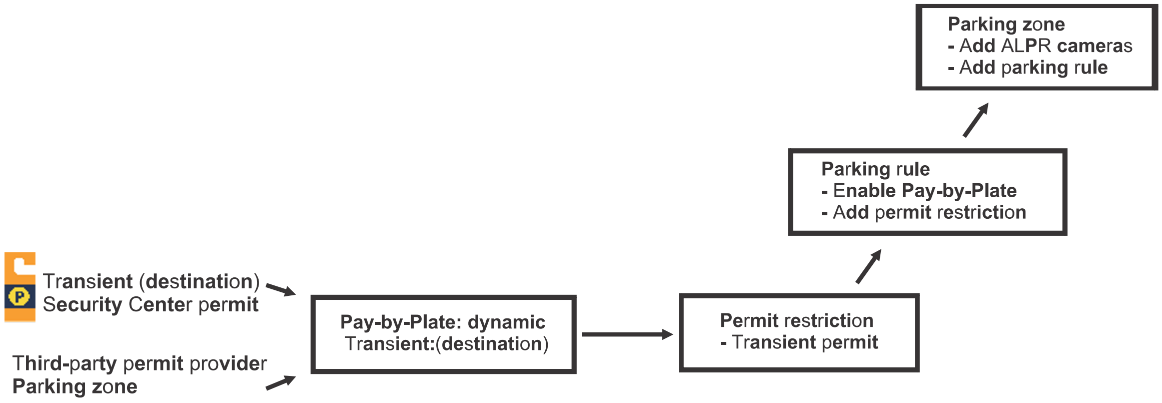
- Read the document Genetec AutoVu™ Free-Flow Best Practices.
- Install a compatible version of the Pay-by-Plate Sync plugin.

  NOTE: In a *transient parking* scenario, the Free-Flow plugin is not required because you do not need to manage multiple tenants. All configuration is done in Config Tool.

  For more information on compatible versions of the plugin, see the "Free-Flow plugin compatibility" topic in the*Free-Flow Plugin Guide*.

What you should know

The following diagram shows a scenario where Free-Flow manages transient parking:



To configure a parking facility for transient parking:

1 Configure the general settings for Free-Flow.

2 Create a *destination* Security Center permit for the parking facility.

For more information, see Creating parking permits on page 1139.

For more information on source permits and destination permits, see Linking permits using the Free-Flow plugin on page 1062.

3 Configure the permit to be used with Pay-by-Plate Sync.

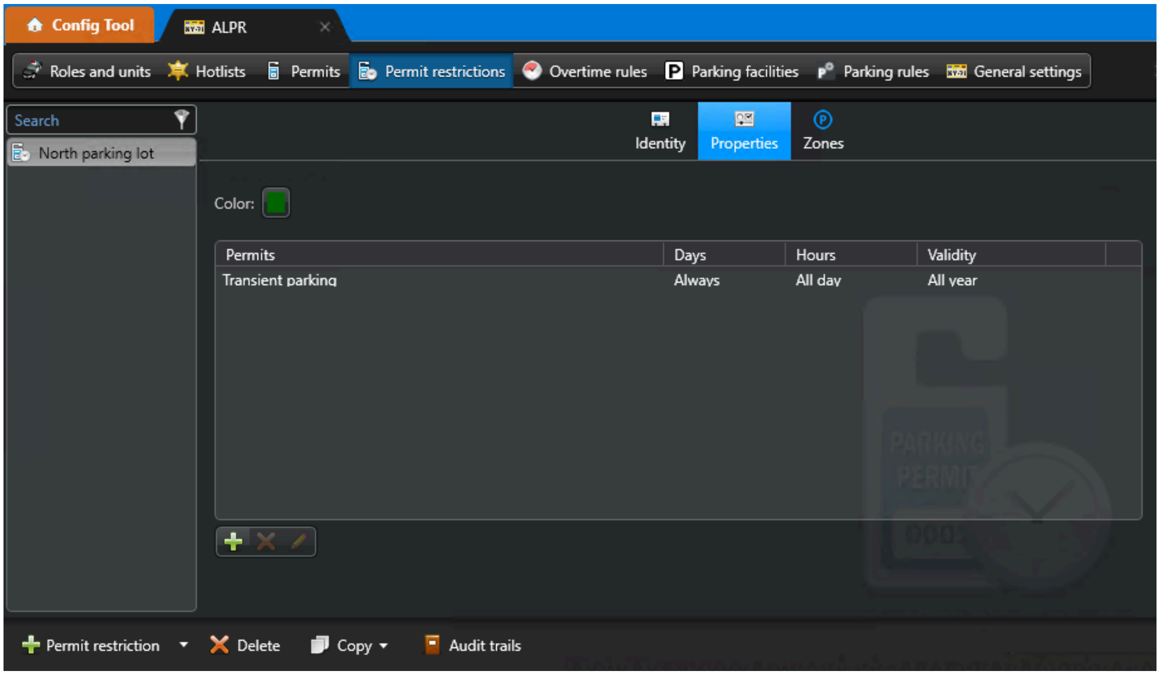
For more information, see Configuring a Security Center permit for Pay-by-Plate Sync in the *Pay-by-Plate Sync Plugin Guide*.

IMPORTANT:

- Pay attention to the instructions on configuring the attributes of the permit. The permits must either include four attributes (*Category*, *PlateState*, *PlateNumber*, and *PermitID*) or six attributes (*Category*, *PlateState*, *PlateNumber*, *PermitID*, *EffectiveDate*, and *ExpiryDate*)

  If you include the *EffectiveDate*, and *ExpiryDate* attributes, the fields cannot be empty.
- The *PermitID* field cannot be empty.
- Pay attention to the instructions on configuring the date format.

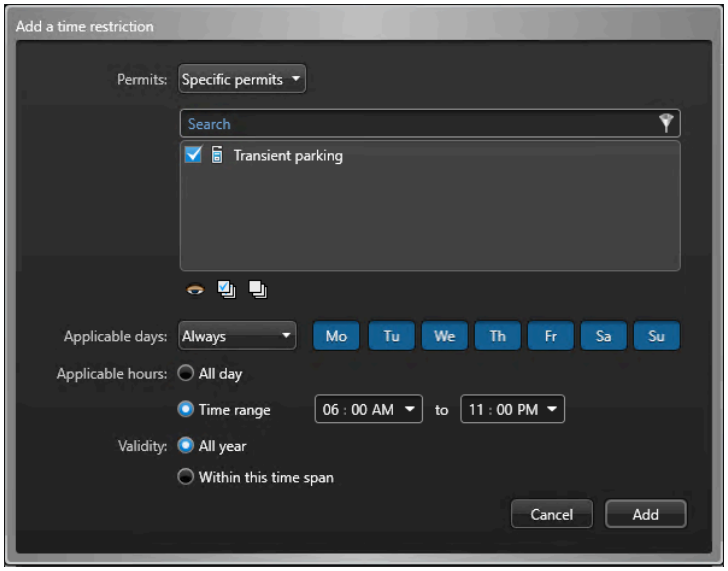
4 Create a permit restriction for the parking lot that includes the *destination* Security Center permit.



Color: 🟩

Permits	Days	Hours	Validity
Transient parking	Always	All day	All year

5 Configure the parking lot's permit restriction.
In this example, transient parking is available from 6 am to 11 pm every day.



Add a time restriction

Permits: Specific permits

☑ Transient parking

Applicable days: Always Mo Tu We Th Fr Sa Su

Applicable hours: ○ All day

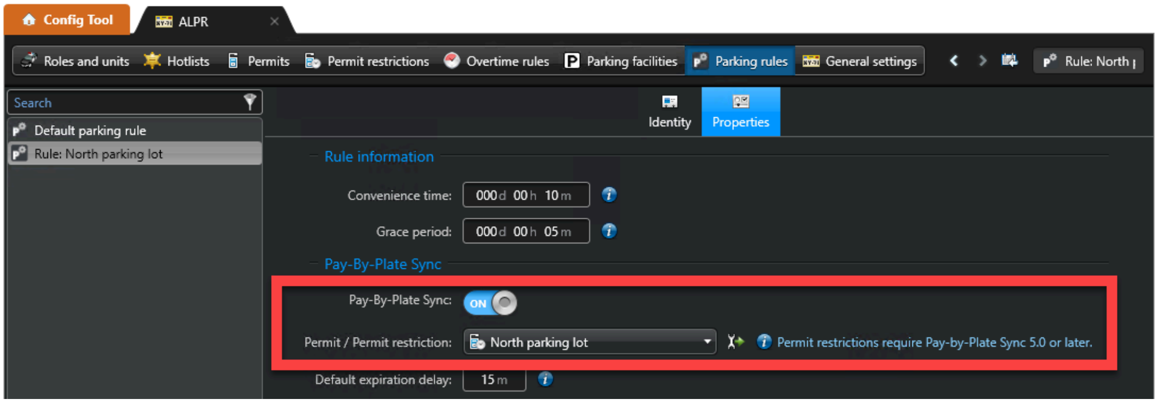
● Time range 06 : 00 AM to 11 : 00 PM

Validity: ● All year

○ Within this time span

6 Create a parking rule.

In this step, you enable Pay-by-Plate Sync and link the permit restriction.



Rule information

Convenience time: 000 d 00 h 10 m

Grace period: 000 d 00 h 05 m

Pay-By-Plate Sync

Pay-By-Plate Sync: ON

Permit / Permit restriction: North parking lot

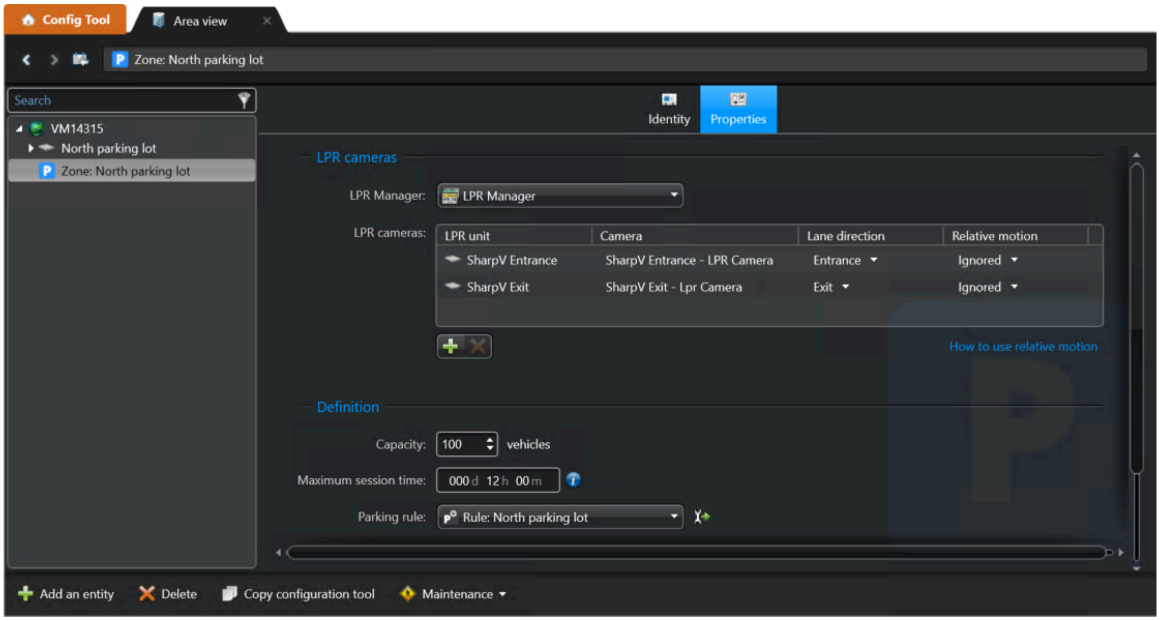
Permit restrictions require Pay-by-Plate Sync 5.0 or later.

Default expiration delay: 15 m

7 Create a parking zone.

In this step, you associate cameras and a parking rule with the parking zone and you set the vehicle capacity.

If you need to send a list of vehicles whose parking sessions have reached a state of *Violation* to a parking enforcement patrol vehicle, you can link the parking zone to a violation hotlist.



LPR cameras

LPR Manager: LPR Manager

LPR cameras:

LPR unit	Camera	Lane direction	Relative motion
SharpV Entrance	SharpV Entrance - LPR Camera	Entrance	Ignored
SharpV Exit	SharpV Exit - Lpr Camera	Exit	Ignored

How to use relative motion

Definition

Capacity: 100 vehicles

Maximum session time: 000 d 12 h 00 m

Parking rule: Rule: North parking lot

Configuring Free-Flow multiple tenants with additional transient parking

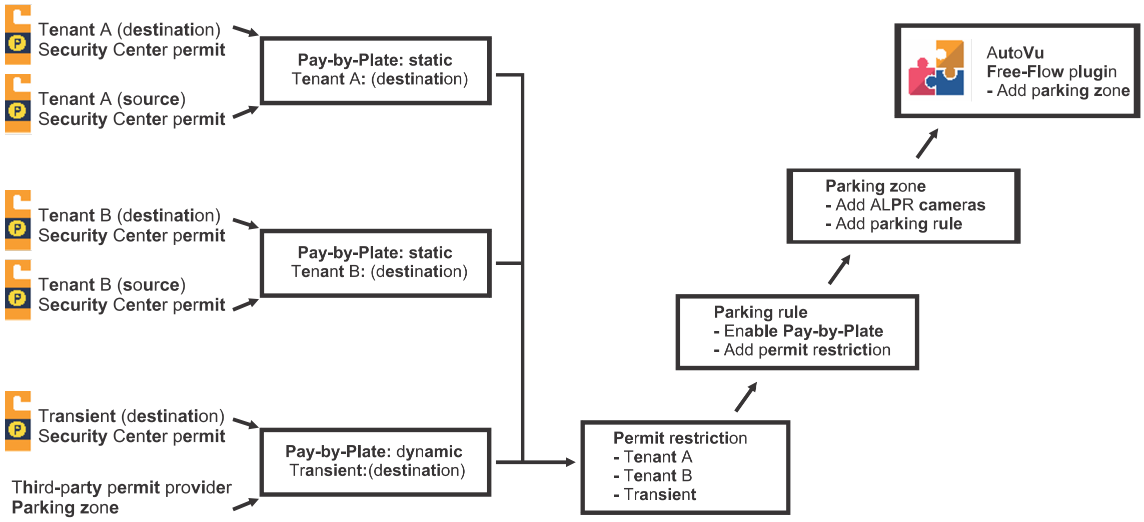
You can configure an AutoVu™ Free-Flow system to manage a multi-tenant parking facility where parking spaces are leased to nearby businesses. In this scenario, the remainder of the spaces can be used for hourly transient parking.

Before you begin

- Read the document Genetec AutoVu™ Free-Flow Best Practices.
- Contact your AutoVu™ representative to verify that cloud services have been enabled for your account.
- Install a compatible version of the Pay-by-Plate Sync plugin. For more information, see "Pay-by-Plate Sync plugin compatibility" in the *Pay-by-Plate Sync Plugin Guide*.
- Install a compatible version of the Free-Flow plugin. For more information, see "" in the *AutoVu™ Free-Flow Plugin Guide*.

What you should know

- The parking lot occupancy for each tenant appears as a separate circle graph on the dashboard.
- The following diagram shows a scenario where two tenants, for example, a medical clinic and a law firm lease spots in a parking lot and the remainder of the spots are used for hourly transient parking:



To configure a parking facility for multi-tenant parking with additional transient parking:

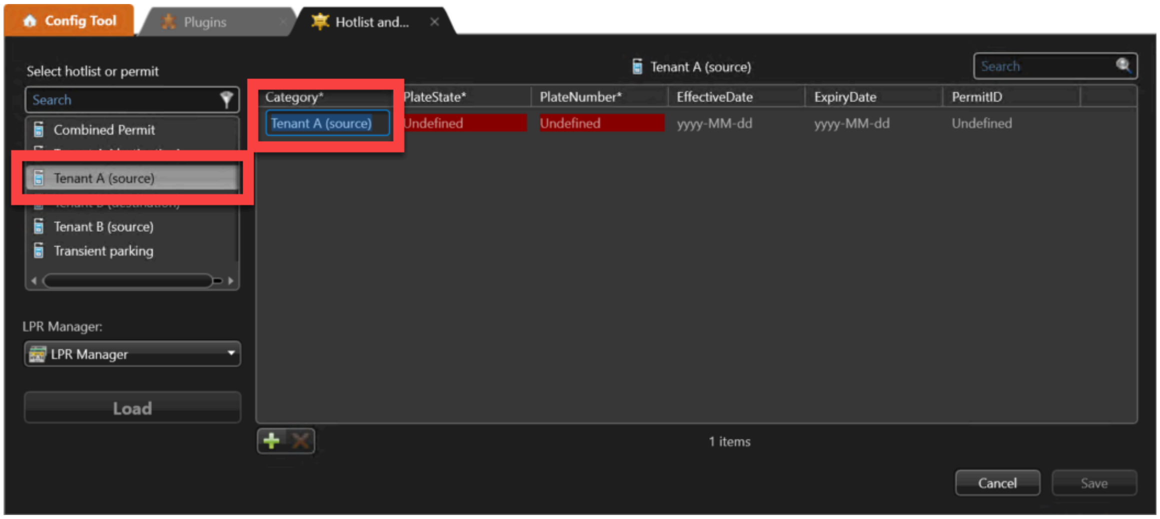
1 Configure the general settings for Free-Flow.

2 Create the required *source* and *destination* Security Center permits for each tenant in the parking lot.

For more information, see Creating parking permits on page 1139.

For more information on source permits and destination permits, see Linking permits using the Free-Flow plugin on page 1062.

IMPORTANT: If you use the *Hotlist and permit editor* to enter vehicle information, the system completes the **Category** field for each row. For more information on the Hotlist and permit editor, see the *Security Center User Guide*. Do not modify this field as it must match the permit name.



Category*	PlateState*	PlateNumber*	EffectiveDate	ExpiryDate	PermitID
Tenant A (source)	Undefined	Undefined	yyyy-MM-dd	yyyy-MM-dd	Undefined

TIP: Name the Security Center permits according to their use as *source* or *destination* permits. This can help you to avoid assigning the wrong Security Center permits when you link them in Pay-by-Plate Sync. If you assign the wrong permits, you might overwrite your source plate list.

3 Configure the Security Center permits to be used with Pay-by-Plate Sync.

For more information, see Configuring a Security Center permit for Pay-by-Plate Sync in the *Pay-by-Plate Sync Plugin Guide*.

IMPORTANT:

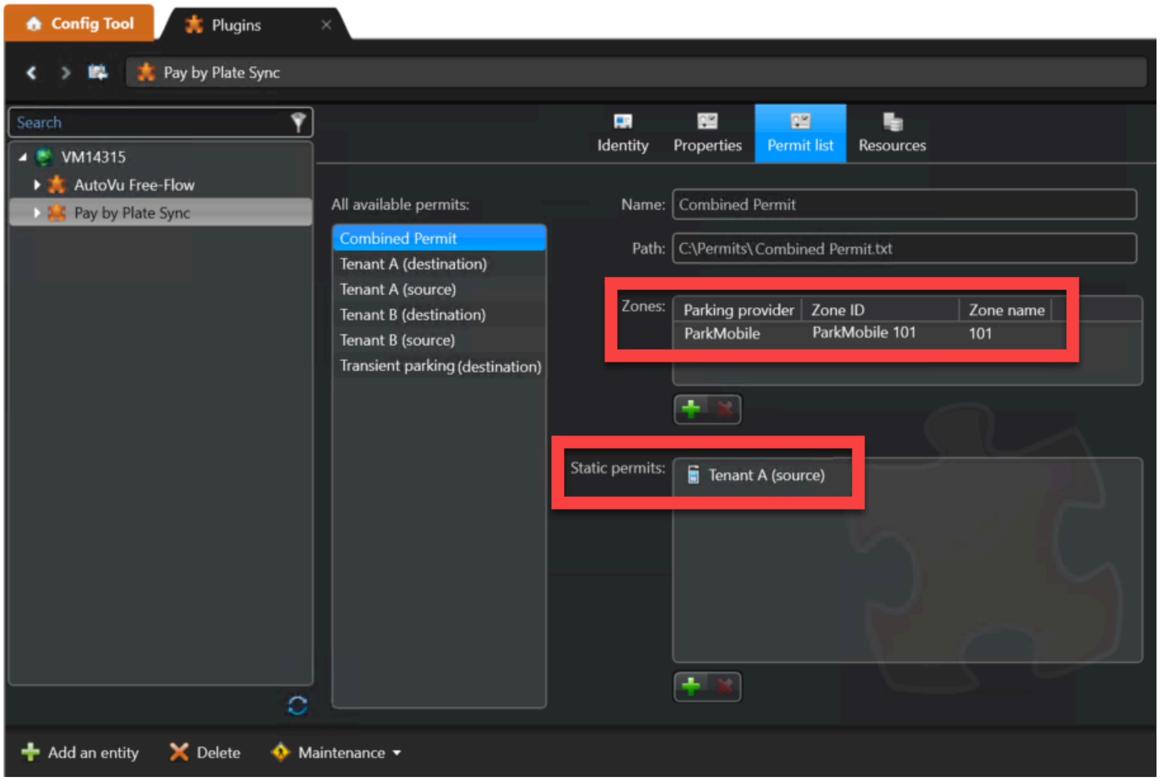
- Pay attention to the instructions on configuring the attributes of the permit. The permits must either include four attributes (*Category*, *PlateState*, *PlateNumber*, and *PermitID*) or six attributes (*Category*, *PlateState*, *PlateNumber*, *PermitID*, *EffectiveDate*, and *ExpiryDate*)
- If you include the *EffectiveDate*, and *ExpiryDate* attributes, the fields cannot be empty.
- The *PermitID* field cannot be empty.

4 In Pay-by-Plate Sync, select each tenant's *destination* Security Center permit and link all of the tenant's *source* permits.

NOTE:

- For more information on which permits you need to link in Pay-by-Plate Sync, see Linking permits using the Free-Flow plugin on page 1062.
- For more information how to link permits in Pay-by-Plate Sync, see "Configuring Pay-by-Plate Sync permit list" in the *Pay-by-Plate Sync Plugin Guide*.

In this example of a Grouped permit, a dynamic parking provider zone and a static permit are linked to the *Combined Permit* Security Center permit in Pay-by-Plate Sync:



All available permits:

- Combined Permit
- Tenant A (destination)
- Tenant A (source)
- Tenant B (destination)
- Tenant B (source)
- Transient parking (destination)

Name: Combined Permit

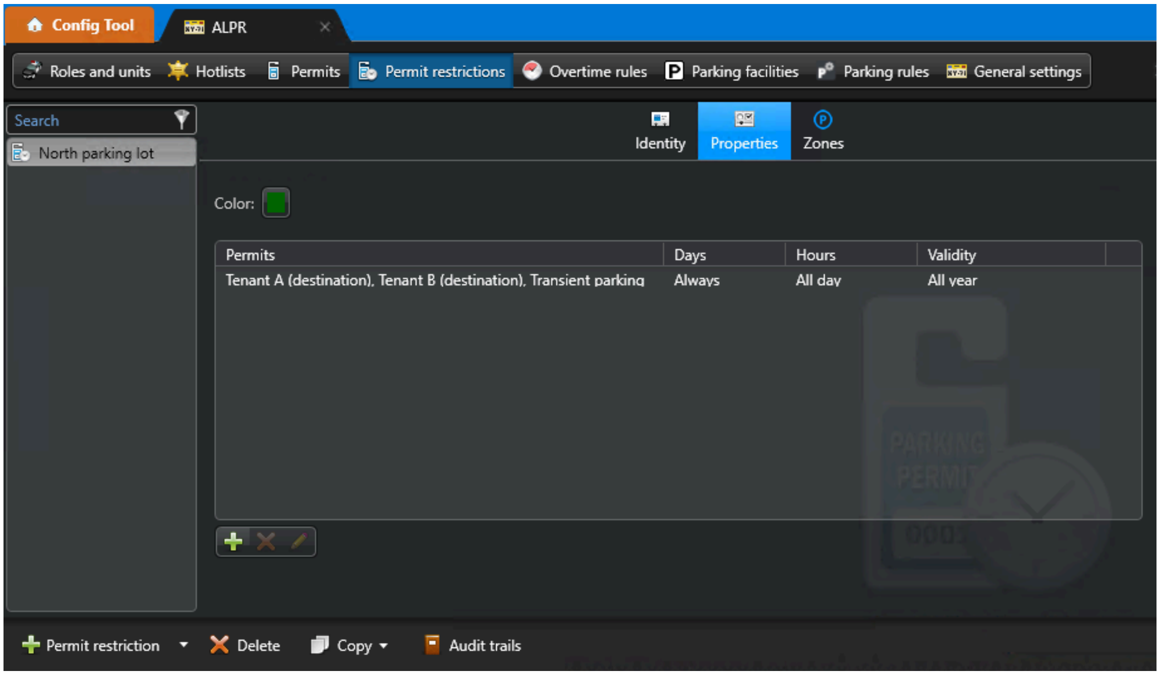
Path: C:\Permits\Combined Permit.txt

Zones:

Parking provider	Zone ID	Zone name
ParkMobile	ParkMobile 101	101

Static permits: Tenant A (source)

5 Create a permit restriction for the parking lot that includes the *destination* Security Center permits for all of the tenants in the parking lot.



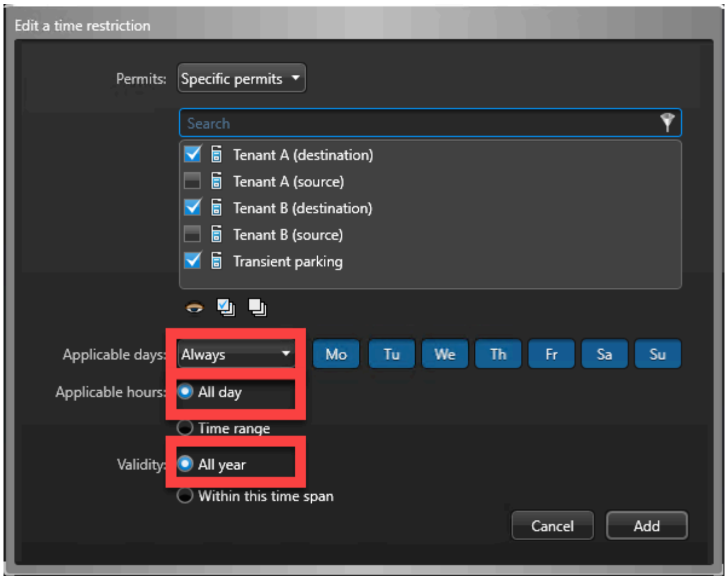
Color: 🟩

Permits	Days	Hours	Validity
Tenant A (destination), Tenant B (destination), Transient parking	Always	All day	All year

6 Configure the parking lot's permit restriction.

IMPORTANT: The Free-Flow plugin ignores any time restrictions configured for the permit restriction. To avoid confusion, configure the time restrictions as follows:

- **Applicable days**: Always
- **Applicable hours**: All day
- **Validity**: All year



Permits: Specific permits

☑ Tenant A (destination)
□ Tenant A (source)
☑ Tenant B (destination)
□ Tenant B (source)
☑ Transient parking

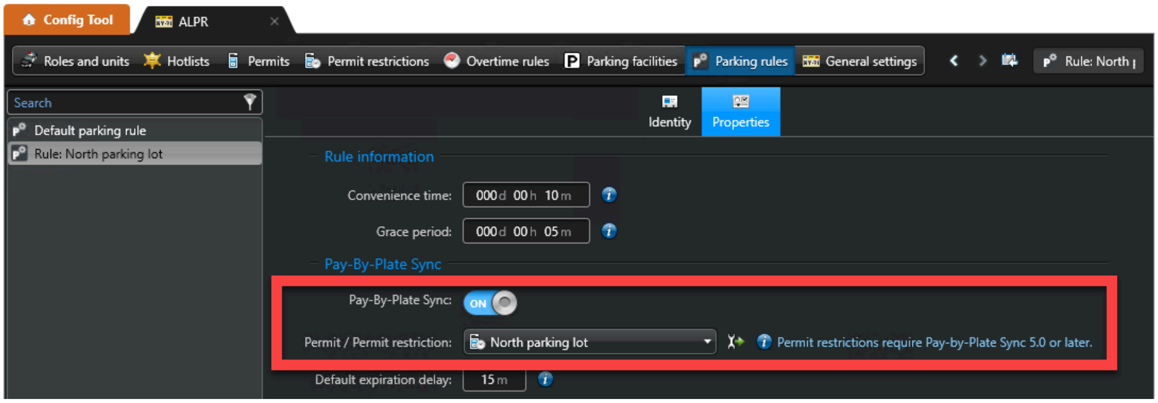
Applicable days: Always

Applicable hours: ● All day ○ Time range

Validity: ● All year ○ Within this time span

7 Create a parking rule.

In this step, you enable Pay-by-Plate Sync and link the permit restriction.



Rule information

Convenience time: 000 d 00 h 10 m

Grace period: 000 d 00 h 05 m

Pay-By-Plate Sync

Pay-By-Plate Sync: ON

Permit / Permit restriction: North parking lot

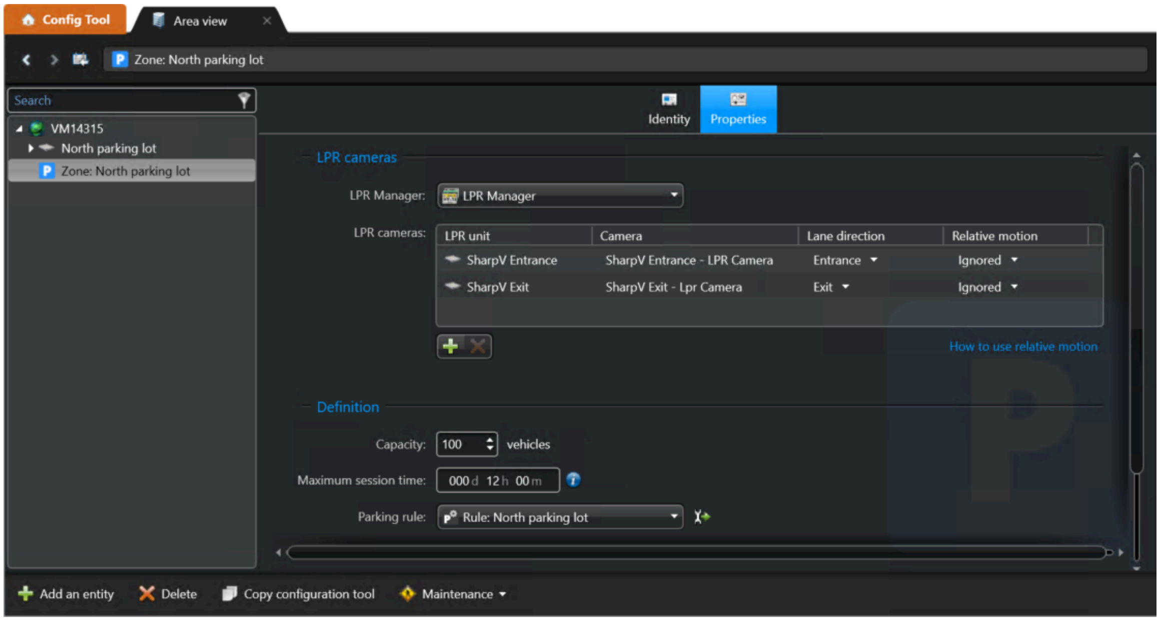
Permit restrictions require Pay-by-Plate Sync 5.0 or later.

Default expiration delay: 15 m

8 Create a parking zone.

In this step, you associate cameras and a parking rule with the parking zone and you set the vehicle capacity.

If you need to send a list of vehicles whose parking sessions have reached a state of *Violation* to a parking enforcement patrol vehicle, you can link the parking zone to a violation hotlist.



LPR cameras

LPR Manager: LPR Manager

LPR cameras:

LPR unit	Camera	Lane direction	Relative motion
SharpV Entrance	SharpV Entrance - LPR Camera	Entrance	Ignored
SharpV Exit	SharpV Exit - Lpr Camera	Exit	Ignored

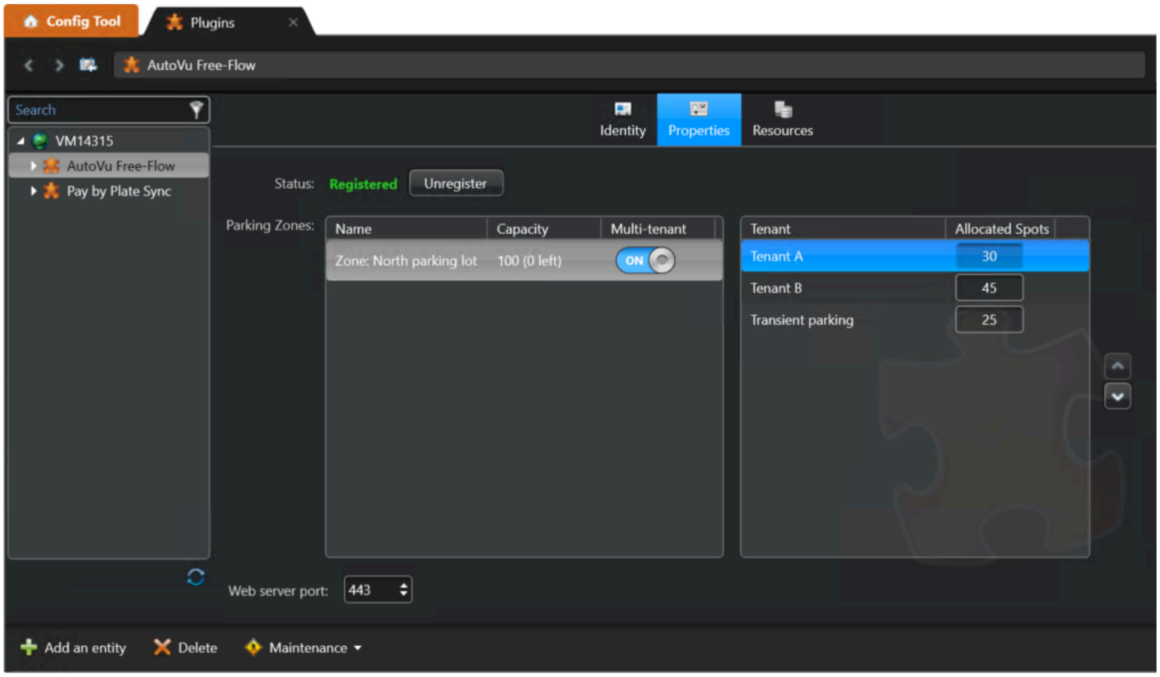
Definition

Capacity: 100 vehicles

Maximum session time: 000 d 12 h 00 m

Parking rule: Rule: North parking lot

9 In the Free-Flow plugin, enable multi-tenant parking and set the parking spots allotted to each tenant. For more information, see "Configuring the Free-Flow plugin" in the *AutoVu™ Free-Flow Plugin Guide*



Status: Registered

Parking Zones:

Name	Capacity	Multi-tenant
Zone: North parking lot	100 (0 left)	ON

Tenant	Allocated Spots
Tenant A	30
Tenant B	45
Transient parking	25

Web server port: 443

Configuring Free-Flow to track employee parking

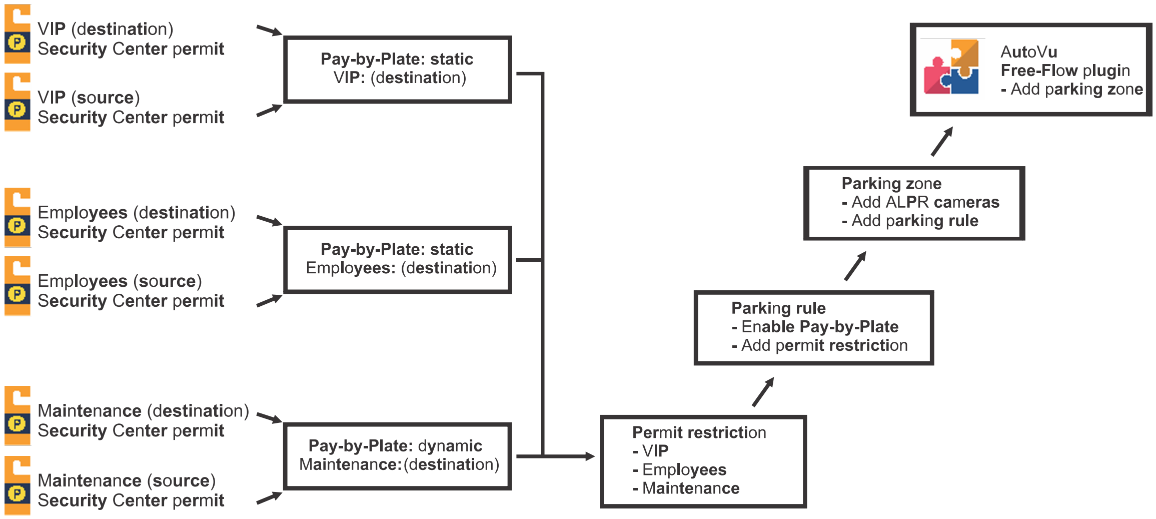
You can configure an AutoVu™ Free-Flow system to track the employee usage of a company parking lot based on employee groups.

Before you begin

- Read the document Genetec AutoVu™ Free-Flow Best Practices.
- Contact your AutoVu™ representative to verify that cloud services have been enabled for your account.
- Install a compatible version of the Pay-by-Plate Sync and Free-Flow plugin. See the "Free-Flow plugin compatibility" topic in the *AutoVu Free-Flow Plugin Guide*.

What you should know

- This configuration is similar to the multi-tenant configuration, but in this case, the term *tenant* is used to describe different employee groups.
- The following diagram shows a scenario where parking usage is tracked for VIPs, regular employees, and maintenance staff:



To configure a parking facility to track employee parking:

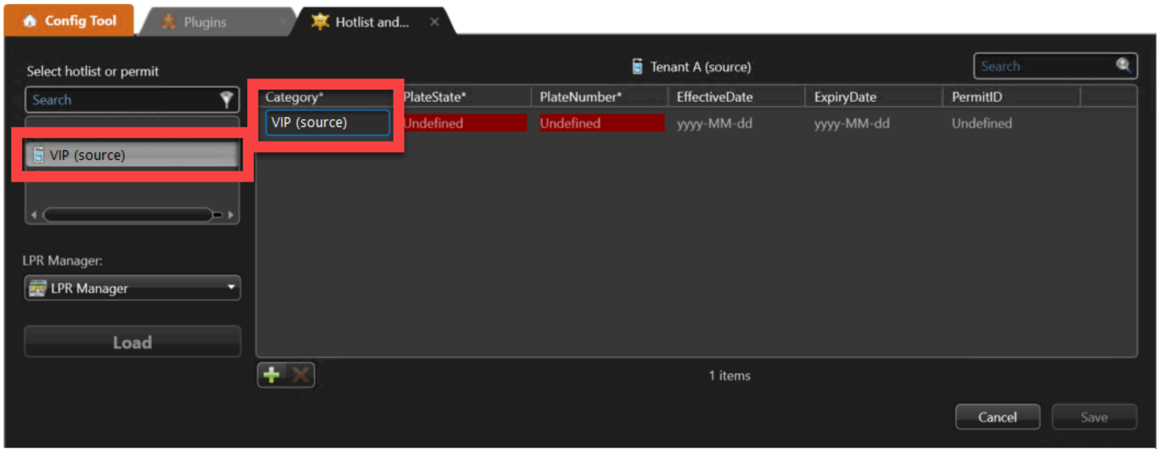
1 Configure the general settings for Free-Flow. For more details, see "Configuring AutoVu Free-Flow general settings".

2 Create the required *source* and *destination* Security Center permits for each employee group in the parking lot.

For more information, see Creating parking permits on page 1139.

For more information on source permits and destination permits, see "Linking permits using the Free-Flow plugin" in the *Security Center Administrator Guide*.

IMPORTANT: If you use the *Hotlist and permit editor* to enter vehicle information, the system completes the **Category** field for each row. For more information on the Hotlist and permit editor, see the *Security Center User Guide*. Do not modify this field as it must match the permit name.



Category*	PlateState*	PlateNumber*	EffectiveDate	ExpiryDate	PermitID
VIP (source)	Undefined	Undefined	yyyy-MM-dd	yyyy-MM-dd	Undefined

TIP: Name the Security Center permits according to their use as *source* or *destination* permits. This can help you to avoid assigning the wrong Security Center permits when you link them in Pay-by-Plate Sync. If you assign the wrong permits, you might overwrite your source plate list.

3 Configure the Security Center permits to be used with Pay-by-Plate Sync.

For more information, see "Configuring a Security Center permit for Pay-by-Plate Sync" in the *Pay-by-Plate Sync Plugin Guide*.

IMPORTANT:

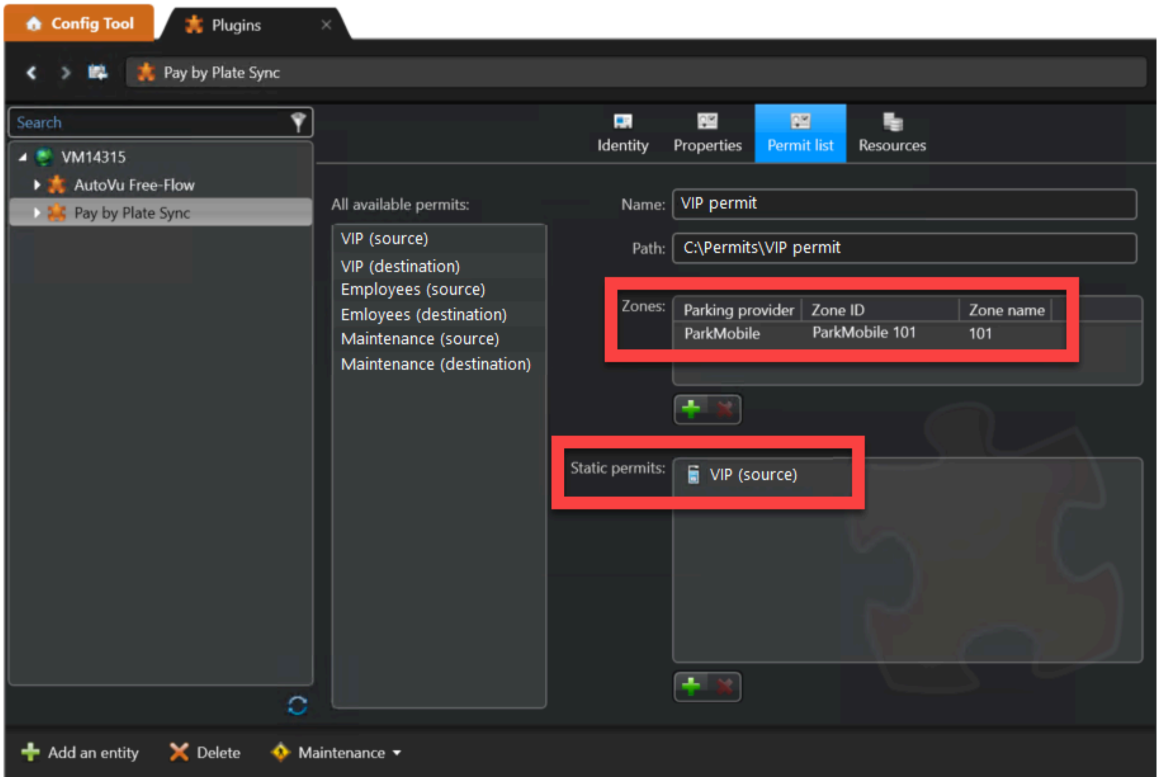
- Pay attention to the instructions on configuring the attributes of the permit. The permits must either include four attributes (*Category*, *PlateState*, *PlateNumber*, and *PermitID*) or six attributes (*Category*, *PlateState*, *PlateNumber*, *PermitID*, *EffectiveDate*, and *ExpiryDate*)
- If you include the *EffectiveDate*, and *ExpiryDate* attributes, the fields cannot be empty.
- The *PermitID* field cannot be empty.

4 In Pay-by-Plate Sync, select each employee group's *destination* Security Center permit and link all of the employee group's *source* permits.

For more information on which permits you need to link in Pay-by-Plate Sync, see "Linking permits using the Free-Flow plugin" in the *Security Center Administrator Guide*.

For more information how to link permits in Pay-by-Plate Sync, see "Configuring Pay-by-Plate Sync permit list" in the *Pay-by-Plate Sync Plugin Guide*.

In this example of a Grouped permit, a dynamic parking provider zone and a static permit are linked to the *Combined Permit* Security Center permit in Pay-by-Plate Sync:



All available permits:
- VIP (source)
- VIP (destination)
- Employees (source)
- Emloyees (destination)
- Maintenance (source)
- Maintenance (destination)

Name: VIP permit

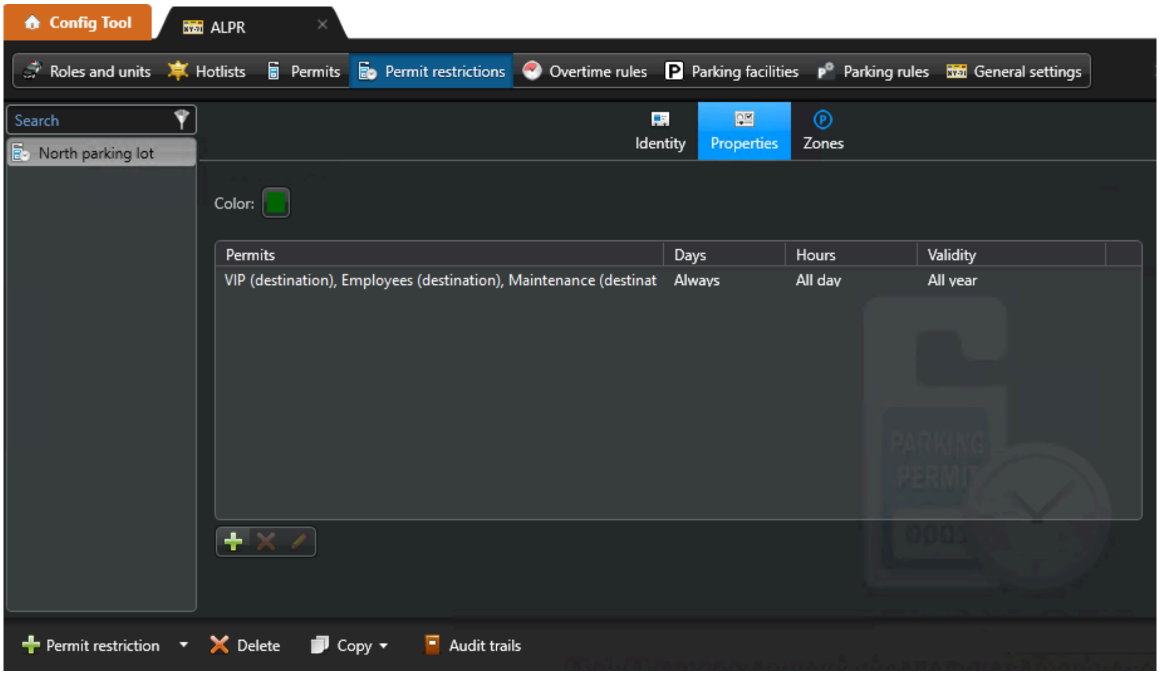
Path: C:\Permits\VIP permit

Zones:

Parking provider	Zone ID	Zone name
ParkMobile	ParkMobile 101	101

Static permits: VIP (source)

5 Create a permit restriction for the parking lot that includes the *destination* Security Center permits for all of the employee groups using the parking lot.



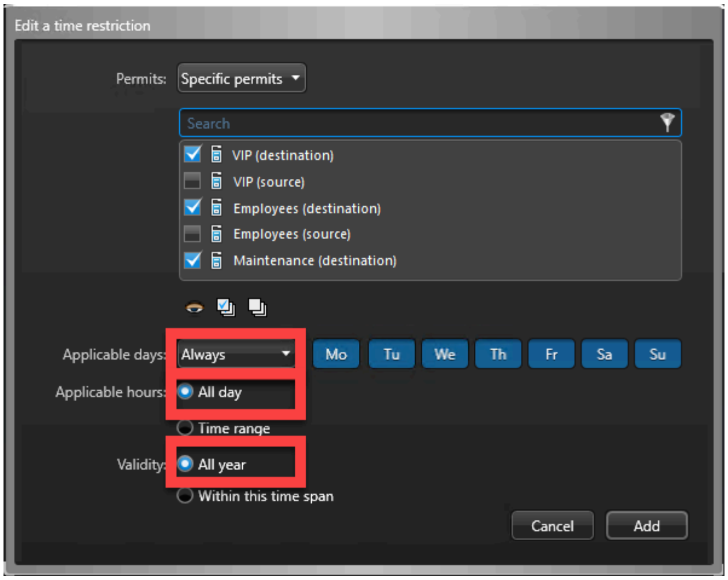
Color: 🟩

Permits	Days	Hours	Validity
VIP (destination), Employees (destination), Maintenance (destinat	Always	All day	All year

6 Configure the parking lot's permit restriction.

IMPORTANT: The Free-Flow plugin ignores any time restrictions configured for the permit restriction. To avoid confusion, configure the time restrictions as follows:

- **Applicable days**: Always
- **Applicable hours**: All day
- **Validity**: All year



Permits: Specific permits

☑ VIP (destination)
□ VIP (source)
☑ Employees (destination)
□ Employees (source)
☑ Maintenance (destination)

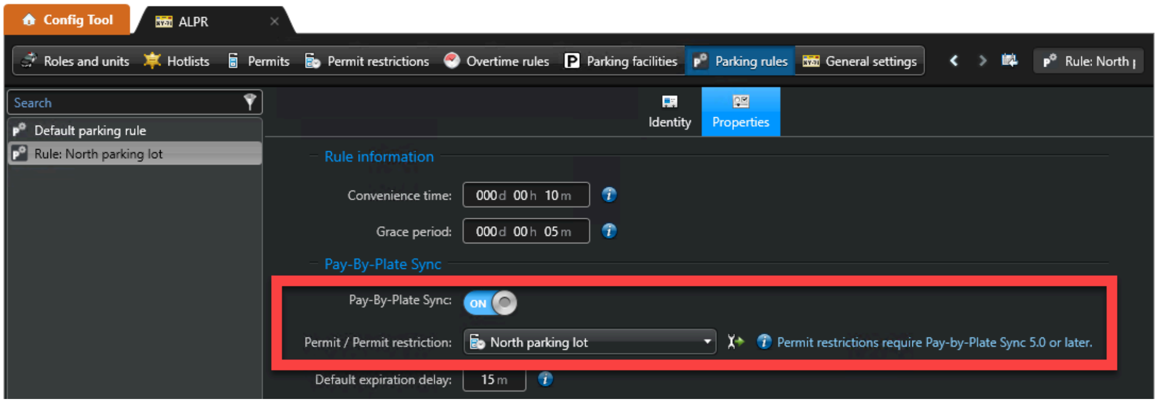
Applicable days: Always

Applicable hours: ● All day ○ Time range

Validity: ● All year ○ Within this time span

7 Create a parking rule.

In this step, you enable Pay-by-Plate Sync and link the permit restriction.



Rule information

Convenience time: 000 d 00 h 10 m

Grace period: 000 d 00 h 05 m

Pay-By-Plate Sync

Pay-By-Plate Sync: ON

Permit / Permit restriction: North parking lot

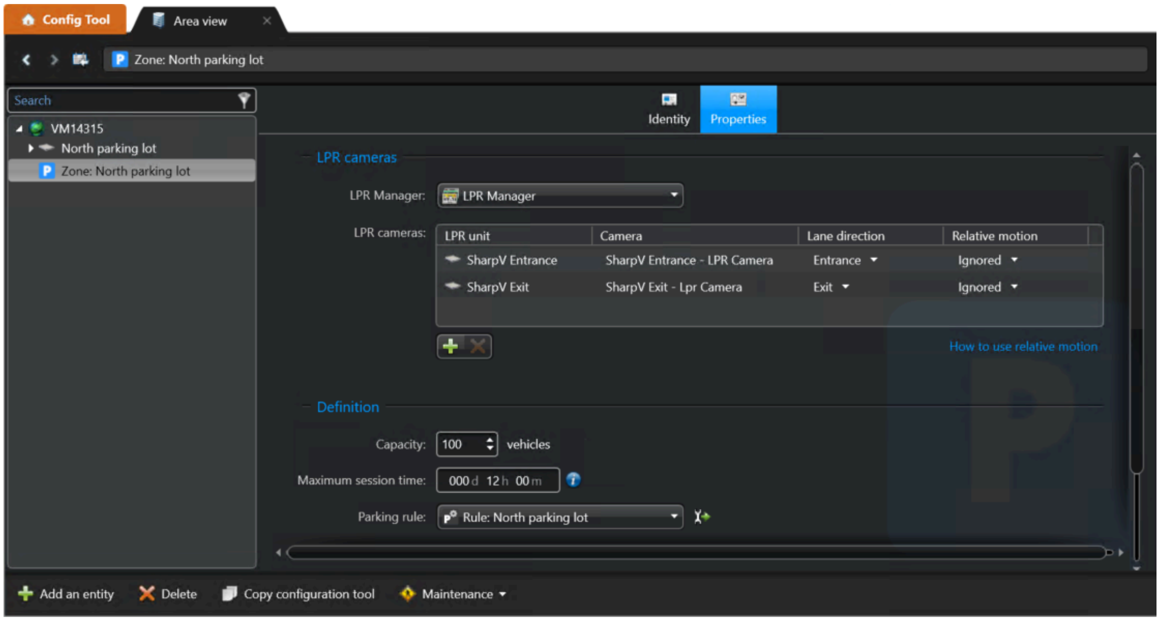
Permit restrictions require Pay-by-Plate Sync 5.0 or later.

Default expiration delay: 15 m

8 Creating a parking zone

In this step, you associate cameras and a parking rule with the parking zone and you set the vehicle capacity.

If you need to send a list of vehicles whose parking sessions have reached a state of *Violation* to a parking enforcement patrol vehicle, you can link the parking zone to a violation hotlist.If you need to send a list of vehicles whose parking sessions have reached a state of *Violation* to a parking enforcement patrol vehicle, you can link the parking zone to a violation hotlist.



LPR cameras

LPR Manager: LPR Manager

LPR cameras:

LPR unit	Camera	Lane direction	Relative motion
SharpV Entrance	SharpV Entrance - LPR Camera	Entrance	Ignored
SharpV Exit	SharpV Exit - Lpr Camera	Exit	Ignored

Definition

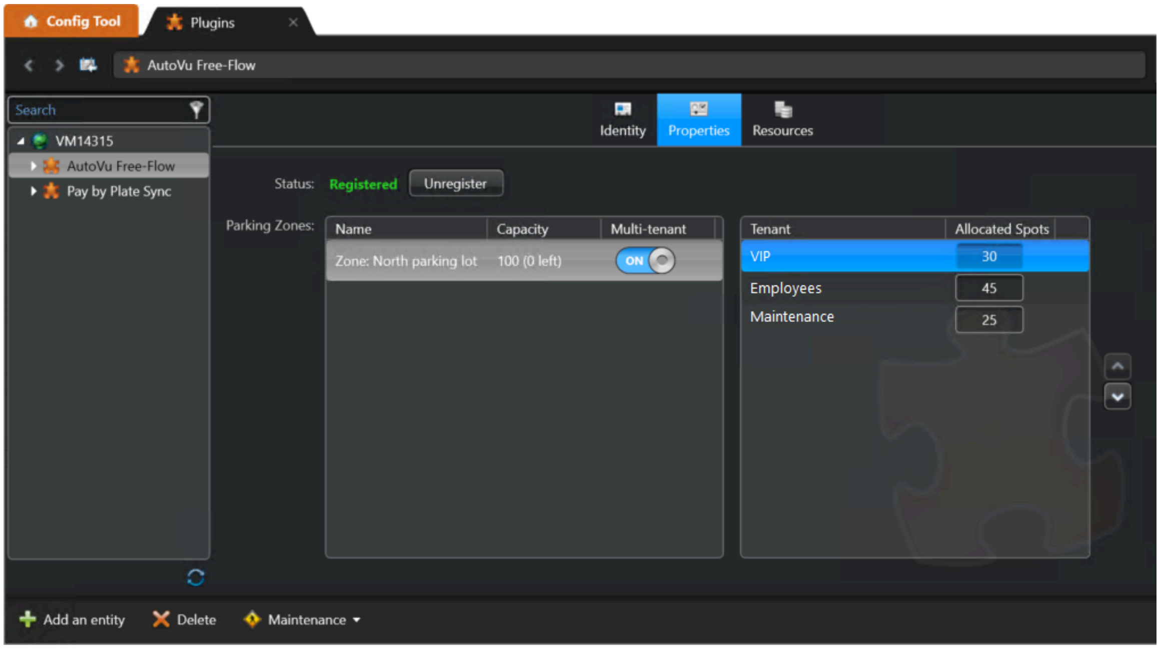
Capacity: 100 vehicles

Maximum session time: 000 d 12 h 00 m

Parking rule: Rule: North parking lot

9 In the Free-Flow plugin, enable multi-tenant parking and set the parking spots allotted to each employee type.

For more information, see "Configuring the Free-Flow plugin" in the *AutoVu™ Free-Flow Plugin Guide*



Status: Registered

Parking Zones:

Name	Capacity	Multi-tenant
Zone: North parking lot	100 (0 left)	ON

Tenant	Allocated Spots
VIP	30
Employees	45
Maintenance	25

Configuring Free-Flow general settings

To use AutoVu™ Free-Flow, you must configure general settings which define how the system handles license plate reads, and how Free-Flow works with Pay-by-Plate Sync.

What you should know

- **IMPORTANT:** Using the SharpV dual-lane monitoring feature reduces the ALPR performance of the camera. Do not configure the SharpV for dual-lane license plate detection if you are monitoring parking occupancy using AutoVu™ Free-Flow in Security Center.
- To use Free-Flow, you must also configure parking rules and parking zones.

To configure Free-Flow:

1 From the Config Tool homepage, click **System** > **Roles**.

2 Select the **ALPR Manager** you want to configure, and then click the **Properties** tab.

3 Select **Free-Flow**.

4 Configure plate matching.

- **Match tolerance threshold:** This value indicates the number of single-character differences between entry and exit plate reads that are still considered a match. Setting the value to 0 is equivalent to an exact match.

  IMPORTANT: Setting this value too high may cause plate reads to be associated with the wrong vehicle. The default value is 1.

5 (Optional) Configure Pay-by-Plate Sync settings if you are using a third-party payment provider.

- **Server:** Enter the IP address of the machine on which Pay-by-Plate Sync is installed.
- **Port:** Enter the port number for the Pay-by-Plate Sync connection (default: 8787).

6 (Optional) Configure XML export settings if you are sending plate reads to a third-party system.

- **XML export folder:** Specify the export folder for Free-Flow XML data.
- **Include vehicle images with export:** By default, vehicle images are not included with exported XML files.

  NOTE: Including vehicle images increases the size of the XML export file.
- **Export occupancy:** Export parking zone occupancy data to a separate XML file.

  NOTE: A single XML file is exported for all parking zones. This file is overwritten once per minute.

  The following is an example of an occupancy XML file:

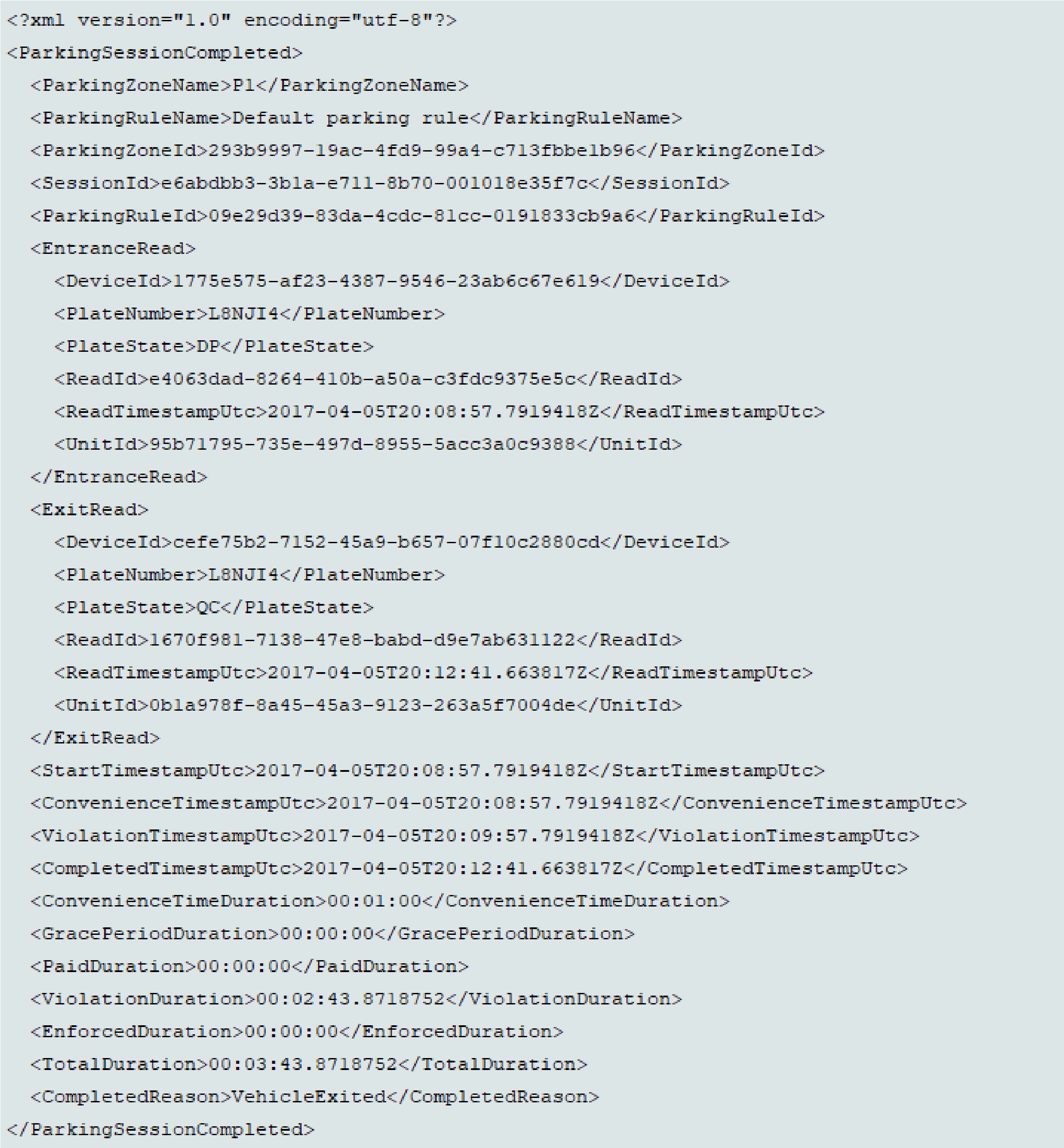
```
<?xml version="1.0" encoding="utf-8"?>
<OccupancyExport>
  <RoleId>8817e652-a9ca-4d06-81d7-8db93b5e3819</RoleId>
  <RoleName>ALPR Manager</RoleName>
  <ParkingOccupancies>
    <Occupancy>
      <Capacity>100</Capacity>
      <ParkingZoneId>293b9997-19ac-4fd9-99a4-c713fbbe1b96</ParkingZoneId>
      <ParkingZoneName>P1</ParkingZoneName>
      <TimestampUtc>2017-04-05T20:15:00Z</TimestampUtc>
      <Vehicles>5</Vehicles>
      <Violations>1</Violations>
      <EnforcedVehicles>0</EnforcedVehicles>
    </Occupancy>
    <Occupancy>
      <Capacity>200</Capacity>
      <ParkingZoneId>9dab3ef5-197f-4a33-87ae-e85dfa01c0b2</ParkingZoneId>
      <ParkingZoneName>P2</ParkingZoneName>
      <TimestampUtc>2017-04-05T20:15:00Z</TimestampUtc>
      <Vehicles>4</Vehicles>
      <Violations>0</Violations>
      <EnforcedVehicles>0</EnforcedVehicles>
    </Occupancy>
  </ParkingOccupancies>
</OccupancyExport>
```

- **Export violations:** When a vehicle is in violation, vehicle information is exported as a separate XML file.

```
<?xml version="1.0" encoding="utf-8"?>
<InLotViolation>
  <ParkingZoneName>P1</ParkingZoneName>
  <ParkingRuleName>Default parking rule</ParkingRuleName>
  <ParkingZoneId>293b9997-19ac-4fd9-99a4-c713fbbe1b96</ParkingZoneId>
  <SessionId>e6abdbb3-3b1a-e711-8b70-001018e35f7c</SessionId>
  <ParkingRuleId>09e29d39-83da-4cdc-81cc-0191833cb9a6</ParkingRuleId>
  <EntranceRead>
    <DeviceId>1775e575-af23-4387-9546-23ab6c67e619</DeviceId>
    <PlateNumber>L8NJI4</PlateNumber>
    <PlateState>DP</PlateState>
    <ReadId>e4063dad-8264-410b-a50a-c3fdc9375e5c</ReadId>
    <ReadTimestampUtc>2017-04-05T20:08:57.7919418Z</ReadTimestampUtc>
    <UnitId>95b71795-735e-497d-8955-5acc3a0c9388</UnitId>
  </EntranceRead>
  <ViolationReason>ConvenienceTimeExpired</ViolationReason>
  <TimestampUtc>2017-04-05T20:09:57.7919418Z</TimestampUtc>
</InLotViolation>
```

- **Export completed sessions:** When a vehicle exits the parking lot, the parking session information is exported as a separate XML file.

  The following is an example of a completed sessions XML file:



```
<?xml version="1.0" encoding="utf-8"?>
<ParkingSessionCompleted>
  <ParkingZoneName>P1</ParkingZoneName>
  <ParkingRuleName>Default parking rule</ParkingRuleName>
  <ParkingZoneId>293b9997-19ac-4fd9-99a4-c713fbbe1b96</ParkingZoneId>
  <SessionId>e6abdbb3-3b1a-e711-8b70-001018e35f7c</SessionId>
  <ParkingRuleId>09e29d39-83da-4cdc-81cc-0191833cb9a6</ParkingRuleId>
  <EntranceRead>
    <DeviceId>1775e575-af23-4387-9546-23ab6c67e619</DeviceId>
    <PlateNumber>L8NJI4</PlateNumber>
    <PlateState>DP</PlateState>
    <ReadId>e4063dad-8264-410b-a50a-c3fdc9375e5c</ReadId>
    <ReadTimestampUtc>2017-04-05T20:08:57.7919418Z</ReadTimestampUtc>
    <UnitId>95b71795-735e-497d-8955-5acc3a0c9388</UnitId>
  </EntranceRead>
  <ExitRead>
    <DeviceId>cefe75b2-7152-45a9-b657-07f10c2880cd</DeviceId>
    <PlateNumber>L8NJI4</PlateNumber>
    <PlateState>QC</PlateState>
    <ReadId>1670f981-7138-47e8-babd-d9e7ab631122</ReadId>
    <ReadTimestampUtc>2017-04-05T20:12:41.663817Z</ReadTimestampUtc>
    <UnitId>0b1a978f-8a45-45a3-9123-263a5f7004de</UnitId>
  </ExitRead>
  <StartTimestampUtc>2017-04-05T20:08:57.7919418Z</StartTimestampUtc>
  <ConvenienceTimestampUtc>2017-04-05T20:08:57.7919418Z</ConvenienceTimestampUtc>
  <ViolationTimestampUtc>2017-04-05T20:09:57.7919418Z</ViolationTimestampUtc>
  <CompletedTimestampUtc>2017-04-05T20:12:41.663817Z</CompletedTimestampUtc>
  <ConvenienceTimeDuration>00:01:00</ConvenienceTimeDuration>
  <GracePeriodDuration>00:00:00</GracePeriodDuration>
  <PaidDuration>00:00:00</PaidDuration>
  <ViolationDuration>00:02:43.8718752</ViolationDuration>
  <EnforcedDuration>00:00:00</EnforcedDuration>
  <TotalDuration>00:03:43.8718752</TotalDuration>
  <CompletedReason>VehicleExited</CompletedReason>
</ParkingSessionCompleted>
```

7 Configure event settings.

- **Capacity threshold:** Specify the parking zone capacity threshold at which a *capacity threshold reached* event is generated.

8 Click **Apply**.

Adding and configuring parking rules

The parking rules that define how and when a vehicle can be parked can vary greatly from one parking zone to another. The parking rules that you configure can be assigned to one or more parking zones.

Before you begin

If you want to incorporate third-party license plate enabled parking (LEP) payment systems, you must install the Pay-by-Plate Sync plugin on all servers and client workstations that must use the plugin. For more information, see the *Pay-by-Plate Sync Plugin Guide*.

What you should know

The following parking scenarios are supported:

- *Overtime parking* (for example, free parking for a maximum of 2 hours).
- *Transient parking* using Pay-by-Plate Sync enabled payment providers.
- *Contract parking* using Pay-by-Plate Sync permits.

To add a new parking rule:

1 From the Config Tool home page, open the *ALPR* task and click **Parking rules**.

2 Click **Parking rule** (✚).

3 In the *Identity* tab, rename your parking rule and add a **Description** and **Logical ID** (optional).

4 You can define **Relationships** to link parking zones and actions to your parking rule.

5 In the **Properties** tab, configure the following:

- **Convenience time:** The convenience time is a configurable leeway time before a vehicle starts to be charged after entering the parking zone. For example, if you need to set up a 2-hour free parking period before paid time or parking enforcement takes effect, you would set the convenience time for 2 hours. For parking lots where parking enforcement begins immediately, you would still need to set a short convenience time to allow vehicle owners time to find a parking spot and purchase parking time before parking enforcement begins.

  NOTE:

  - If you are setting up a parking lot that uses permits, you can set the convenience time for 10 minutes. This allows clients enough time to park and purchase a permit before they are in violation. You can also give the client leniency when exiting by configuring a grace period.
  - If you are setting up a parking lot that is free, but with a 1-hour time limit, you must configure a 1-hour convenience time. Note that this scenario does not use third-party parking permits and does not require the Pay-by-Plate Sync plugin.

- **Grace period:** A grace period can be added to a parking session for purposes of lenient enforcement. Following the expiration of the vehicle's parking time, extra time is given before a vehicle's parking session is flagged as a violation.

6 If your system uses the Pay-by-Plate Sync plugin to incorporate third-party payment systems, turn on the feature and configure the following:

- **Permit / permit restriction:** Select the Pay-by-Plate Sync permit or permit restriction you want to apply.

  NOTE: Permit restrictions require Pay-by-Plate Sync 5.0 or later.
- **Default expiration delay:** It is recommended that you configure an *EffectiveDate* and *ExpiryDate* for Pay-by-Plate Sync permits (if supported by the payment providers). This reduces the volume of queries to the third-party providers. The *Default expiration delay* is used for permits that do not include an expiration. In this case, AutoVu™ Free-Flow checks with the parking permit provider to see if the permit is still valid. Increasing this value reduces the frequency of the permit checks. For example, if the

parking lot charges for parking in increments of 15 minutes, you could set the *Default expiration delay* to 15 minutes.

For more information on the *EffectiveDate* and *ExpiryDate* attributes, refer to the instructions on creating Security Center permits in the *Pay-by-Plate Sync Plugin Guide*.

- **Convenience time and grace period:** When using Pay-by-Plate Sync for transient parking, you can also configure convenience time and a grace period for purposes of lenient enforcement.

Related Topics

Creating parking permits on page 1139

Creating permit restrictions on page 1143

Adding and configuring parking zones

To manage physical parking lots in Security Center using AutoVu™ Free-Flow, you must first define parking zones and assign Sharp cameras as entrance or exit cameras.

Before you begin

- Add the Sharp cameras that are monitoring the parking zone to the ALPR Manager.
- To make the video feed available, add the Sharp cameras that are monitoring the parking zone to the Archiver.
- Create a parking rule.

To add a new parking zone:

1. From the Config Tool home page, click the *Area view* task.
2. In the entity tree, click the area you want to add the parking zone to.
3. Click **Add an entity** (➕) and select **Parking zone**.

   A new parking zone is added under the area.

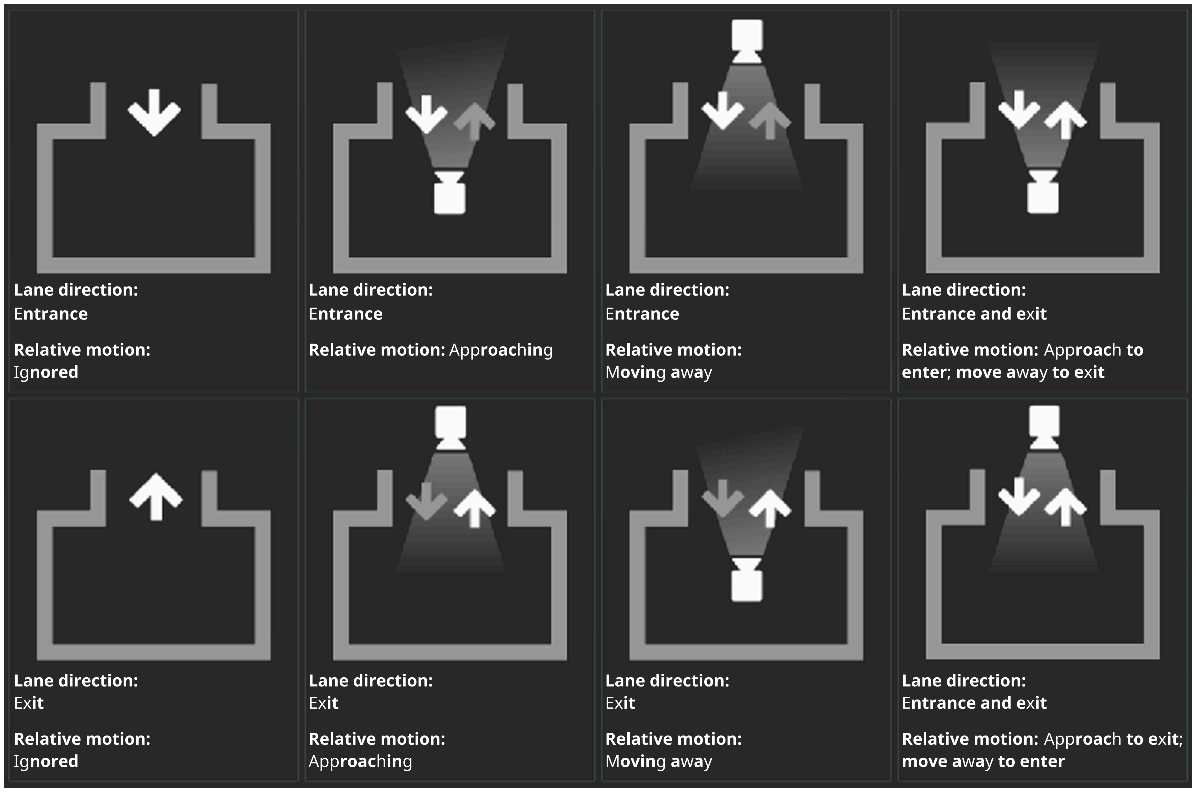
To configure the parking zone:

1. In the *Identity* tab, rename your parking rule and add a **Description** and **Logical ID** (optional).
2. Click the **Properties** tab of parking zone.
3. From the **ALPR Manager** list, select the ALPR Manager to which the parking zone is assigned.

   WARNING: If you delete an ALPR Manager, all parking zones that are assigned to it are also deleted and all related parking data is lost.

   NOTE: Only the Sharp cameras associated with the selected ALPR Manager are available to monitor the parking zone.
4. In the **ALPR cameras** section, click **Add an item** (➕). Select the Sharp cameras that are installed in the parking zone, and click **OK**.

5 For each Sharp camera that is monitoring the parking zone, you must specify whether the monitored lane is an exit, an entrance, or whether the lane serves as both an entrance and an exit.



Lane direction: Entrance

Relative motion: Ignored

Lane direction: Entrance

Relative motion: Approaching

Lane direction: Entrance

Relative motion: Moving away

Lane direction: Entrance and exit

Relative motion: Approach to enter; move away to exit

Lane direction: Exit

Relative motion: Ignored

Lane direction: Exit

Relative motion: Approaching

Lane direction: Exit

Relative motion: Moving away

Lane direction: Entrance and exit

Relative motion: Approach to exit; move away to enter

Define the lane direction using the following parameter:

Lane direction:

- **Entrance:** The Sharp camera is monitoring a parking lot entrance lane.
- **Exit:** The Sharp camera is monitoring a parking lot exit lane.
- **Entrance and exit:** A Sharp camera can detect whether a vehicle is moving toward it or away from it. As a result, if vehicles have both a front and rear license plate, you can use a single Sharp camera to monitor a lane that is used as both an entrance and an exit to a parking zone.

6. For each Sharp camera that is monitoring the parking zone, you must specify the direction that traffic is moving in relation to the camera.

   Define the relative motion using the following parameter:

   Relative motion: A Sharp camera can detect whether a vehicle is moving toward it or away from it. Using this information, the parking zone can ignore vehicles traveling in a certain direction.

   IMPORTANT: Only filter by relative motion if necessary. If you position the camera so that only one lane is visible, and the lane has only one direction of travel, you do not need to use the relative motion feature. For more information on defining a region of interest, see the *Sharp Administrator Guide*.

   The following options are available if you select a lane direction of **Entrance** or **Exit**.

   - **Ignored:** Use this option if only one lane is visible in the context image with only one direction of travel.
   - **Approaching:** If the camera might detect vehicles moving in both directions, use this setting to only register vehicles if they are moving toward the camera or if the direction of travel cannot be detected.
   - **Moving away:** If the camera might detect vehicles moving in both directions, use this setting to only register vehicles if they are moving away from the camera or if the direction of travel cannot be detected.

   The following options are available if you select a lane direction of **Entrance and exit**.

   - **Approach to enter:** Use this option if one camera is used to detect both entering and exiting vehicles and if vehicles approach the camera as they enter the parking lot.
   - **Approach to exit:** Use this option if one camera is used to detect both entering and exiting vehicles and if vehicles approach the camera as they exit the parking lot.

7. In the **Definition** section, configure the following parameters for the parking lot:

   - **Capacity:** The number of physical parking spaces in the parking lot.

     NOTE: The parking zone capacity works in conjunction with the *Capacity threshold* setting of the ALPR Manager. When the capacity threshold is reached, a *capacity threshold reached* event is generated.
   - **Maximum session time:** This is the period of time before a vehicle's *parking session* is considered to have exceeded the limit of stay in the *parking zone*. After this point, it is assumed that the vehicle's plate was not read at the exit and that the vehicle is no longer in the parking zone. The vehicle no longer appears in parking session reports created in the Security Desk *Parking sessions* task.
   - **Parking rule:** Select a parking rule to apply to the parking zone.

     To jump to a parking rule's configuration page, select the rule, and click ➔.

8. In the **Enforcement** section, define the following parameters for the parking lot:

   - **Violation hotlist:** Select a hotlist to be populated with the information of vehicles whose parking sessions have reached a state of *Violation*. The selected hotlist is updated every minute and can be used to enforce violations using a Genetec Patroller™ vehicle.

9. Click **Apply**.

After you finish

(Optional) At a certain point (for example, when the parking lot closes) you can assume that all parking sessions have ended and that any vehicles remaining in the parking zone have been issued tickets or must be towed. You can reset the parking zone inventory using the action *Reset parking zone inventory*.

Related Topics

Configuring parking lots in Security Center on page 1146

Linking cameras to parking zones

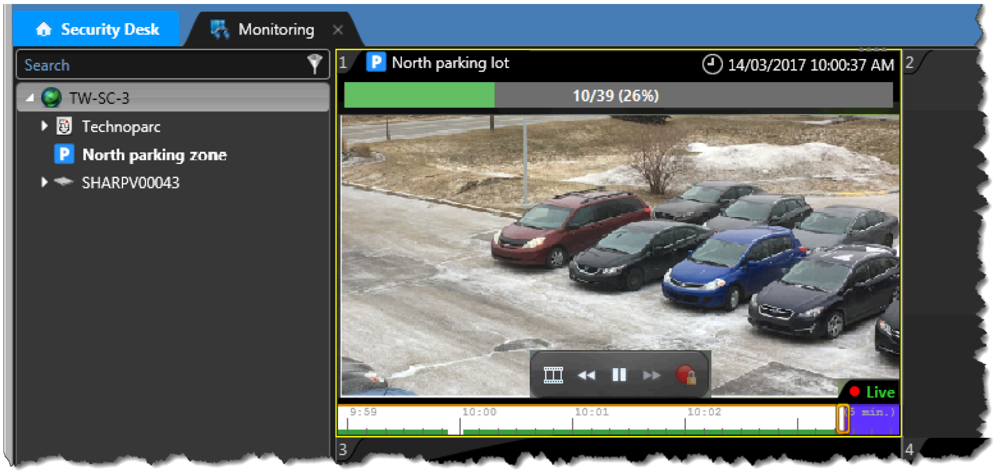
In addition to the Sharp cameras that read the license plates of vehicles entering a parking zone, you can also associate one or more additional video cameras to the parking zone. This allows the operator to perform surveillance in addition to monitoring parking zone occupancy.

Before you begin

- Create a parking zone.

What you should know

When cameras are linked to a parking zone, the parking zone occupancy information is displayed as a bar graph above the video feed in the *Monitoring* task.



To monitor parking zones with cameras, you must have one of the following Security Center configurations:

- An Archiver role with available cameras.
- An Omnicast™ Federation™ role to connect to an external Omnicast system.
- A Security Center Federation™ role to connect to an external Security Center system with cameras.

To link a camera to a parking zone:

1. From the Config Tool home page, click the *Area view* task.
2. In the entity tree, click the parking zone to which you want to link cameras.
3. In the *Relationships* section of the **Identity** tab, select **Cameras**.
4. Click **Add an item** (✚).
5. In the **Search** window, click the camera entity you want to add and click **Select**.
6. Click **Apply**.
7. In the *Relationships* section of the *Identity* tab, expand **Cameras** and verify that the camera has been added.

Configuring automatic enforcement of parking zone violations

In AutoVu™ Free-Flow systems where patrol vehicles send live hits, you can configure Security Center to automatically enforce violations in Security Desk.

What you should know

If you do not configure the system to automatically enforce violations, an operator must manually enforce the violations in Security Desk.

To configure automatic enforcement of parking zone violations:

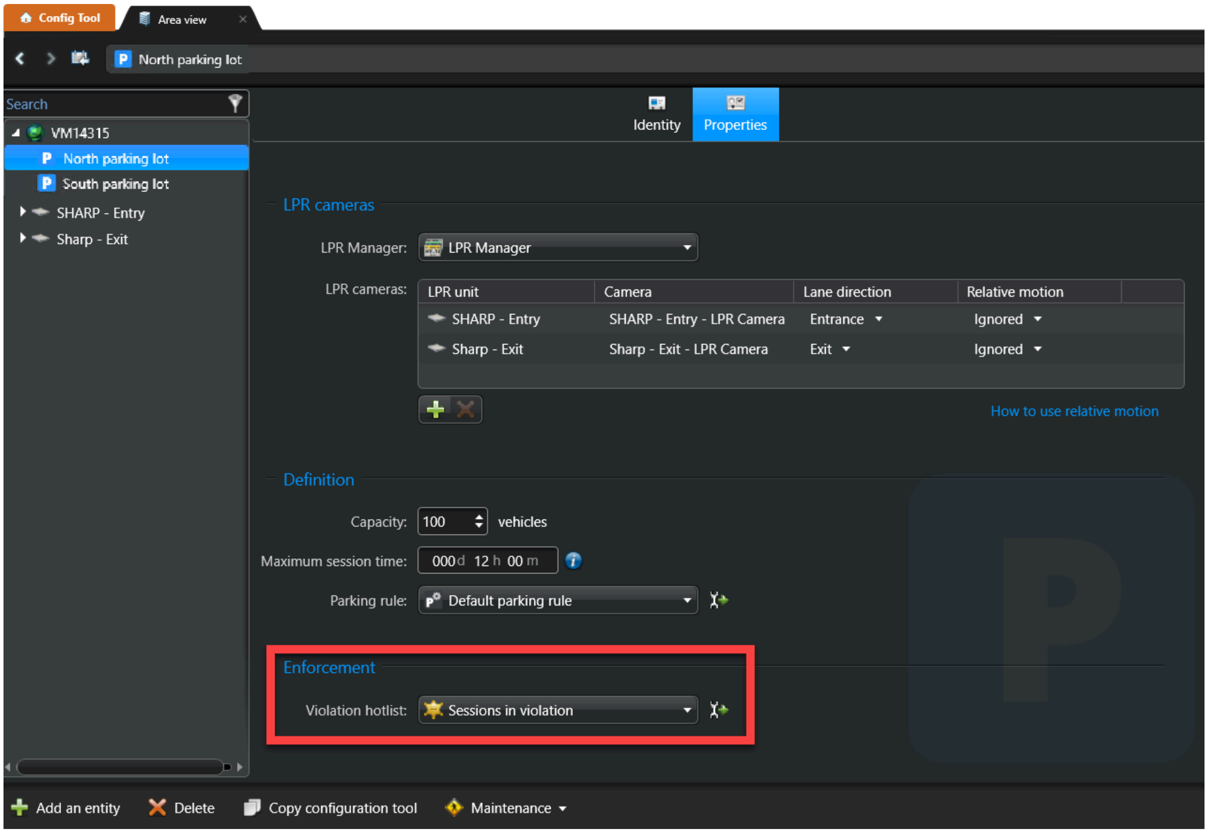
1 Assign a hotlist to the parking zone.

a) From the Config Tool home page, click the *Area view* task.

b) In the entity tree, click the parking zone you want to configure for automatic enforcement.

c) Click the **Properties** tab of parking zone.

d) In the *Enforcement* section, select the hotlist to be populated with the parking sessions that are in violation.



LPR cameras

LPR Manager: LPR Manager

LPR cameras:

LPR unit	Camera	Lane direction	Relative motion
SHARP - Entry	SHARP - Entry - LPR Camera	Entrance	Ignored
Sharp - Exit	Sharp - Exit - LPR Camera	Exit	Ignored

Definition

Capacity: 100 vehicles

Maximum session time: 000 d 12 h 00 m

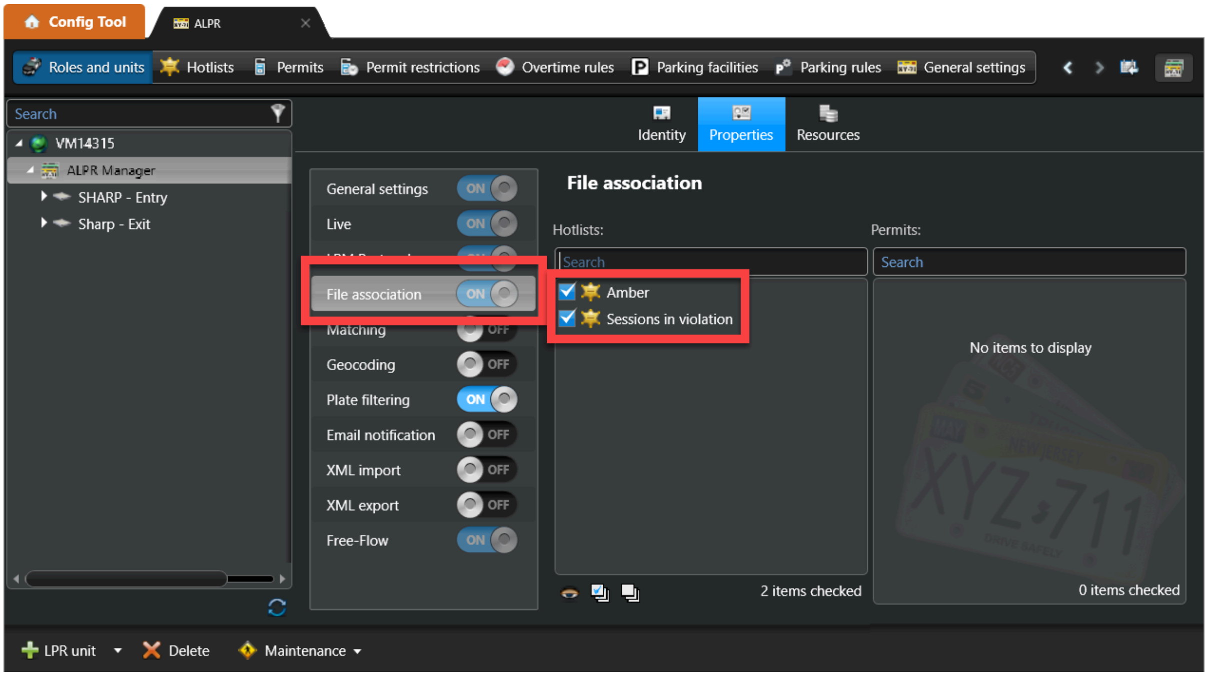
Parking rule: Default parking rule

Enforcement

Violation hotlist: Sessions in violation

e) Click **Apply**.

2 Assign the hotlist to the ALPR Manager role.
   a) From the Config Tool home page, open the *ALPR* task.
   b) In the entity tree, click the ALPR Manager role that you want to assign the hotlist to.
      IMPORTANT: Genetec Patroller™ must be able to connect to the ALPR Manager role to which the hotlist is assigned.
   c) Click the **Properties** tab.
   d) Turn on **File association**.
   e) In the *Hotlists* section, select the hotlists you want to assign to the ALPR Manager role.



General settings ON
Live ON
File association ON
Matching OFF
Geocoding OFF
Plate filtering ON
Email notification OFF
XML import OFF
XML export OFF
Free-Flow ON

File association

Hotlists:
☑ Amber
☑ Sessions in violation
2 items checked

Permits:
No items to display
0 items checked

   f) Click **Apply**.

When a patrol vehicle operator marks a parking session as *enforced*, the parking session status is also updated in Security Desk.

Related Topics

Creating hotlists on page 985
Adding and configuring parking zones on page 1086

How parking zone occupancy is calculated

As Sharp cameras detect vehicles entering and exiting a parking zone, the AutoVu™ Free-Flow system calculates the occupancy of the parking zone. You can then display this information in Security Desk *Monitoring* task tiles.

Event	Vehicle count
Vehicle enters This can include vehicles with: • Accurate license plate reads • License plates that are not read correctly • NOPLATE reads • License plates that were not captured when exiting the parking zone, and are now reentering the parking zone	Parking zone occupancy increases by one.
Vehicle exits This can include vehicles with: • Accurate license plate reads • License plates that are not read correctly • NOPLATE reads • Unknown vehicle exited (indicating that the exit read does not match the entry read)	Parking zone occupancy decreases by one.
Inventory reset You can reset the inventory of a parking zone using the *Reset parking zone inventory* action. This action can be triggered by either a *hot action* or a *scheduled task*. For more information on hot actions, see the *Security Center User Guide*.	Parking zone occupancy reset to zero.

NOTE: If a parking session is closed because the maximum session time has been exceeded, there is no change to the parking zone occupancy count.

How editing plate reads affects parking sessions and parking zone occupancy

- **Editing an entry plate read:**
  - If you edit the entry plate read for a vehicle that has an active parking session, the parking session is updated with the correct plate number. In this case, the parking zone's occupancy is not affected. If the system uses Pay-by-Plate Sync parking permits, the parking session's *paid time*, *violation*, or *grace period* state is reevaluated with Pay-by-Plate Sync.
  - If a vehicle's plate is misread when it enters the parking zone, a parking session is created and the parking zone's occupancy is increased. In this case, you must edit the entry plate read before the vehicle leaves the parking zone or before the parking session exceeds the *maximum session time* because at this point, the session is closed and editing the plate read does not update the parking session. However, this situation does not affect occupancy. When the vehicle's license plate is read

correctly at the parking zone exit, the vehicle will be flagged as an *unknown vehicle* and the parking zone's occupancy is reduced.
    - If the entry read is a NOPLATE read, the vehicle is included in the occupancy of the parking zone, but a parking session is not created. Editing the read creates a parking session for the vehicle and the permit is evaluated based on the entry time of the vehicle.

- **Editing an exit plate read:**
    - If you edit an exit plate read that matches the plate number of an active parking session, the system closes the session and the parking zone's occupancy is updated accordingly.
    - When a NOPLATE read is generated at the exit of a parking zone, the occupancy count for that zone is reduced. If that event is edited to a plate number that matches that of an active session in the parking zone, then the parking session is closed because we know that NOPLATE read is the same vehicle.

Recommendations for improving parking zone occupancy metrics

To ensure that AutoVu™ Free-Flow parking zone occupancy metrics are accurate, you can create alerts to notify parking zone operators when a license plate read must be edited. You can also automate the parking zone inventory reset.

When using Free-Flow, we recommend that you configure the following actions:

Configure event-to-actions for low confidence scores and NOPLATE reads

To ensure that the parking zone's occupancy is accurate, it is important that operators edit all NOPLATE plate reads (if enabled on the Sharp) and plate reads that have a low confidence score. It is recommended that you configure *event-to-actions* to notify operators when a plate read must be edited.

- **Confidence score:** Create an event-to-action using *When: License plate read* with *And: [Confidence Score] < 50*.

  NOTE: An acceptable confidence score depends on the environment and the ALPR context used.
- **NOPLATE:** Create an event-to-action using *When: License plate read* with *And: [PlateNumber] = "NOPLATE"*.

Configure a scheduled task to reset the parking zone inventory

At a certain point during the day (for example, when the parking lot closes), you can assume that all parking sessions have ended and that any vehicles remaining in the parking zone have been issued tickets or must be towed. You can reset the parking zone inventory by creating a *scheduled task* with the *Action: Reset parking zone inventory*.

About shared permits in Free-Flow

If your AutoVu™ Free-Flow system is configured to allow shared parking permits, then the same parking permit can be associated with multiple vehicles. Shared permits are generally used if the permit holder owns more than one vehicle, or for drivers who carpool.

Shared permits apply to one vehicle at a time. For example, if all four carpool members who share a permit decide to drive their own vehicles on a certain day, only the first vehicle entering the parking zone would be allowed to park using the permit. The other three vehicles would generate *shared permit* hits if they enter the parking zone while the first vehicle is parked.

Using Pay-by-Plate Sync

Consider the following when configuring shared permits:

- To use shared permits, the permits must come from a third-party parking permit provider using the Pay-by-Plate Sync plugin. You can define static permits for vehicles in Security Center, however these permits cannot be shared between vehicles.
- To use this feature, the Pay-by-Plate Sync permit provider must support shared permits.
- Vehicles are considered to share a permit if they have the same permit ID. For this reason, ensure that all permits have a unique permit ID. If two permits share the same permit ID when this feature is enabled, they can generate shared permit hits.

How shared permits work

1. When a vehicle enters a parking zone, the system starts a new *parking session* for the vehicle and validates the parking permit associated with the license plate.

   NOTE: If the Sharp camera misreads certain characters of the vehicle's license plate, the system can still associate the vehicle's license plate to the parking permit. The system does this using an ALPR matcher technique that only requires five common characters and four contiguous characters.
2. The system compares the *permit ID* with vehicles that are already in the parking zone.
   - If no other license plates share the same permit ID, the parking session's *paid time* stage begins.
   - If another license plate does share the same permit ID, then the parking session goes into violation.
   - If the license plate does not have a permit, then the parking session's *convenience time* starts.
   - If the system cannot communicate with the Pay-by-Plate Sync permit provider to validate the permit, the parking session's convenience time starts. The system attempts to validate the permit again at the end of the vehicle's parking session.

Enabling shared parking permits

In an AutoVu™ Free-Flow parking system, to use the same parking permit for more than one vehicle, you must enable shared permits in Security Center.

What you should know

- When you enable shared permits, the configuration applies to all parking zones that are configured in Security Center.
- To use shared permits, the permits must come from a third-party parking permit provider using the Pay-by-Plate Sync plugin. You can define static permits for vehicles in Security Center, however these permits cannot be shared between vehicles.
- To use this feature, the Pay-by-Plate Sync permit provider must support shared permits.

To enable shared permits:

1 Start the **Security Center Server Admin** ( ) application.

2 Enter the server password that you set during the server installation, and click **Log on**.

The Server Admin *Overview* page is displayed.

3 Select your server from the *Servers* list.

4 From the **Actions** list, select **</> Console**.

5 Select the *Commands* tab.

6 From the commands list, expand **Parking management commands**.

7 Click one of the following to run its associated command:

- **Disable shared permit feature:** Disabling this feature turns off the handling of shared permit hits. Vehicles with the same permit ID are not be placed in violation.
- **Enable shared permit feature:** Enabling this feature activates the handling of shared permit hits in the parking zones posessing the same Pay-by-Plate Sync permit entity. Vehicles with the same permit ID are placed in violation.

  TIP: Running the **Print module settings** command displays the current status of several configurations, including the shared permit feature.

Assigning a map to a parking zone

When you assign a map to a parking zone, you give this entity a map representation which can be used for monitoring purposes. You can assign a map to a parking zone from the Config Tool *Area view* task or *Map designer* task.

Before you begin

Add and configure a parking zone.

What you should know

- You can add a parking zone entity (represented as a polygon) to an existing map. You can then overlay the entity's location on a geographical map.
- You can add a drill-down view to a map so that the operator can, for example, click on a multi-level parking lot to have a view of each parking level.
- As an alternative to assigning a map to a parking zone, you can also add a parking zone to a map.

To assign a map to a parking zone from the *Area view* task:

1 From the Config Tool home page, open the *Area view* task.

2 In the entity tree, select the parking zone that you want to assign a map to.

3 Click the **Identity** tab, and click **Create map**.

4 Select one of the following methods to create your map background.

- **Image:** Import the map background from an image file.
- **Geographic:** Connect to a map provider.

5 Configure the default map view and other presets.

6 Configure the default information to display when someone opens this map.

7 Click **Create**.

8 To add a Sharp camera that is monitoring the parking zone, click **Area view** (), and drag the ALPR camera onto the map.

To assign a map to a parking zone from the *Map designer* task:

1 From the Config Tool homepage, open the *Map designer* task.
The Map designer wizard displays a list of recent maps.

2 Click **Create** ().

3 From the area tree, select the parking zone you are creating a map for.

4 Click **Next**.

5 Select one of the following methods to create your map background.

- **Image:** Import the map background from an image file.
- **Geographic:** Connect to a map provider.

6 Configure the default map view and other presets.

7 Configure the default information to display when someone opens this map.

8 Click **Create**.

9 To add a Sharp camera that is monitoring the parking zone, click **Area view** (), and drag the ALPR camera onto the map.

Adding a parking zone to a map

After you have created a parking zone in the AutoVu™ Free-Flow system, you can add the parking zone entity to an existing map, or create a new map to display the zone. Doing this allows operators to view the occupancy of the parking zone in the Security Desk *Maps* task.

Before you begin

- Create a map in Map designer.
- Add and configure a parking zone.

What you should know

- A parking zone can be represented on the map as a position marker, a polygon, or both. Each representation serves a different purpose:
  - Clicking the marker displays the parking zone occupancy and number of violations in a pop-up.
  - Clicking the polygon jumps to the map assigned to the parking zone.
- You can add a drill-down view to a map so that the operator can, for example, click a multi-level parking lot to have a view of each parking level.

To add a parking zone to a map as a position marker:

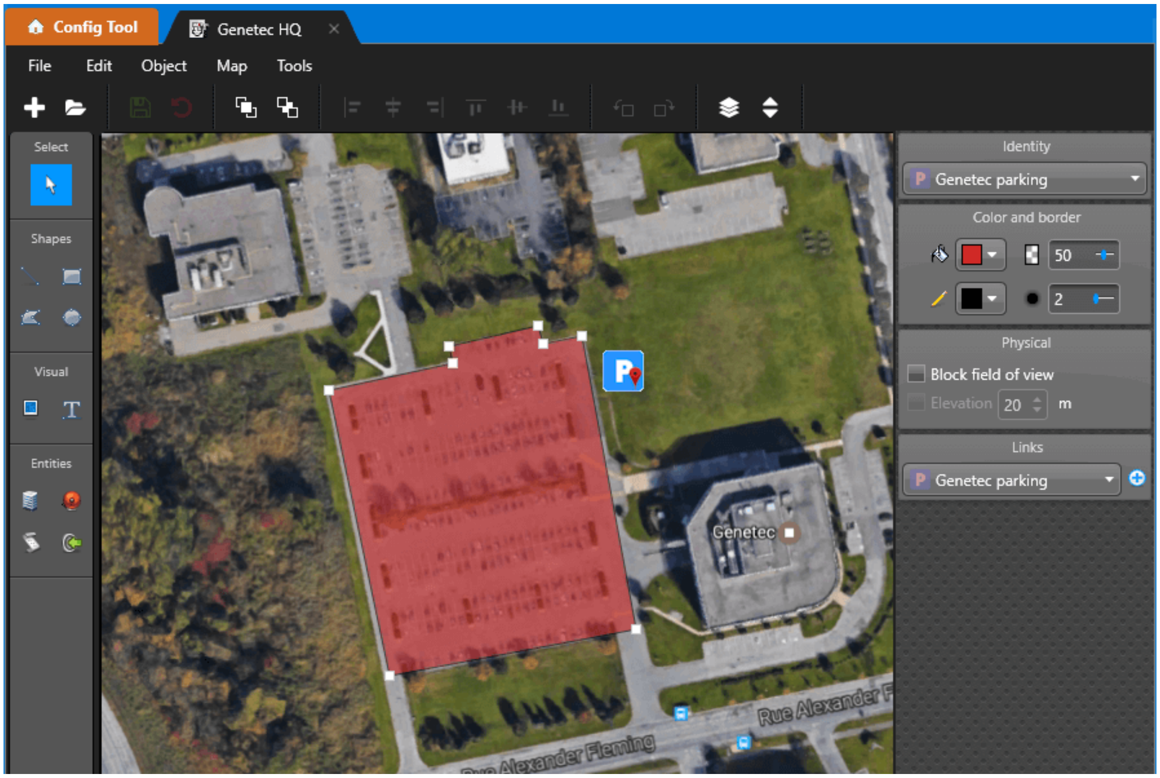
1. Open the *Map designer* task and select the map that includes an image, for example, of the parking lot or of the geographical region.
2. From the **Entities** toolbar, click **Area view** (🏢).
3. Click the parking zone in the list and drag it onto the map.

   The parking zone marker (P) appears on the map.
4. In the *Map designer* toolbar, click **Save** (💾).

To add a parking zone to a map as a polygon:

1. Open the *Map Designer* task and select the map that includes an image of the parking lot.
2. From the **Shapes** toolbar, select **Draw polygon**.

3 On the map, click the corners of the parking lot to draw the polygon. Double-click to close the polygon.



TIP: After you finish drawing the polygon, press Shift and click to add or remove points on the border of the polygon.

4 Click **Unassigned** in the *Identity* widget and select the parking zone that you want to assign to the polygon.

5 In the *Map designer* toolbar, click **Save** (💾).

If a map is assigned to your parking zone, then clicking the polygon on a map in Security Desklinks you to that map.

Adding drill-down views to maps

When Security Desk operators need to monitor a large geographic area with many entities, creating a drill-down view can make it easier for the operator to manage the area. This can be especially useful when managing parking zones.

What you should know

In the following example, we will create a drill-down view from the city level, to a multi-level parking lot, to a parking level within the parking lot.

To configure a map drill-down:

1 In Config Tool, open the *Area view* task and create the areas needed for the drill-down.

This example uses the following areas:

Airport parking (added as an *Area* entity)

Multi-level parking lot (added as an *Area* entity)

Parking level 3 (added as an *Parking zone* entity)

Parking level 2 (added as an *Parking zone* entity)

Parking level 1 (added as an *Parking zone* entity)

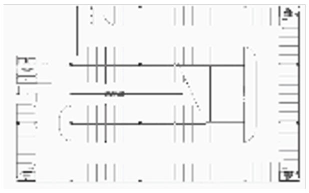
2 To add maps to the areas, in the **Identity** tab for each of the areas, click **Create map** and add a map of the area.

This example uses the following area maps:

Airport parking

Multi-level parking

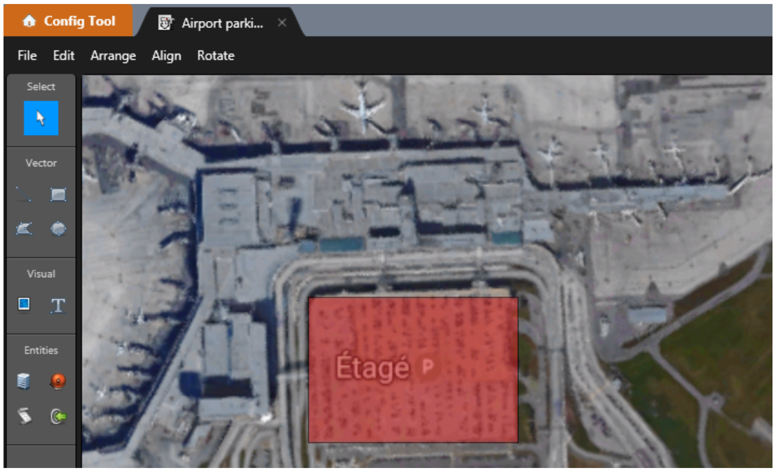
Parking levels



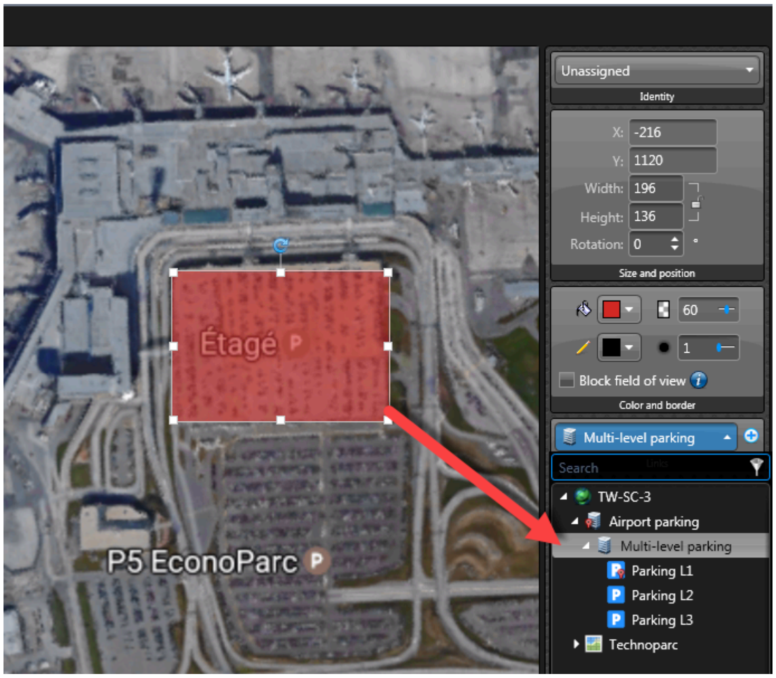
3 Create *map links* to drill down through the areas. For this example, we are drilling down from the airport parking map, to the multi-level parking map, to the parking level map.

a) In the *Map designer* task, open the *Airport parking* map.

b) Using the **Vector** tools, draw a polygon over the multi-level parking lot.



c) From the **Links** widget, assign the multi-level parking lot area to the polygon.


Unassigned

Identity

X: -216

Y: 1120

Width: 196

Height: 136

Rotation: 0

Size and position

60

1

□ Block field of view

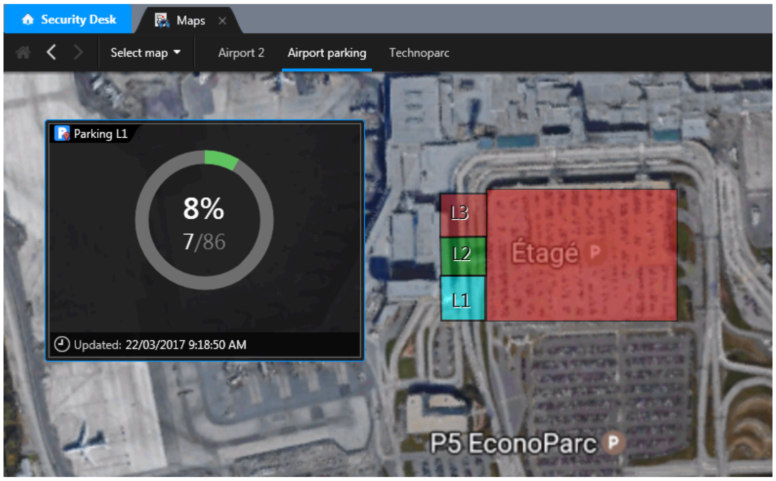
Color and border

Multi-level parking

NOTE: You can select a color for the polygon from the **Color and border** widget.

d) To display the occupancy of each parking zone on the map, in the toolbar, click **Area view** (), and drag each of the parking zones onto the map. The parking zones appear as polygons on the map. You can select a color for each polygon and use the **Add text** (T) tool to identify the parking zone.

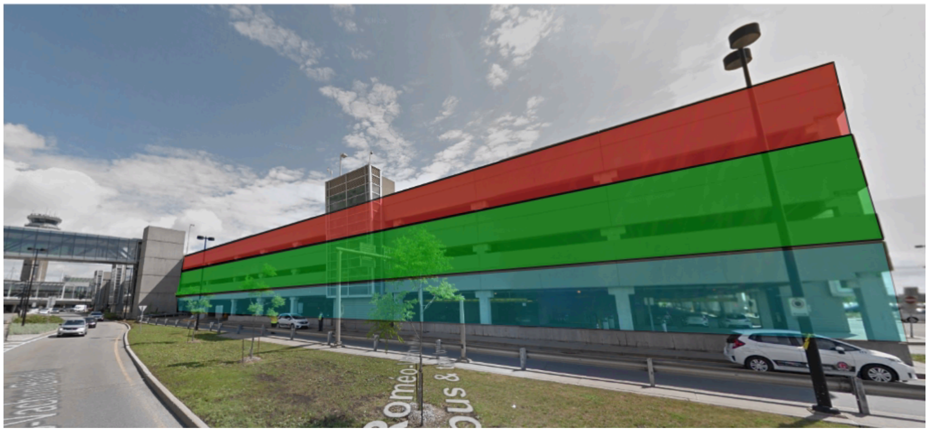
e) In the *Map designer* toolbar, click **Save** ().



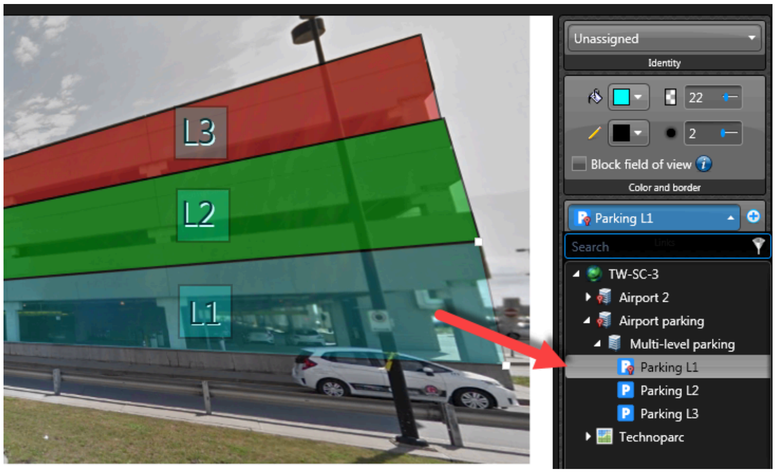
When this map is displayed in Security Desk, clicking one of the parking zone polygons displays the parking zone occupancy. Clicking the multi-level parking lot polygon drills down to the multi-level parking lot map.

f) In the *Map designer* task, open the *multi-level parking* map.

g) Using the **Vector** tools, draw a polygon over each level of the parking lot.



h) From the **Links** widget, assign the parking zone that corresponds to each polygon.

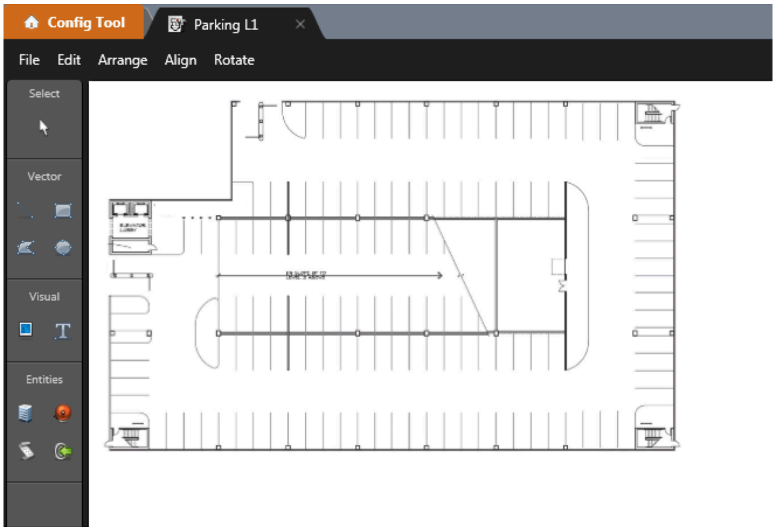


i) To display the occupancy of each parking zone on the map, in the toolbar, drag each of the parking zones onto the map from the **Area view** as you did for the first map.

j) In the *Map designer* toolbar, click **Save** ().

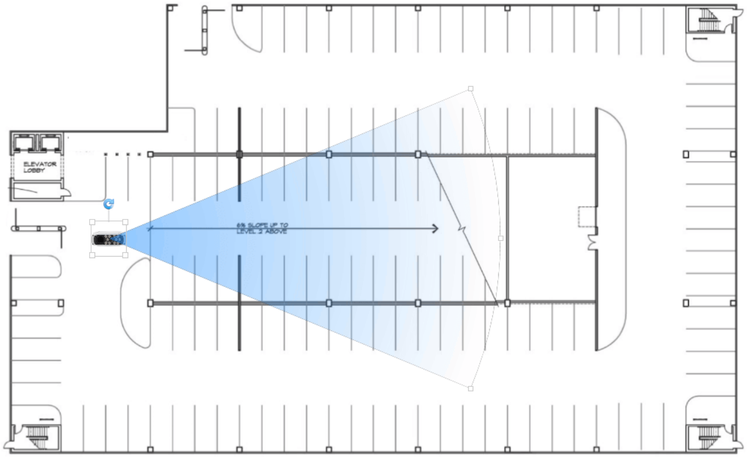
k) In the *Map designer* task, open the *Parking level 1* map.

NOTE: It is not necessary to link polygons to any additional maps because for this example, the parking zone is the lowest level of this drill-down.



l) To add a Sharp video unit that is monitoring the parking zone, click **Area view** (🏢), and drag the Sharp onto the map.

- If you want to display license plate reads, drag in the Sharp unit.
- If you want to display a representation of the Sharp's field of view, drag in the ALPR camera that is listed under the Sharp unit, as shown in the following image. Select **Show field of view** from the *Field of view* widget.



m) In the *Map designer* toolbar, click **Save** (💾).

48

AutoVu mobile systems

This section includes the following topics:

Preparing to deploy a mobile SharpZ3 system

To make sure that your mobile AutoVu™ deployment goes smoothly, you must perform a series of pre-configuration steps.

The following steps describe a typical AutoVu deployment. Depending on your specific installation requirements, your process might be different.

NOTE: Settings that are pre-configured during your installation are not listed in this task. For example, when you install Security Center, the ALPR Manager root folder is automatically created on your computer at the location *C:\Genetec\AutoVu\RootFolder*.

Security Center

Step	Task	Where to find more information
1	Install Security Center Server software on your *main server*.	• Installing Security Center in the *Security Center Installation and Upgrade Guide*.
2	(Optional) Install Security Center Server software on *expansion servers*.	• Adding expansion servers in the *Security Center Installation and Upgrade Guide*.
3	(Optional) Add an additional server to act as *secondary server* for the ALPR Manager to set up failover.	• Setting up role failover on page 164.
4	Install Security Center Client software on at least one workstation.	• Installing Security Center client software in the *Security Center Installation and Upgrade Guide*.

SharpZ3 hardware

Step	Task	Where to find more information
1	Install the SharpZ3 camera system on the patrol vehicle.	• Deployment overview for law, university parking, city parking, overtime parking, or MLPI in the *SharpZ3 Deployment Guide*.
2	Update the SharpZ3 system to the latest SharpOS version.	• Updating a Sharp unit in the *SharpZ3 Deployment Guide*.
3	Configure the SharpZ3 system in the Sharp Portal.	• Logging on to the Sharp Portal in the *SharpZ3 Administrator Guide*.

Genetec Patroller

Step	Task	Where to find more information
1	Install Patroller on the in-vehicle computer.	• Installing Patroller in the *Patroller Administrator Guide*
2	Upgrade Patroller to the latest software version.	• Upgrading Patroller in the *Patroller Administrator Guide*

After you finish

Configure the additional settings for your AutoVu mobile installation type:

- Law Enforcement
- City and University Parking Enforcement
- Mobile License Plate Inventory

Deployment overview for your mobile AutoVu system

To integrate ALPR-equipped patrol vehicles into Security Center, you can deploy a mobile AutoVu™ system.

The following steps describe a typical AutoVu deployment. Depending on your specific installation requirements, your process might be different.

Step	Task	Where to find more information
1	Complete the pre-configuration steps.	• Preparing to deploy a mobile SharpZ3 system on page 1104.
2	Use the Admin account in Config Tool to connect your system.	• Logging on to Security Center through Config Tool on page 7.
3	Configure the ALPR Manager server and database settings.	• Configuring the ALPR Manager role on page 961.
4	Configure the Archiver role in Security Center.	• Setting up the Archiver role for ALPR on page 963.
5	Connect Genetec Patroller™ to Security Center so that Patroller is discovered by the ALPR Manager.	• Connecting Patroller to Security Center on page 1108.
6	(Optional) Create and configure hotlist, permit, and overtime rules.	• Creating hotlists on page 985. • Creating parking permits on page 1139. • Creating overtime rules on page 1131.

After you finish

Configure the additional settings for your AutoVu mobile installation type:

- Law Enforcement.
- City and University Parking Enforcement.
- Mobile License Plate Inventory.

About Patroller

A *Genetec Patroller*™ entity represents the software that runs on a patrol vehicle's in-vehicle computer. The software verifies license plates captured by ALPR units mounted on the vehicle against lists of vehicles of interest and vehicles with permits. It also collects data for time-limited parking enforcement.

The *Patroller* interface alerts users of license plates matching the above rules so that immediate action can be taken.

Depending on your AutoVu™ solution, Patroller can be used to do the following:

- Verify license plate reads from an *ALPR camera* against lists of vehicles of interest (hotlists) and vehicles with permits (permit lists).
- Alert you of hotlist, permit, or overtime hits so that you can take immediate action.
- Collect data for time-limited parking enforcement.
- Collect license plate reads to create and maintain a license plate inventory for a parking facility.

Connecting Patroller to Security Center

You need to configure Genetec Patroller™ and Security Center so the ALPR Manager can discover and communicate with the Patroller units it controls.

To connect a Patroller to Security Center:

1 From the home page in Security Center Config Tool, click **System** > **Roles**, and then select the ALPR Manager you want to configure.

2 Click the **Properties** tab, and then click **Live**.

3 In the **Listening port** option, select the port to listen for connection requests coming from Patrollers.

4 To encrypt the communication between Security Center and Genetec Patroller™ Config Tool, select the **Encrypt communication channel** option.

   IMPORTANT: This setting also needs to be applied in Genetec Patroller™ Config Tool.

5 To allow Security Center to still accept incoming connections from Patrollers that do not have the encryption option enabled, select the **Access non encrypted messages** option.

6 Click **Apply**.

7 Open Genetec Patroller™ Config Tool.

8 Go to Security Center, and turn on the **Connect to Security Center** option.

9 Enter the IP address of the Security Center machine hosting the ALPR Manager role.

10 Enter the Port number Patroller should use to connect to the ALPR Manager role.

11 If you chose the Encrypt communication channel option in Security Center Config Tool, turn the on the Encrypt communication channel option.

12 Select which **Live events** you want to send to Security Center.

13 Beside **Periodic transfer**, specify how often hotlist and permit list changes are downloaded to Patroller (if you have a live connection). The default transfer period is every 240 minutes. You can disable Periodic transfer on specific hotlists (not permit lists) in Config Tool on the hotlist’s Advanced page. For more information, see Configuring advanced hotlist settings on page 1012.

14 Click **Apply**.

Configuring the Patroller entity in Security Center

From the *ALPR* task, you can configure sound management, acknowledgment buffer settings, and a hit delay for the patrol vehicle.

Before you begin

Connect Genetec Patroller™ to Security Center.

What you should know

- When you select the Patroller entity that you added to Security Center, you cannot modify the computer's settings in the computer's **Properties** tab.
- Information about the computer hosting the Patroller entity under **Properties** cannot be modified.

To configure the Patroller entity:

1 From the Config Tool home page, open the *ALPR* task, and click **Roles and units**.

2 Under the ALPR Manager, select the Patroller entity you want to configure, and click the **Properties** tab.

3 Under **File association**, configure how hotlists and permits should be used.
   - **Inherit from ALPR Manager role:** Patroller uses the hotlists and permit lists associated with its parent ALPR Manager. This is the default setting.
   - **Specific:** Associate specific hotlists or permit lists with the Patroller unit rather than the ALPR Manager. If you move the Patroller entity to another ALPR Manager, the hotlist or permit list will follow.

4 Under **Sound management**, configure Patroller to play a sound when reading a plate and/or generating a hit, and choose whether sounds should be played even when the application is minimized
   - **Play sound on hit:** Plays a sound when Patroller generates a hit.
   - **Play sound on read:** Plays a sound when Patroller reads a plate.
   - **Play sounds even when minimized:** Play sounds even if the Patroller window is minimized.

5 Under **Acknowledgment buffer**, specify a buffer restriction that limits how many hits can remain unacknowledged (not accepted or rejected) before Patroller starts automatically rejecting all subsequent hits. You can also choose (by priority) which hotlists should comply with this restriction
   - **Reject count:** How many unacknowledged hits are allowed.
   - **Reject priority:** When you create a hotlist entity, you can specify a priority for that hotlist. This setting tells Patroller which hotlist(s) should comply with the buffer restriction.

6 Under **Hotlist and permit**, specify the **Duplicate hit delay** that tells Patroller to disregard multiple hits on the same plate for the duration of the delay. For example, if you set a delay of 10 minutes, no matter how many times Patroller reads the same plate during those 10 minutes, it will generate only one hit.

The Patroller entity is configured in Security Center. The settings will be pushed to the Patroller running on the in-vehicle computer the next time it connects to Security Center.

After you finish

Configure Patroller using Genetec Patroller™ Config Tool (see the *Genetec Patroller™ Administrator Guide)*.

Adding user custom fields to license plate reads and hits

To associate a user's metadata with individual Genetec Patroller™ reads and hits so you can query and filter for those user custom fields in Security Desk *Reads* and *Hits* reports, you can add user custom fields to ALPR annotation fields.

Before you begin

- Configure Patroller to require a username and/or password to log on. For more information, see the *Genetec Patroller™ Administrator Guide*.

What you should know

- If you add additional attributes to a hotlist, they are automatically added as annotation fields when a hit occurs for the hotlist. For more information on configuring hotlist attributes, see Configuring hotlist and permit attributes on page 1007.
- You cannot add custom fields to reads and hits if Patroller is set to "No logon", because the reads and hits must be attached to a valid username.

To add user-related custom fields to reads and hits:

1. Create the custom field that applies to user entities.
2. Define the custom field for your Patroller users.
3. Add the custom field as an annotation field.

The custom field is now available as two separate columns in Security Desk "Reads" and "Hits" reports. One is a *Custom field* column that displays the latest value configured for the User entity. The other column is an *Annotation field* column that displays the value for the User entity when the read or hit was stored by the ALPR Manager role. For more information about Viewing ALPR events in Security Desk, see the *Security Center User Guide*.

Example

You have several Patroller users that alternate between different patrol teams, such as police officers moving between different city zones. By defining each patrol team as a user custom field, you can generate a report in Security Desk that displays the reads or hits collected when the officer was in patrol team A, patrol team B, and so on.

Creating user custom fields for reads and hits

To add more information to the properties of license plate hits and reads, you can create custom fields.

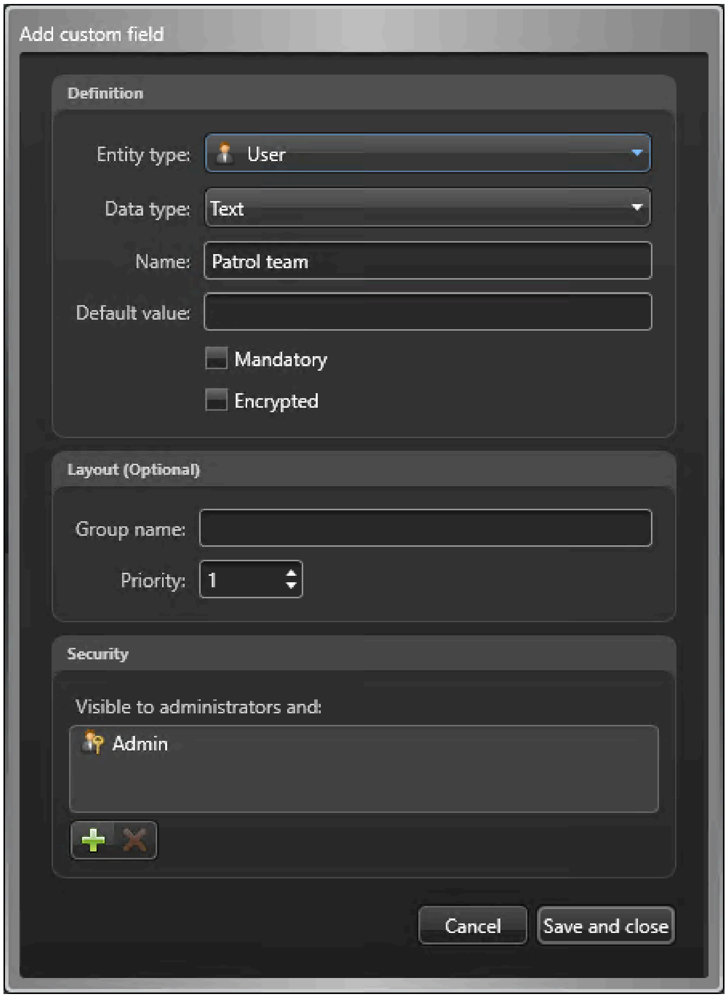
Before you begin

If you want to create a custom field using your own custom data type, the data type must already be created.

To create a user custom field:

1. Open the *System* task and click the **General settings** view.
2. Click the **Custom fields** tab, and click **Add an item** (+) at the bottom of the custom field list.

3 From the **Entity type** list in the *Add custom field* dialog box, select **User**.



Entity type: User

Data type: Text

Name: Patrol team

Default value:

□ Mandatory

□ Encrypted

Group name:

Priority: 1

Visible to administrators and:

Admin

4 From the **Data type** list, select a standard or custom data type for the custom field.

5 In the **Name** field, type the name for the custom field.

For example, type `Patrol Team`.

6 (Optional) In **Default value** field, type or select the default value for this field.

7 Depending on the selected data type, the following additional options are available:

- **Mandatory:** Select this option if the custom field cannot be empty.
- **Value must be unique:** Select this option if the value of the custom field must be unique.

  NOTE: The *unique value* option can only be enforced after the field is created. To enforce this option, you must first make sure that all entities in your system have a distinct value for this custom field, then edit this custom field to apply the unique value option to it. Selecting this option automatically selects the **Mandatory** option.
- **Encrypted:** Select this option if you want this field to be encrypted in the database (encryption at rest).

  NOTE: You must make that decision at creation time. You cannot change this option after the field is created. For other limitations regarding custom field encryption, see About custom fields on page 91.

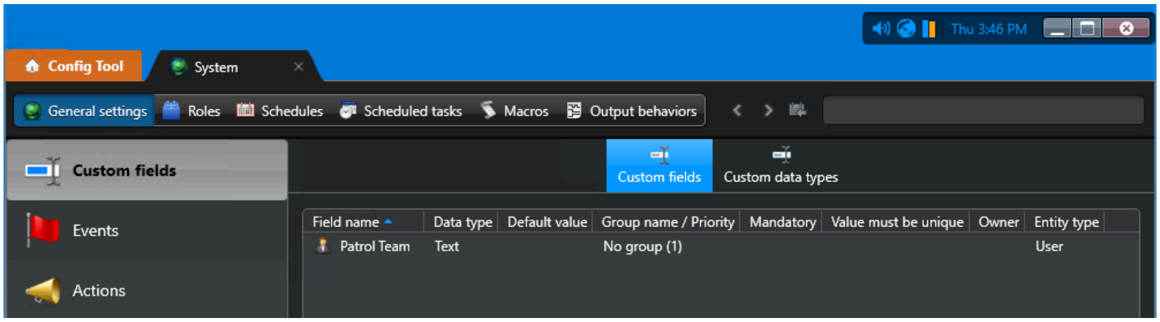
8 Under the *Layout* section, type the **Group name**, and select the **Priority** from the drop-down list.

These two attributes are used when displaying the unit's web page, field in the *Custom fields* page of associated entity. The group name is used as the group heading, and the priority dictates the display order of the field within the group.

9 In the *Security* section, click + to add users and user groups that are able to see this custom field.

By default, only administrators can see a custom field.

10 Click **Save and close**.



Field name	Data type	Default value	Group name / Priority	Mandatory	Value must be unique	Owner	Entity type
Patrol Team	Text		No group (1)				User

11 Click **Apply**.

The new custom field is available in your users' *Custom fields* page.

Related Topics

About custom fields on page 91

Defining custom fields for Patroller users

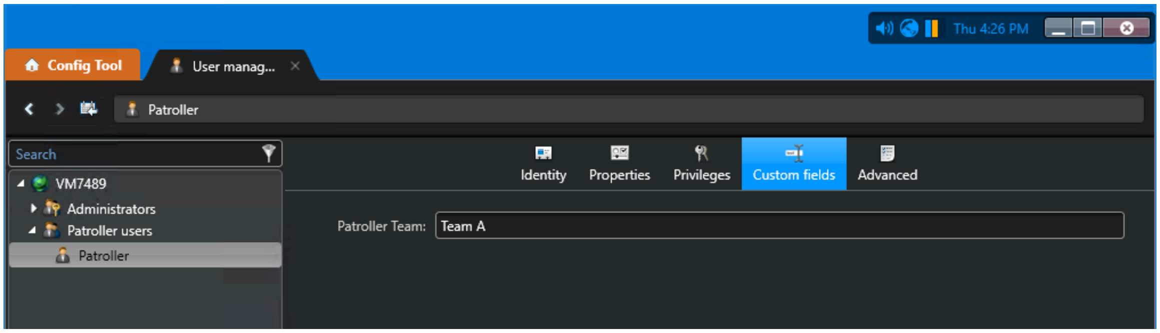
After user custom fields are created in Security Center, you can define them in the *Custom fields* tab of the Genetec Patroller™ users.

To define a custom field for a Patroller user:

1 From the Config Tool home page, click **Security** > **Users**, and then select the user you want to configure.

2 Select the **Custom fields** tab.

Custom fields that are already created for user entities are displayed.



Patroller Team: Team A

3 Type the **Patroller Team** for the current Patroller user.

For example, type **Team A**.

4 Click **Apply**.

This Patroller user now has a User ID of *Team A*. You can now add this custom field as an annotation field for reads and hits.

Related Topics

Creating user custom fields for reads and hits on page 1110

Adding custom fields as annotation fields

After you have created and defined custom fields for Genetec Patroller™ users, you must add those custom fields to the list of annotation fields for Patroller reads and hits.

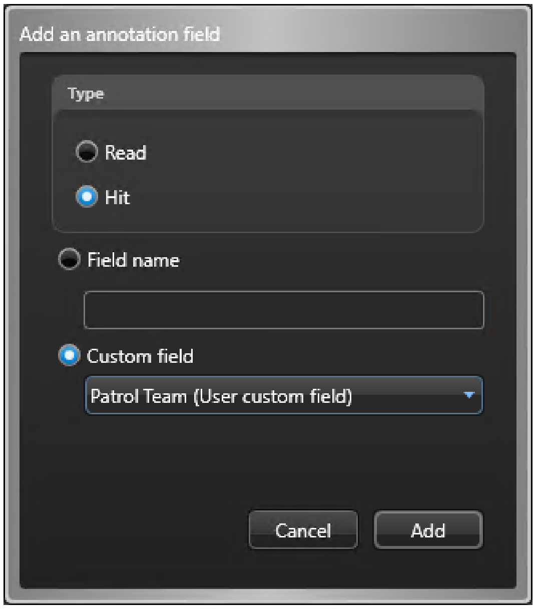
To add a custom field as an annotation field:

1 From the Config Tool home page, click **ALPR** > **General settings** > **Annotation fields**.

2 Click **Add an item** (➕).

The **Add an annotation field** window appears.

3 Under **Type**, in the *Add an annotation field* dialog box, select **Read** or **Hit**.



Add an annotation field

Type

○ Read

● Hit

○ Field name

● Custom field

Patrol Team (User custom field)

4 Select **Custom field**, and then select the user custom field you created.

5 Click **Add**.

Your user custom field is added to the list of annotation fields for all Patroller reads or hits. Security Center now associates reads or hits with the user custom field (the **Patrol Team** in this case**)** that was logged on to Patroller at the time the event occurred. This value is stored in the database for each read or hit.

NOTE: If you want the same user custom field for reads *and* hits, you must define it as an annotation field twice, once for reads and once for hits.

Related Topics

Creating user custom fields for reads and hits on page 1110

Sound files used in Patroller

Genetec Patroller™ uses sounds to communicate information and to prompt the patrol vehicle operator to take action. The sound files are located on the in-vehicle computer in the folder: *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds* (default location).

The following *.wav* sound files are included:

- **Ambiguity:** Indicates that Patroller is configured to automatically select the zone, but operator confirmation is needed.
- **CalibrationError:** Indicates that an AutoVu™ Navigation system calibration step was not successful
- **CalibrationInstruction:** Indicates the next step in the AutoVu Navigation calibration
- **EnterZone:** Indicates that the patrol vehicle has entered a parking zone or overtime zone
- **ExitZone:** Indicates that the patrol vehicle has exited a parking zone or overtime zone
- **HotlistHitEvent:** Indicates that the license plate is included in a hotlist
- **NotificationError:** Indicates that an error has occurred.
- **OvertimeHitEvent:** Indicates that the parked vehicle has an overtime violation
- **PermitHitEvent:** Indicates that the parked vehicle does not have the required permit to park in the zone
- **TooManyReadsEvent:** Indicates that the maximum number of plates in the MLPI inventory has been exceeded
- **VehicleEvent:** Indicates that a license plate has been read

Changing sound files for ALPR events

You can add new sound files to Genetec Patroller™ to use for ALPR events by manually copying the files to the Patroller in-vehicle computer.

What you should know

- The sound files must be *.wav* format.
- You can replace a default sound file with a new sound file that has the same file name.

  Example: If you have a file called *alert.wav*, and you want to use it for a permit hit, you must rename your file to *PermitHitEvent* to match the default sound file name before copying it to the *Sounds* folder (either manually or through the updater service). This way it overwrites the default sound file, and Patroller can play it.
- Sounds for hotlist hits have more flexibility. You can overwrite the default sound *HotlistHitEvent* in the *Sounds* folder, or you can use a different filename for each hotlist loaded in Patroller, as long as you specify the path to each hotlist's sound file in Security Center Config Tool.

  BEST PRACTICE: New hotlist sound files can be stored anywhere on the in-vehicle computer, but you should keep them in the same *Sounds* folder as the default sound files. This makes it easier to update them later.

To replace a sound file:

1 To overwrite the default sound files, do the following:

   a) Open the folder *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds*.

   b) Rename your new sound file to match the default file you want to overwrite.

   c) Copy your renamed sound file to the *Sounds* folder so that it overwrites the default file.

2 Restart Patroller for your changes to take effect.

To configure a unique sound for each hotlist:

1 Copy your new sound file to any location on the in-vehicle computer.

2 Open Config Tool and select the **ALPR** task.

3 Select the hotlist to configure, and click the **Advanced** tab.

4 In the **Sound file** field, specify the path and filename to the sound file on the in-vehicle computer.

   To configure sounds for additional hotlists, repeat Steps 3 and 4.

Changing sound files for ALPR events using the updater service

You can send different sound files to the patrol vehicle's *MobileClient* folder using the Security Center updater service.

What you should know

The sound files for permit hits, overtime hits, and plate reads must be in the default *Sounds* folder for Genetec Patroller™ to be able to play them.

After sending the files to the *MobileClient* folder, you can manually move the files to the *Sounds* folder if you choose, but you can also zip your sound file so that Windows extracts it to the *Sounds* folder automatically.

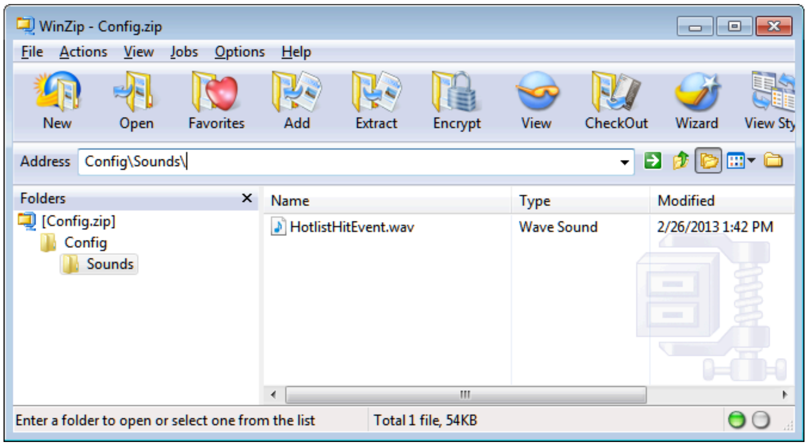
To change the sound files for ALPR events using the updater service:

1 (Optional) To overwrite a default sound file, rename your new sound file to match the name of the default file you want to replace (for example, *HotlistHitEvent.wav*).

2 On the Security Center computer, create the same Windows Explorer file structure found on the Patroller in-vehicle computer (for example, *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds*).

3 Copy your new sound file to the *Sounds* folder you created.

4 Zip the sound file at the *Config* level so that it mirrors the relative path from the *MobileClient* folder to the *Sounds* folder on the in-vehicle computer.



Address Config\Sounds\

[Config.zip]
Config
Sounds

Name	Type	Modified
HotlistHitEvent.wav	Wave Sound	2/26/2013 1:42 PM

Enter a folder to open or select one from the list
Total 1 file, 54KB

The file extracts to the destination defined in the zip file path (*Sounds* folder).

5 (Optional for hotlist sounds) If the file has a different filename than the default *HotlistHitEvent*, you must specify the full path to the file, including the new filename:

a) From the Config Tool home page, open the **ALPR** task.

b) Select the hotlist to configure, and click the **Advanced** tab.

c) In the **Sound file** field, specify the path and filename to the sound file on the in-vehicle computer.

d) Repeat the steps for as many hotlists as you want.

6 Send the sound file to Patroller as if you were installing an update wirelessly. For more information, see the *Genetec Patroller™ Administrator Guide*.

Patroller restarts after installing the update, and now uses the new sound file for your chosen ALPR event.

49

AutoVu Law Enforcement systems

This section includes the following topics:

About Law Enforcement

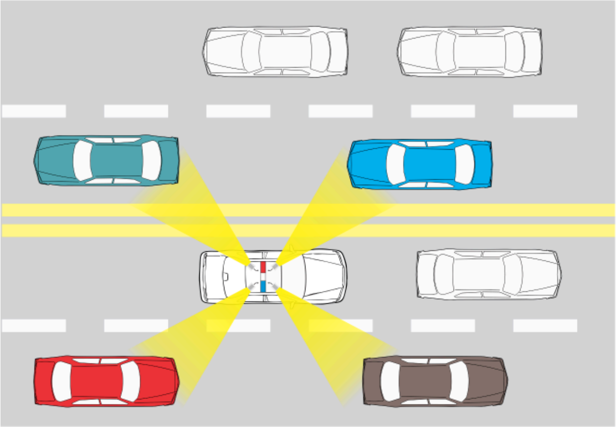
Law Enforcement is a Genetec Patroller™ software installation that is configured for law enforcement: the matching of license plate reads against lists of wanted license plates (hotlists). The use of maps is optional.

As you patrol, the Sharp cameras installed on the vehicle automatically read plates and send the information to Genetec Patroller™. If a plate is on a loaded hotlist, Patroller alerts you, and you can take immediate action.

Hotlists typically contain information on stolen vehicles, scofflaw suspects, amber alerts, and so on. The use of in-vehicle mapping with a Law Enforcement installation is optional.

Example

You can have up to six Sharp cameras installed on a patrol vehicle. This allows you to capture the maximum number of plates on vehicles in different lanes and even those traveling in the opposite direction. The following diagram shows a Patroller law enforcement vehicle equipped with four cameras:



Creating hit accept and hit reject reasons for hotlist hits

When an operator chooses to accept or reject a license plate hit, in addition to the pre-defined reasons that the operator can choose from, you can also define custom hit accept or hit reject reasons that can be selected by the operator.

What you should know

- **Hit reject reasons:** List of reasons for rejecting hotlist hits. These values also become available as Reject reason filter options for generating hit reports in Security Desk. Several categories are pre-configured for you when you install Security Center.
- **Hit accept reasons:** A form that contains a list of questions that Genetec Patroller™ users must answer when they accept a hit. The information from the hit form can be queried in the Security Desk Hit report. There are no pre-configured categories.
- The settings are downloaded along with the selected hotlists and permit lists to Patroller when the operator logs on.
- Hit reject and accept reasons are applied at the Directory level, which means that all the ALPR Managers in your system share the same settings.
- The attributes you create are also available as filter options for hit reports in Security Desk.

To create a hit accept or hit reject reason:

1. From the Config Tool home page, click **ALPR** > **General settings** > **Hotlist**.
2. Add **Hit accept reasons** or **Hit reject reasons** as needed.

   For example, you can add the following questions as **Hit accept reasons** to have the patrol officer collect the necessary information:

   - Number of people in the vehicle
   - Did you perform a vehicle search
   - Are any children present in the vehicle
3. Click **Apply**.

The new hit accept and reject reasons are downloaded to Patroller the next time it is connected to Security Center.

Creating *New Wanted* attributes and categories

You can create customized license plate attributes and categories to appear in Genetec Patroller™. Patrol vehicle operators can select from these attributes when adding a *New wanted* license plate.

What you should know

- If a patrol vehicle has a wireless connection, updated hotlists can be automatically pushed to Patroller. If, however the vehicle does not have a wireless connection, the operator can still manually add a license plate to a local hotlist by creating a *New wanted* license plate entry. In Security Center, you can configure attributes and categories that are visible to the operator when creates a *New wanted* entry.
  - **New wanted attributes:** Attributes other than the standard ones (plate number, plate issuing state, category) that a Patroller user is asked to specify when entering a new wanted item in the Patroller. One category is pre-configured for you when you install Security Center.
  - *New wanted* **categories:** List of categories that a Patroller user can pick from when entering a new wanted item. The category is the attribute that says why a license plate number is wanted in a hotlist. Several categories are pre-configured for you when you install Security Center.

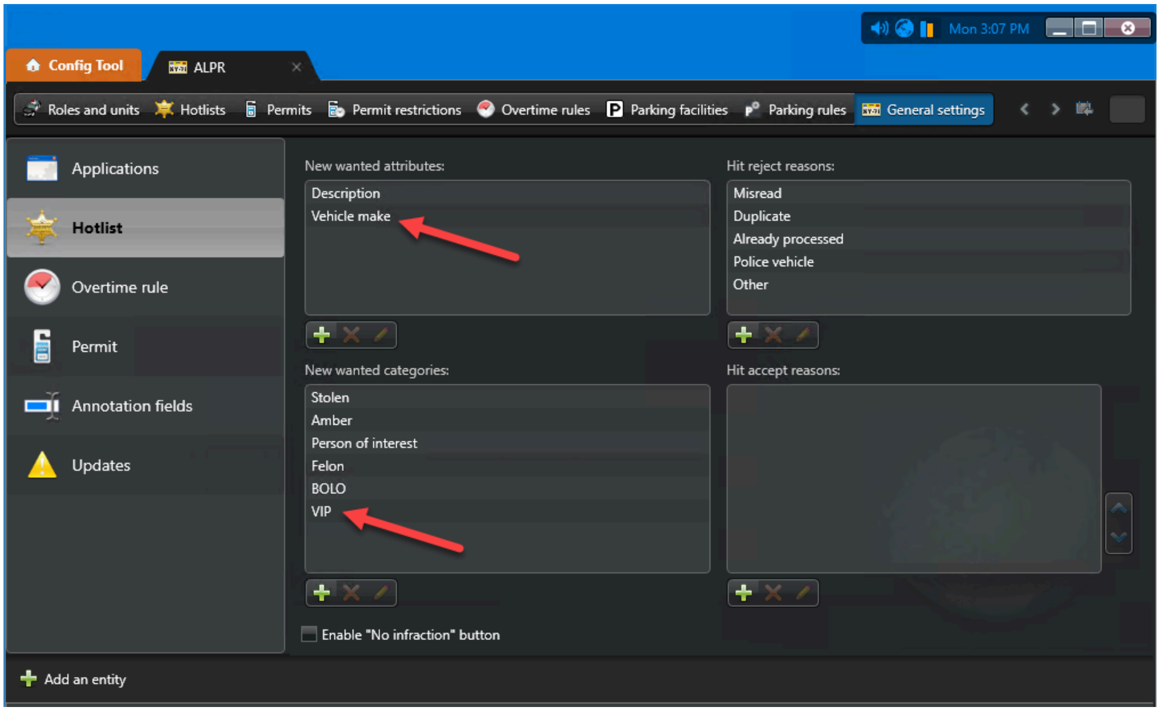
    NOTE: BOLO is an acronym for “Be On The Lookout”, sometimes referred to as an all-points bulletin (APB).
- *New wanted* categories and attributes are applied at the Directory level, which means that all the ALPR Managers in your system will share the same settings.

To create *New wanted* attributes and categories:

1 From the Config Tool home page, click **ALPR** > **General settings** > **Hotlist**.

2 Add **New wanted attributes** or **New wanted categories** as needed.

In this example, we've added the **Attribute:** *Vehicle make* and the **Category:** *VIP*.



New wanted attributes:
Description
Vehicle make

Hit reject reasons:
Misread
Duplicate
Already processed
Police vehicle
Other

New wanted categories:
Stolen
Amber
Person of interest
Felon
BOLO
VIP

Hit accept reasons:

□ Enable "No infraction" button

3 Click **Apply**.

The new attribute and category are uploaded to Patroller the next time it is connected to Security Center.

When the operator adds a *New wanted* license plate, the new the *Vehicle make* field and the *VIP* category selection are available.

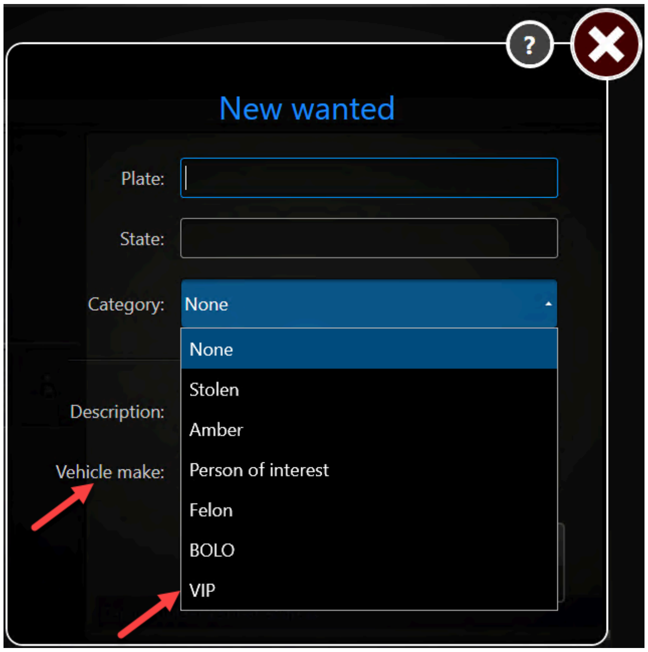

New wanted

Plate:

State:

Category: None

- None
- Stolen
- Amber
- Person of interest
- Felon
- BOLO
- VIP

Description:

Vehicle make:

After you finish

Configure the *New wanted* attributes and categories in Patroller Config Tool. For more information, see the *Genetec Patroller™ Administrator Guide*.

50

AutoVu City and University Parking Enforcement systems

This section includes the following topics:

About City Parking Enforcement

City Parking Enforcement is a Genetec Patroller™ software installation that is configured for the enforcement of parking permit and overtime restrictions.

In City Parking Enforcement, Genetec Patroller™ matches plates on parked vehicles to overtime rules (rules about how long vehicles are allowed to park), permit lists (lists of vehicles that are allowed to park), or for both overtime rules and permit lists.

You can also use a city parking enforcement system with wheel imaging with to provide additional evidence of whether or not a vehicle has moved.

For information on how to deploy a city parking enforcement system, refer to the *AutoVu™ SharpZ3 Deployment Guide*.

Example

Here are some examples of when you would use each type of enforcement rule:

- **Overtime rule alone:** To maximize turnover and to avoid free parking abuse in a commercial area, vehicles are allowed to park for only two hours on main streets between 8:00 and 18:00. Any vehicles parked for more than two hours are in violation of the overtime rule. This results in an overtime hit in Patroller. In this example, you don't need a permit list because there are no exceptions to the rule.
- **Permit list alone:** Some residential areas allow only permit holders to park on neighborhood streets. Any vehicle parked in the area without a permit is in violation of the permit list. This results in a permit hit in Patroller. In this example, you don't need an overtime rule because there are no time limits. Any vehicle parked without a valid permit (for example, an expired permit or no permit) is in violation, regardless of the day or time.
- **Overtime rule and permit list together:** Some residential areas allow permit holders to park indefinitely, and non-permit holders to park for a limited time. Any vehicle without a permit, that is parked in the area longer than the limit allows, is in violation of the overtime rule. This results in an overtime hit. In this example, you need both an overtime rule, and a permit list to determine if a parked vehicle is in violation.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

▶

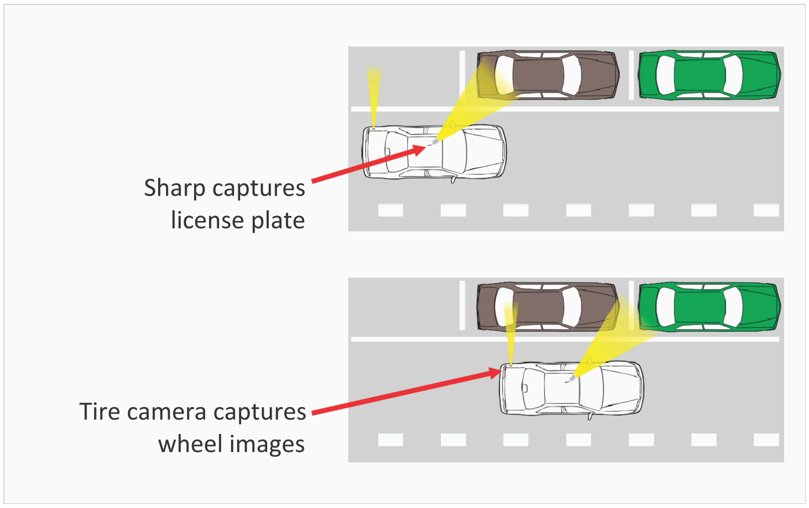
City Parking Enforcement with Wheel Imaging

In a City Parking Enforcement with Wheel Imaging system, Genetec Patroller™ uses wheel images taken by "tire cameras" as additional evidence of whether or not a parked vehicle has moved even a small distance.

For example, when you get an overtime hit, you can look at an image of the vehicle's wheels and see by the valve stem or other reference point (for example, a crack in the hubcap), that the vehicle hasn't moved. This photographic evidence can help prove the overtime offense if the driver claims to have moved the vehicle, and then parked again in the same area.

Example

Here is a Patroller vehicle with a Sharp camera and a single tire camera.



You cannot do wheel imaging on both sides of a street at the same time.

To accurately record wheel images, the SharpZ3 system must include the Navigation expansion module. This allows the system to interface into the vehicles odometry signal to know how far the patrol vehicle has traveled.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

Long-term overtime

To use a City Parking Enforcement system to monitor on-street parking for overtime violations between one and five days, you can configure long-term overtime settings in Security Center and Genetec Patroller™.

For more information on configuring Patroller for long-term overtime settings, see the *Genetec Patroller™ Administrator Guide*.

About University Parking Enforcement

University Parking Enforcement is a Genetec Patroller™ software installation that is configured for university parking enforcement: the enforcement of scheduled parking permits or overtime restrictions. The use of maps is mandatory. Hotlist functionality is also included.

University parking differs from City parking in several ways. With University parking:

- You apply a permit restriction to one or more permit lists, to specify where and when the permits apply.
- You can enforce overtime rules or permit restrictions for a selected parking lot, but not both at the same time.
- Wheel imaging is not supported.

For information on how to deploy a university parking enforcement system, refer to the *AutoVu™ SharpZ3 Deployment Guide*.

Example

The following examples show when you would use an overtime rule, and when you would use a permit restriction:

- **Overtime rule:** A university campus has several parking lots reserved for students and faculty, but also has conveniently located parking areas that are used by delivery vehicles for the loading or unloading of equipment.

  Using an overtime rule, you can allow any vehicle to park in the loading area at any time of day, but only for a limited time (for example, 20 minutes). A vehicle parked longer than 20 minutes is in violation of the overtime rule. This results in an overtime hit in Genetec Patroller™. In this example, you don't need a permit restriction because any vehicle can park, but only for a limited time.
- **Permit restriction:** A university parking lot can be used by both faculty and students, but at different times. Faculty can park on weekdays from 8:00 am to 6:00 pm, while students can park from 10:00 am to 4:00 pm This reserves the prime parking spaces for the university's faculty, but still allows students convenient parking during peak class hours. You wouldn't be able to create this parking scenario with an overtime rule. You need a permit restriction and associated permit lists. Vehicles without a permit, with an expired permit, or parked at the wrong time, are in violation of the permit restriction. This results in a permit hit in Patroller.

Related Topics

About permits on page 1137

Differences between City and University Parking Enforcement

The enforcement rules that you use, and how you configure them, depend on whether your system is configured for city or university enforcement.

The following table shows you which parking enforcement concepts and features are used with each type of system:

Concept or feature	City Parking Enforcement	University Parking Enforcement
Enforce permits and overtime simultaneously	Yes	No
District overtime	Yes	Yes
Block face overtime	Yes	Supported but not typically used.
Same position overtime	Yes	Supported but not typically used.
Multiple violations	Yes	Yes
Permits	Yes	Yes[1]
Permit restrictions	No	Yes
Shared permits	Yes	Yes
Parking lots ("zones")	Yes	Yes
Wheel imaging	Yes[2]	No
Long-term overtime	Yes[3]	No
Hotlist hits	Yes	Yes

[1] Permits must have permit restrictions applied to them in University Parking Enforcement.

[2] Used to provide more evidence that a vehicle has not moved.

[3] Requires the City Parking Enforcement with Wheel Imaging option to determine if a parked vehicle has not moved during the overtime period.

Deploying AutoVu City and University Parking Enforcement systems

You can configure your mobile AutoVu™ system specifically for City Parking Enforcement (with or without wheel imaging) or University Parking Enforcement.

Before you begin

- Perform the general configuration tasks for mobile AutoVu systems.

What you should know

- All parking enforcement systems require GPS and mapping capability.

To deploy an AutoVu City or University Parking Enforcement system:

1. Create the overtime rules.
2. Create the permit lists.
3. (*University Parking Enforcement* only) Create the permit restrictions.
4. Create parking lots for your overtime rules and permit restrictions.
5. (*City Parking Enforcement with Wheel Imaging* only) To provide accurate odometry readings to Genetec Patroller™, calibrate the AutoVu Navigation settings.

   For more information, see "Enabling Patroller Navigator box GPS settings" in the *Genetec Patroller™ Administrator Guide*.
6. Enable and configure overtime settings in Patroller.

   For more information, see "Configuring overtime settings" the *Genetec Patroller™ Administrator Guide*.
7. Enable and configure permit lists in Patroller.

   For more information, see "Configuring permit settings in Genetec Patroller™" the *Genetec Patroller™ Administrator Guide*.
8. (*City Parking Enforcement with Wheel Imaging* only) Configure the Patroller settings related to wheel imaging.

   For more information, see "Configuring wheel imaging settings in Genetec Patroller™" the *Genetec Patroller™ Administrator Guide*.
9. Configure the Patroller GPS and Map settings.

   For more information, see "Enabling Genetec Patroller™ Map settings" the *Genetec Patroller™ Administrator Guide*.

About overtime rules

An overtime rule is an entity that defines a parking time limit and the maximum number of violations enforceable within a single day. Overtime rules are used in city and university parking enforcement. For university parking, an overtime rule also defines the parking area where these restrictions apply.

The overtime rule is downloaded to Genetec Patroller™. In Patroller, an overtime hit occurs when the time between two plate reads of the same plate is beyond the time limit specified in the overtime rule. For example, your overtime rule specifies a **four hour** parking limit within a city district. The Patroller operator does a first pass through the district at 9:00 collecting license plate reads. The operator then does a second pass through the district at 13:05 If a plate was read during the first and second pass, Patroller generates an overtime hit.

An overtime rule is a type of hit rule. A hit rule is a method used by AutoVu™ to identify vehicles of interest. Other types of hit rules include *hotlist*, *permit*, and *permit restriction*. When a plate read matches a hit rule, it is called a *hit*. When a pair of plate reads (same plate read at two different times) violates an overtime rule, it is called an *overtime hit*.

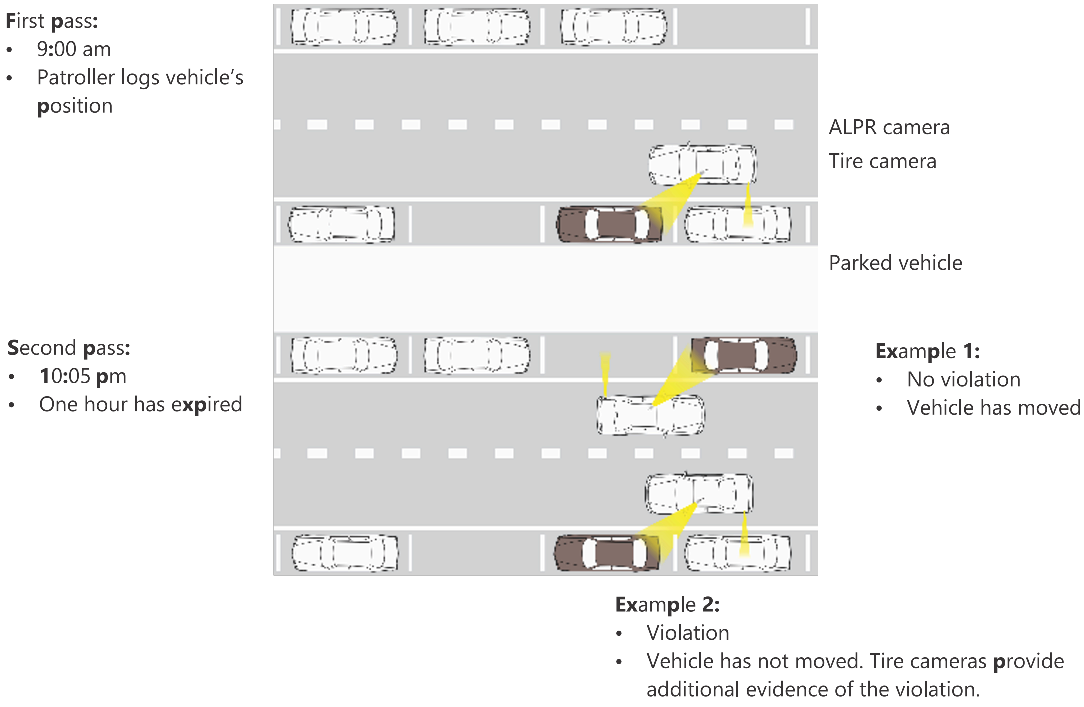
In City enforcement the wheel imaging option can be used to provide additional evidence of the violation by showing whether or not the vehicle has moved even a small distance.

Same position overtime rules

Same position overtime rules specify how long a vehicle is allowed to park in a *single parking space* on a particular street.

Example

The overtime rule states that vehicles can park for one hour in any parking space on this street. You do a first pass at 9:00 collecting license plate reads. You then do a second pass at 10:05. If Patroller reads the same plate in the same parking space, Patroller generates an overtime hit.



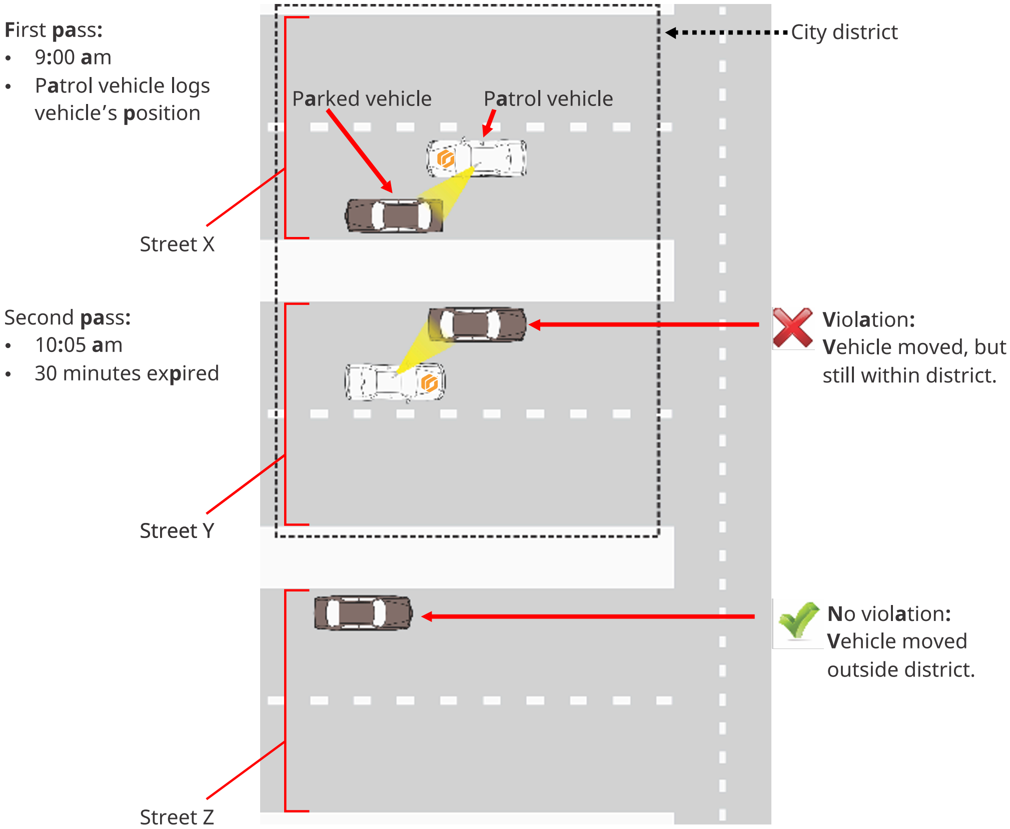
District overtime rules

District parking enforcement is a type of overtime rule that specifies when a vehicle is allowed to park *within a specific geographic location* (for example, a city district).

The borders of a "district" are not defined in Security Center Config Tool (for example, by drawing a polygon on a map), and there is no correlation with a city's formal boroughs or municipalities. A district exists where the Patroller user chooses to enforce it.

Example

The overtime rule states that between 9:00 and 17:00 on weekdays, vehicles can park for only 30 minutes within the district defined by Street X and Street Y. You do a first pass through the district at 9:30 collecting license plate reads. You then do a second pass through the district at 10:05. If the patrol vehicle reads the same plate within the same district (regardless if the vehicle has moved or not), the vehicle is in violation of the overtime rule, and you get an overtime hit.



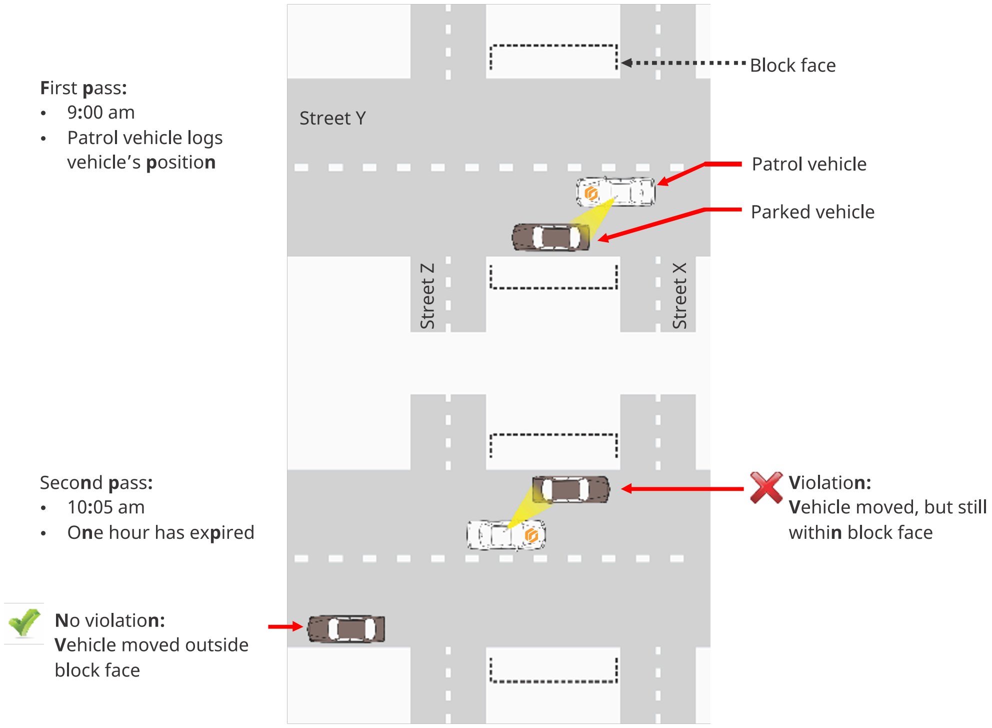
Block face overtime rules

Block face parking enforcement is a type of overtime rule that specifies when a vehicle is allowed to park *on both sides of a street*, between intersecting cross-streets.

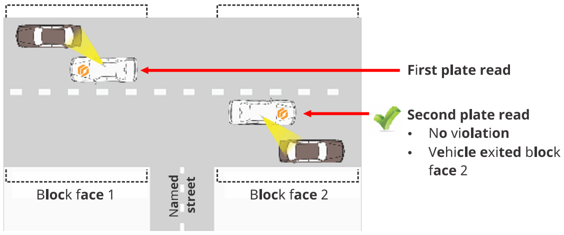
The borders of a "block face" are not defined in Config Tool (for example, by drawing a polygon on a map). They are defined on the spot for each individual plate read. For example, when a Patroller user selects a block face overtime rule, and then reads a license plate, Patroller uses GPS to determine the block face for that particular plate read based on the intersecting cross-streets closest to the parked vehicle's position.

Example

The overtime rule states that vehicles can park for one hour on either side of Street Y, between Street X and Street Z. You do a first pass through the block face at 9:00 collecting license plate reads. You then do a second pass down the block face at 10:05. If Patroller reads the same plate within the same block face, the vehicle is in violation of the overtime rule, and you get an overtime hit.



NOTE: Patroller considers “T intersections” to be valid borders of a block face. For example, in the following scenario, Patroller would *not* raise an overtime hit because the T intersection is seen as the end of *Block face 1*, and the beginning of *Block face 2*.



Creating overtime rules

You can create an overtime rule entity in Security Center Config Tool to define the parking time limit and the maximum number of violations enforceable within a single day. After you create the entity, you must configure its settings for your enforcement scenario.

What you should know

You can use overtime rules for both City Parking Enforcement and University Parking Enforcement.

To create an overtime rule:

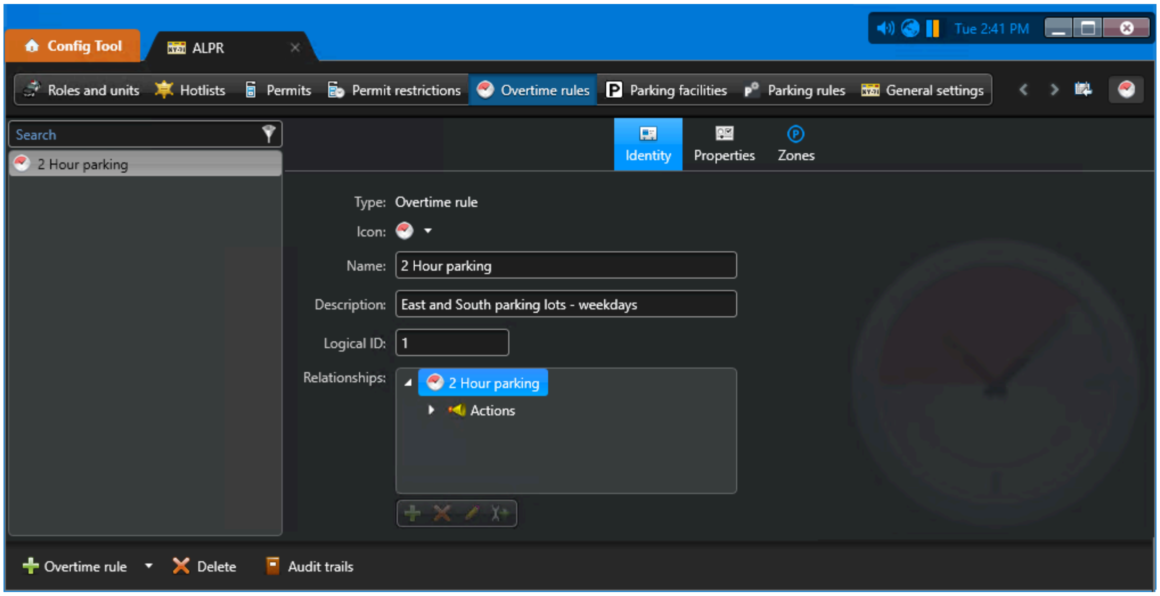
1 From the Config Tool home page, click **ALPR** > **Overtime rules** and then click **Overtime rule** (✚).

2 In the **Identity** tab, enter the required information:

- **Name:** In City Parking Enforcement, this name appears in Genetec Patroller™ on the overtime rule selection page. In University Parking Enforcement, this name appears appended to the parking lot name on the zone selection page.

  TIP: Choose a name that describes the details of the enforcement scenario. This makes it easier to select it in Patroller when you have more than one available.
- **(Optional) Description:** You can add a longer description for the rule. This field does not appear in Patroller.
- **(Optional) Logical ID:** Enter a Logical ID if applicable.

3 Click **Apply**.



Type: Overtime rule

Icon:

Name: 2 Hour parking

Description: East and South parking lots - weekdays

Logical ID: 1

Relationships: 2 Hour parking
Actions

The overtime rule appears in a flat list view that displays all the overtime rules on your system. Patroller downloads overtime rules when it connects to Security Center.

After you finish

Configure the overtime rule.

Configuring overtime rules

To use an overtime rule entity after you have added in Security Center, you must configure it for your enforcement scenario.

Before you begin

Create the overtime rule.

What you should know

You must configure an enforcement area (or parking lot) for each permit restriction and overtime rule that you create.

To configure an overtime rule:

1. From the Config Tool home page, click **ALPR** > **Overtime rules**, and select the overtime rule you want to configure.
2. Click the **Properties** tab.
3. Select a **Color** for the overtime rule.

   This will be the color of the overtime hit screen in Genetec Patroller™ and Security Desk, as well as the plate reads due for enforcement on the Patroller map.
4. (City Parking Enforcement with Wheel Imaging only) Select the **Vehicle parking position**.

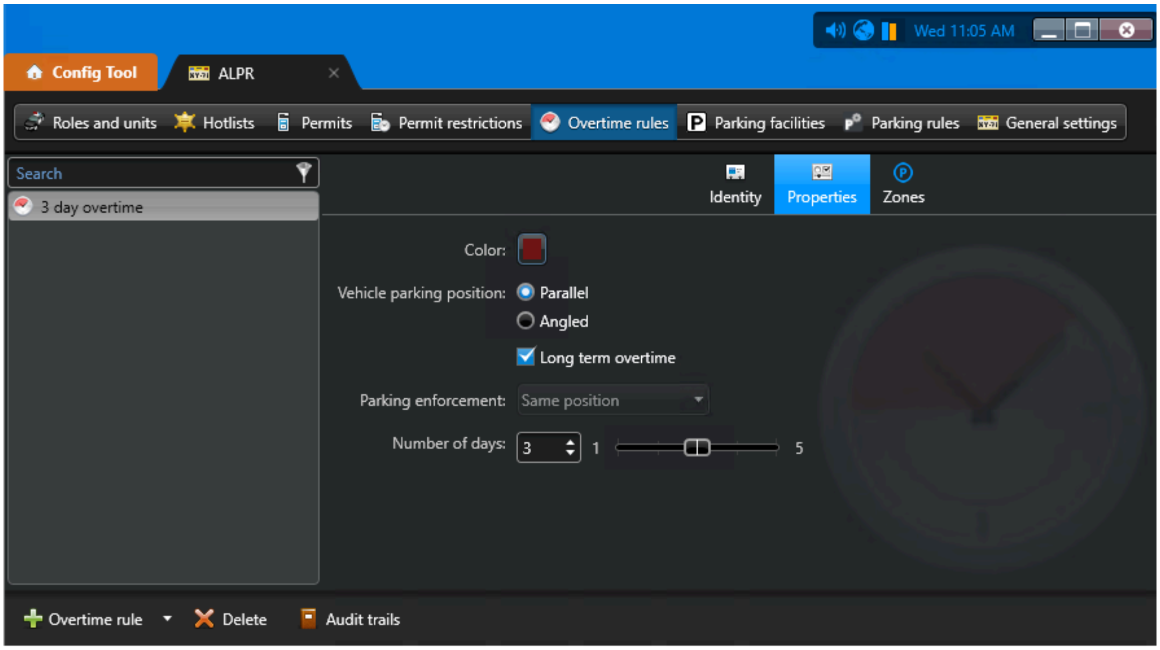
   This option tells Patroller which parameters to use for wheel imaging: Parallel or Angled (45-degree).

   NOTE: You cannot use the same overtime rule for both Parallel and Angled parking enforcement. If you're doing both types of enforcement, you must create separate overtime rule entities for each.
5. (Optional) Select **Long term overtime** to allow vehicles to park in the same spot for up to five days in Patroller City Parking Enforcement systems.

   NOTE:

   - A patrol vehicle can only be linked to one long-term overtime rule and cannot switch between long-term overtime rules. For example, if a city has three long-term overtime rules, it needs at least three patrol vehicles.
   - You can have only one *Long term overtime* rule per Directory role.
   - For more information on configuring Patroller for long-term overtime settings, see the *Genetec Patroller™ Administrator Guide*.

6 If you are using long-term overtime, set the **Number of days** that vehicles can park in the zone. When a patrol vehicle enters the long-term overtime zone, the system considers all reads for the number of days defined here.



Color: 🟥

Vehicle parking position: ● Parallel ○ Angled

☑ Long term overtime

Parking enforcement: Same position

Number of days: 3 1 5

7 From the **Parking enforcement** list, select the type of restricted parking area that applies to the time limit: a single parking spot, a district within a city, or both sides of a city block:

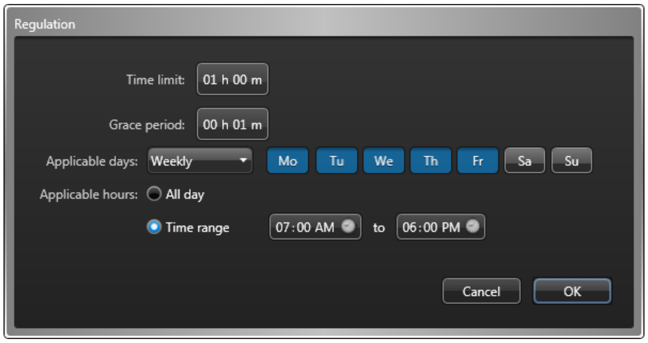
- **Same position:** A vehicle is parked overtime if it parks in the same spot longer than the specified time limit. For example, your overtime rule specifies a one hour parking limit for a single parking space. The Patroller operator does a first pass through the district at 9:00 am collecting license plate reads. The operator does a second pass at 10:05 am If Patroller reads the same plate in the same spot both times, it results in an overtime hit.

  IMPORTANT: For this feature to work, Patroller needs GPS capability.

  NOTE: When you select **Long term overtime**, the **Parking enforcement** option is automatically set to **Same position**, meaning the vehicle has parked overtime when it stays in the same parking space beyond the parking time limit set for such parking space.
- **District:** A vehicle is parked overtime if it is parked anywhere within a city district (a geographical area) longer than the specified time limit. For example, your overtime rule specifies a four hour parking limit within a city district. The Patroller user does a first pass through the district at 9:00 am collecting license plate reads. The operator does a second pass through the district at 1:05 pm If Patroller reads the same plate in the same district both times, it results in an overtime hit.
- **Block face (2 sides):** A vehicle is parked overtime if it is parked on either side of a road between two intersections longer than the specified time limit. For example, your overtime rule specifies a 1hour parking limit within a city block face. The Patroller operator does a first pass through the block face at 9:00 am collecting license plate reads. The operator does a second pass down the block at 10:05 am If Patroller reads the same plate in the same block face both times, it results in an overtime hit.

8 To define the parameters of the overtime rule (for example, time limit, grace period, applicable days, and so on), under **Regulation**, click **Add an item** (➕) .

9 In the *Regulation* dialog box, configure the following, then click **OK**:



Regulation

Time limit: 01 h 00 m

Grace period: 00 h 01 m

Applicable days: Weekly Mo Tu We Th Fr Sa Su

Applicable hours: ○ All day

● Time range 07:00 AM to 06:00 PM

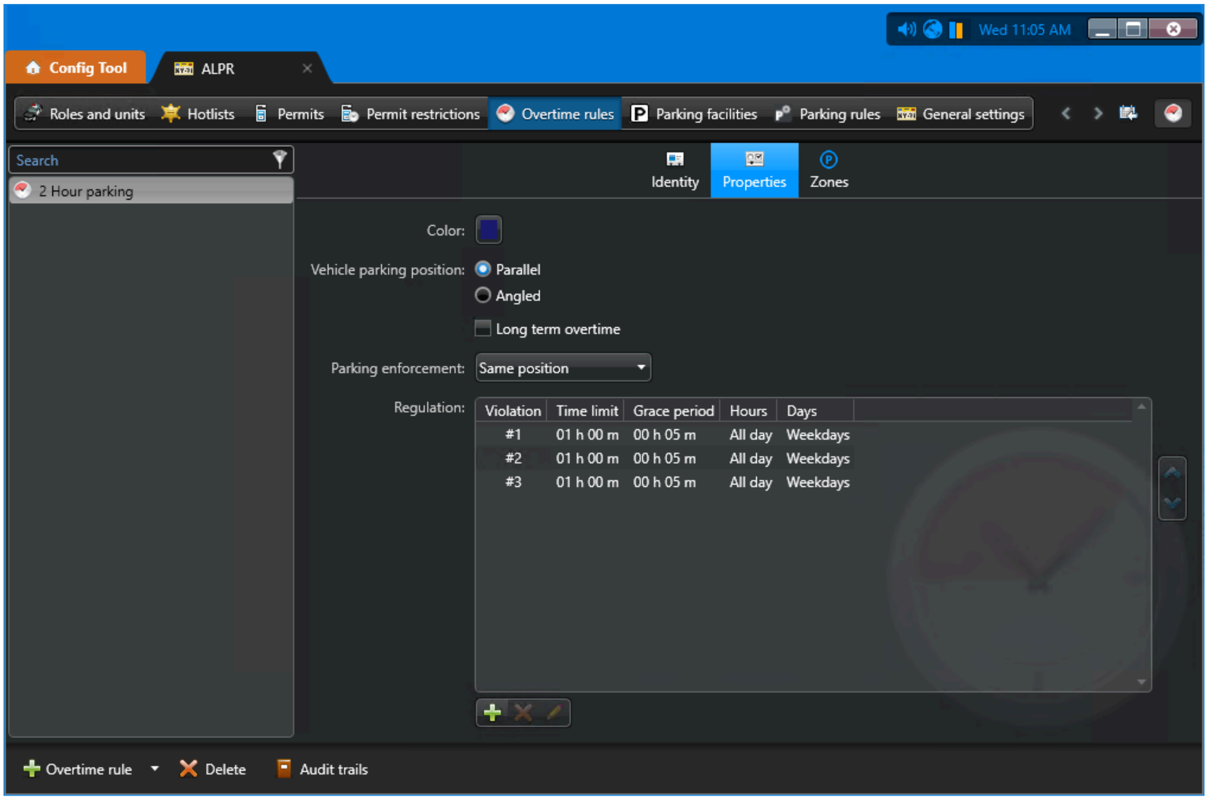
- **Time limit:** The parking time limit in hours and minutes.
- **Grace period:** For purposes of lenient enforcement, the grace period is time beyond the parking time limit during which the overtime violation is waived. For example, Patroller will generate an overtime hit on a plate when the time between the capture of the same plate exceeds the **Time limit** plus the **Grace period**.
- **Applicable days:** Days of the week when the time limit is enforced. You can select a weekly time frame from the drop-down list:
  - **Always:** 7 days a week
  - **Weekdays:** Monday to Friday
  - **Custom:** To create a custom time frame, click on the days.
- **Applicable hours:** Select when the time limit is enforced:
  - **All day:** 24 hours a day
  - **Time range:** Click in the date picker field, and use the text field or the graphical clock to specify the time.

10 (Optional) To set the maximum number of citations that can be issued to the same vehicle for the same overtime offense, add additional regulations. In the following example, a vehicle can be issued three violations of the one-hour overtime rule in one day:

Here are two examples to explain the difference between having an overtime rule with one violation, and an overtime rule with multiple violations:

- **Overtime rule with one violation:** Your overtime rule allows vehicles to park for one hour on a specific street. If a vehicle is parked in that area longer than an hour, it is in violation of the overtime rule. This results in an overtime hit in Patroller. However, because the overtime rule allows only one violation for the offense, even if the vehicle is parked in the same place all day, you'll only get one overtime hit for it. In this scenario, you would issue one ticket for the offense.
- **Overtime rule with multiple violations:** Your overtime rule allows vehicles to park for one hour on a specific street, but your system is configured to allow a vehicle to accumulate, for example, up to three violations of the one-hour rule. If a vehicle is parked in that area all day, and you patrol the area three

times during your shift, you'll get three violations of the overtime rule, and three separate overtime hits in Patroller. In this scenario, you would issue three tickets for the same offense.



Color: 🟦

Vehicle parking position: ● Parallel ○ Angled

□ Long term overtime

Parking enforcement: Same position

Regulation:

Violation	Time limit	Grace period	Hours	Days
#1	01 h 00 m	00 h 05 m	All day	Weekdays
#2	01 h 00 m	00 h 05 m	All day	Weekdays
#3	01 h 00 m	00 h 05 m	All day	Weekdays

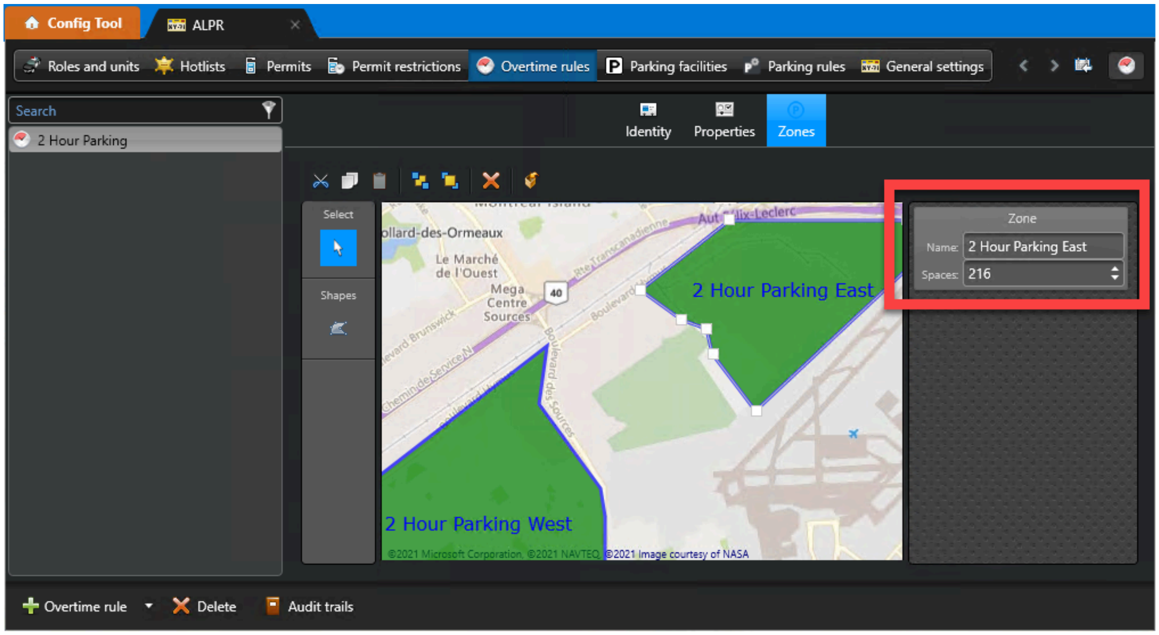
TIP: Notice that in this example, the three regulations are valid on weekdays only. This ensures that if the Patroller operator mistakenly select this overtime zone on the weekend, no citations will be issued

11 Click the **Zones** tab.

12 Click **Shapes** (![icon]) and draw one or more polygons to define the zone boundaries.

Click once for each endpoint, and click the first endpoint to close the polygon.

13 Double click each polygon and enter the **Name** and number of **Spaces** in the zone.



Zone

Name: 2 Hour Parking East

Spaces: 216

14 Click **Apply**.

The overtime rule is configured, and is downloaded to Patroller the next time it connects to Security Center.

About permits

A permit is an entity that defines a single parking permit holder. Each permit holder is characterized by a category (permit zone), a license plate number, a license issuing state, and optionally, a permit validity range (effective date and expiry date). Permits are used in both city and university parking enforcement.

The permit entity belongs to a family of methods used by AutoVu™ to identify vehicles of interest, called hit rules. Other types of hit rules include *hotlist*, *overtime*, and *permit restriction*. When a plate read matches a hit rule, it is called a *hit*. When a read fails to match any permit loaded in the Genetec Patroller™, it generates a *permit hit*.

Permits in City Parking Enforcement

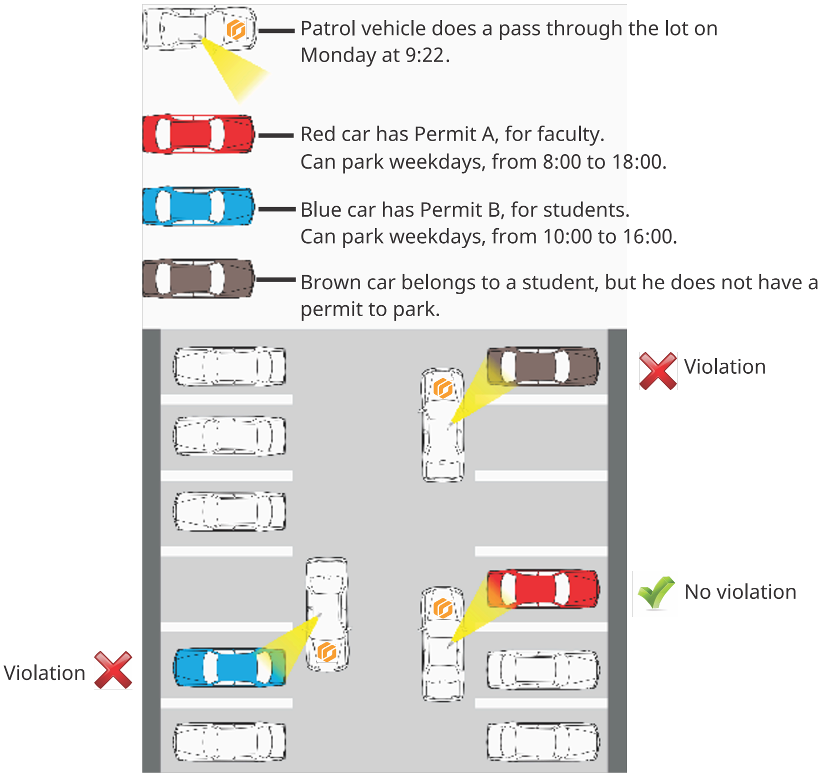
In City Parking Enforcement, you create the permit list and configure its basic properties, but you do not need to define a parking lot or permit restriction. It is the city or municipality that decides when and where the permit is applicable. The patrol vehicle operator chooses which permit to enforce in Patroller based on the parking rule signs displays on the street.

Permits in University Parking Enforcement

In University Parking Enforcement, you create and configure a permit list the same way you would in City Parking Enforcement, but you also need to assign *permit restrictions* and parking lots to create an enforcement "zone" that is downloaded to Patroller. This additional configuration is needed because the patrol vehicle is monitoring individual parking lots, not city streets with specific regulations already in place.

Example

In this example, you use a permit restriction to specify different time limits for different permit holders.


Patrol vehicle does a pass through the lot on Monday at 9:22.
Red car has Permit A, for faculty. Can park weekdays, from 8:00 to 18:00.
Blue car has Permit B, for students. Can park weekdays, from 10:00 to 16:00.
Brown car belongs to a student, but he does not have a permit to park.
Violation
No violation
Violation

Shared permits

A permit list includes a field called *Permit ID*, which allows different vehicles to share the same permit by having the same *Permit ID* value in the permit list's source file. For example, a car pool permit could be shared between several vehicles. Each member of the car pool takes a turn driving the other members to work or school, therefore each member needs to share the same permit to park.

However, the permit still applies to *one vehicle at a time*. For example, if all four members of the car pool decide to take their own vehicles one day, they can't all use that car pool permit to park at the same time. Patroller allows one vehicle with the car pool permit to park (the first license plate detected), but will raise a *Shared permit* hit for every other vehicle seen with the same permit.

NOTE: For information on how shared permits work in AutoVu™ Free-Flow installations, see About shared permits in Free-Flow on page 1094.

Related Topics

About permit restrictions on page 1142

Creating parking permits

To use permit entities in Security Center, you must create the permit, map it to its source text file, and configure it for your enforcement scenario.

What you should know

If you are using University Parking Enforcement, you must also apply restrictions to permits to create an enforcement rule.

To create a permit:

1 From the Config Tool home page, click **ALPR** > **Permits** and then click **Permit** (➕).

The **Creating a permit** wizard opens.

2 On the *Basic information* page, in the **Entity name** field, type a name for the permit.

This name appears in Genetec Patroller™ on the permit selection page.

IMPORTANT: The permit entity name must match the **Category** field from the permit list source file.

3 (Optional) In the **Entity description** field, enter a description for the new permit, and click **Next**.

This field does not appear in Patroller.

4 Enter the **Path** on the computer where the source file for the permit list is located.

If you start typing a path to a network drive, the **Username** and **Password** fields appear and you'll need to type the username and password to access the network drive.

5 If the attribute fields in the source text file vary in length, switch the **Use delimiters** option to **ON**, and enter the type of character (delimiter) used to separate each field.

By default, **Use delimiters** is set to **ON**, and the delimiter specified is a **semi-colon** (;). If your source text file is made up of fixed length fields, set **Use delimiters** to **Off** . Security Center supports the following delimiters:

- Colon (:)
- Comma (,)
- Semi-colon (;)
- Tab (type “Tab”)

IMPORTANT: If your source list file uses Tab as a delimiter, only use one Tab space. Do not use more than one Tab space to align columns in your file, or Security Center might not be able to parse the permit list.

NOTE: The maximum number of entries is 1.8 million when using Patroller in 64-bit mode. Adding more entries causes the system to respond slowly.

6 (Optional) If you don't want users to be allowed to edit this permit in Security Desk, turn off **Visible in editor**.

NOTE: To edit a permit in Security Desk, users must have the *Hotlist and permit editor* privilege.

7 Configure the permit **Attributes** and click **Next**. See Configuring hotlist and permit attributes on page 1007.

8 On the *ALPR Manager assignment* page, choose one of the following, then click **Next**.

   - **All ALPR Managers**. All ALPR Managers and any entities configured to inherit permits from them will synchronize the new permit.

     NOTE: Future ALPR Managers will not automatically synchronize the new permit.

   - **Specific ALPR Managers**. Only the selected ALPR Managers and the entities that inherit permits from them will synchronize the new permit.

     NOTE: Entities created in the future that are configured to inherit permits from one of the selected ALPR Managers will also synchronize the permit.

   - **Assign later**. No existing ALPR Managers and associated entities will synchronize the new permit. For more information on how to assign a permit to an ALPR Manager, see Selecting which hotlists and permits a patrol vehicle monitors on page 990.

9 On the *Unit specific assignment* page, select the specific patrol vehicles and/or Sharp cameras that will synchronize the new permit, and click **Next**.

10 (Optional) If you have custom fields in your permit, enter the appropriate values on the *Custom fields* page and click **Next**.

   NOTE: The *Custom fields* page only appears if there are custom fields in your hotlist.

11 In the *Creation summary* window, check to see that your permit information is correct and click **Next**.

12 In the *Entity creation outcome* window, you will receive a notification whether or not your operation is successful.

13 (Optional) Choose one of the following:

   - **Edit this permit**. Opens the **Hotlist and permit editor** task so you can edit the permit.

     NOTE: To edit a permit, you must have the *Hotlist and permit editor* privilege.

   - **Create a permit based on this permit**: Create a new permit that uses the same settings as the permit you just created. You only need to specify the **Entity name**, **Entity description**, and **Permit path**.

14 Click **Close**.

The permit entity is configured and enabled in Security Center.

Configuring parking permits

After you create a parking permit in Security Center, you can configure its settings.

Before you begin

Create the permit.

What you should know

The source text file must be located on the ALPR Manager computer's local drive (for example, the C drive), or on a network drive that is accessible from the computer hosting the ALPR Manager.

To configure a permit:

1 From the Config Tool home page, click **ALPR** > **Permits**, and select the permit you want to configure.

2 In the **Identity** tab, enter a **Description** for the permit, and click **Apply**.

You can add a longer description for the permit. This field does not appear in Genetec Patroller™.

3 In the **Properties** tab, enter the **Path** on the computer where the permit list's source text file is located.

If you start typing a path to a network drive, the **Username** and **Password** fields appear and you'll need to type the username and password to access the network drive.

NOTE: The Windows credentials you enter must have read/write access to the hotlist file.

4 If the attribute fields in the source text file vary in length, switch the **Use delimiters** option to **ON**, and enter the type of character (delimiter) used to separate each field.

By default, **Use delimiters** is set to **ON**, and the delimiter specified is a **semi-colon** (;). If your source text file is made up of fixed length fields, set **Use delimiters** to **Off** . Security Center supports the following delimiters:

- Colon (:)
- Comma (,)
- Semi-colon (;)
- Tab (type "Tab")

IMPORTANT: If your source list file uses Tab as a delimiter, only use one Tab space. Do not use more than one Tab space to align columns in your file, or Security Center might not be able to parse the permit list.

5 Decide whether users are allowed to edit this permit in Security Desk.

6 Configure the **Attributes** for the permit list's text file so that Patroller can parse the information in the list.

7 Click **Apply**.

About permit restrictions

A permit restriction is an entity that applies time restrictions to a series of parking permits for a given parking area. Permit restrictions can be used by patrol vehicles configured for University Parking Enforcement and for systems that use the AutoVu™ Free-Flow feature.

Different time restrictions can be applied to different *permits*. For example, a permit restriction may limit the parking in zone A from Monday to Wednesday for permit P1 holders, and from Thursday to Sunday for permit P2 holders.

The permit restriction entity is a type of hit rule. A hit rule is a method used by AutoVu™ to identify vehicles of interest. Other types of hit rules include *hotlist, overtime*, and *permit*. When a plate read matches a hit rule, it is called a *hit*. When a plate read matches a permit restriction, it generates a *permit hit*. Additionally, a *shared permit hit* occurs when two plates sharing the same permit ID are read in the same parking area within a specific time period.

Related Topics

About permits on page 1137

Creating permit restrictions

You can add a permit restriction entity in Security Center Config Tool to apply restrictions to a permit. After you create the entity, you'll configure its settings for your enforcement scenario.

Before you begin

Create the permit and configure the permit.

What you should know

- In University Parking Enforcement, to create an enforcement rule, you need to apply restrictions to the permits you add. Genetec Patroller™ downloads permit restrictions when it connects to Security Center.
- Ideally, a permit restriction should only contain the permits that are relevant to the restriction, that is, it is best practice not to add all of your permits to every permit restriction.

  NOTE: There is no limit to the number of permits that can be added to a permit restriction, but if you put all the permits in all permits restriction, you might notice a delay before the Patroller hit pop-up is displayed. In this case, you can configure the system to only search permits from the zone currently being scanned by the patrol vehicle. For more information, see [KBA-79138] Patroller hit detection delay in University mode.
- You can apply permit restrictions to AutoVu™ Free-Flow parking rules.

To create a permit restriction:

1. From the Config Tool home page, click **ALPR** > **Permits restrictions**, and then click **Permit restriction** (✚).

   A new permit restriction entity is added in the list of all the permit restrictions on your system.
2. In the **Identity** tab, enter the required information:
   - **Name:** In City Parking Enforcement, this name appears in Genetec Patroller™ on the overtime rule selection page. In University Parking Enforcement, this name appears appended to the parking lot name on the zone selection page.

     TIP: Choose a name that describes the details of the enforcement scenario. This makes it easier to select it in Patroller when you have more than one available.
   - **(Optional) Description:** You can add a longer description for the rule. This field does not appear in Patroller.
   - **(Optional) Logical ID:** Enter a Logical ID if applicable.
3. Click **Apply**.

After you finish

Configure the permit restrictions.

Configuring permit restrictions

After you have created a permit restriction entity in Security Center Config Tool, you need to configure it for your enforcement scenario.

Before you begin

Create the permit restriction.

What you should know

You must configure an enforcement area (or parking lot) for each permit restriction and overtime rule that you create.

To configure a permit restriction:

1 From the Config Tool home page, click **ALPR** > **Permit restrictions**.

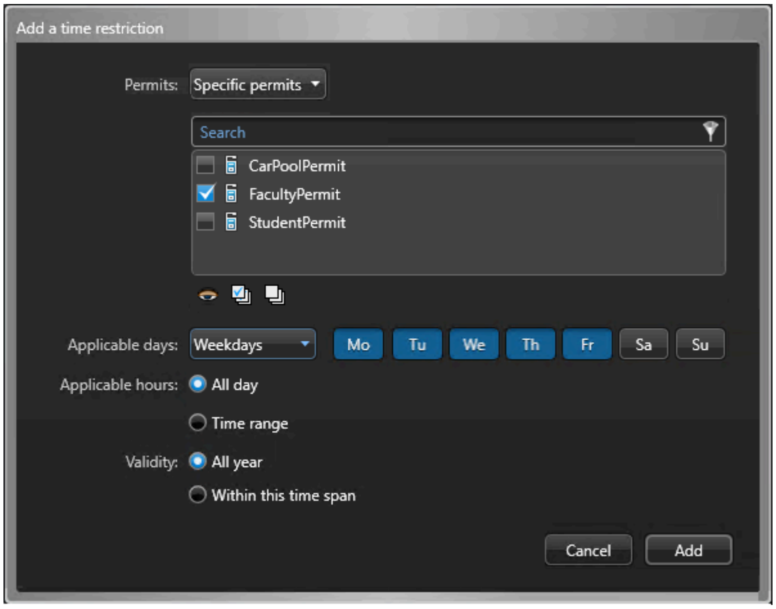
2 Select the permit restriction you want to configure, then click the **Properties** tab.

3 To assign a color to the permit restriction, click the **Color** icon, select a color, and click **OK**.

The color is displayed in the permit hit screen in Genetec Patroller™ and Security Desk, as well as the plate reads due for enforcement on the Patroller map.

4 To select when this restriction applies, click **Add an item** (✚).

The **Add a time restriction** window opens.



Add a time restriction

Permits: Specific permits

Search

☐ CarPoolPermit
☑ FacultyPermit
☐ StudentPermit

Applicable days: Weekdays — Mo Tu We Th Fr Sa Su

Applicable hours: ● All day ○ Time range

Validity: ● All year ○ Within this time span

5 From **Permits** list, select which permits the restriction applies to:

- **Everyone:** Parking is available to everyone, regardless of whether they have a permit or not. No restriction is enforced during the specified time period. This restriction is used with other restrictions as a temporary override. For example, if a university is hosting a football game, parking would be made available to everyone during the game instead of specific permit holders.

- **No permit:** Only vehicles without permits can park. For example, you can use this type of restriction to reserve a zone for visitors parking. A plate read that matches any of the permits downloaded to the Patroller raises a hit.
- **All permits:** Only vehicles with a permit can park. A plate read that does not match any of the permits downloaded to the Patroller raises a hit.
- **Specific permits:** Only vehicles having one or more of the specified permits can park. A plate read that does not match any of the specified permits raises a hit.

When multiple time restrictions apply at a given time, conflicts are resolved by evaluating the restrictions in the following order: 1. *Everyone*, 2. *No permit*, 3. *All permits*, 4. *Specific permits*. Moreover, a hit is raised when a matched permit is not valid (either not yet effective or already expired).

6 In the **Applicable days** option, select the days of week when parking is allowed.

- **Always:** Seven days a week.
- **Weekly:** Monday to Friday.
- **Weekend:** Saturday and Sunday.
- **Custom:** Select the days that apply.

7 In the **Applicable hours** option, select the times during the day when parking is allowed.

8 In the **Validity** option, select the dates during the year when parking is allowed.

Choose **All year**, or select a specific time span using the date picker.

NOTE: The date span must be longer than one day.

9 Click **Add** and then click **Apply**.

The permit restriction entity is configured and enabled in Security Center.

After you finish

Configure a parking lot in Security Center for the permit restriction.

Configuring parking lots in Security Center

You must configure an enforcement area (or parking lot) for each permit restriction and overtime rule that you create.

What you should know

- When you have a enforcement rule and a parking lot defined, this makes up the *parking area* that is displayed in Genetec Patroller™. You create parking lots in Security Center Config Tool by drawing a polygon around the parking lot's geographical location on the map. You can add multiple parking lots to a map.
- You can also import *KML files* to your map that have been created in another map application such as Google Earth.

To configure a parking lot in Security Center:

1 From the Config Tool home page, click **ALPR** > **Permits**, **Permit restrictions**, or **Overtime rules**.

2 Select the permit, permit restriction, or overtime rule you want to configure, then click **Zones**.

The map appears.

3 Zoom in to the area of the map where your parking lot is located.

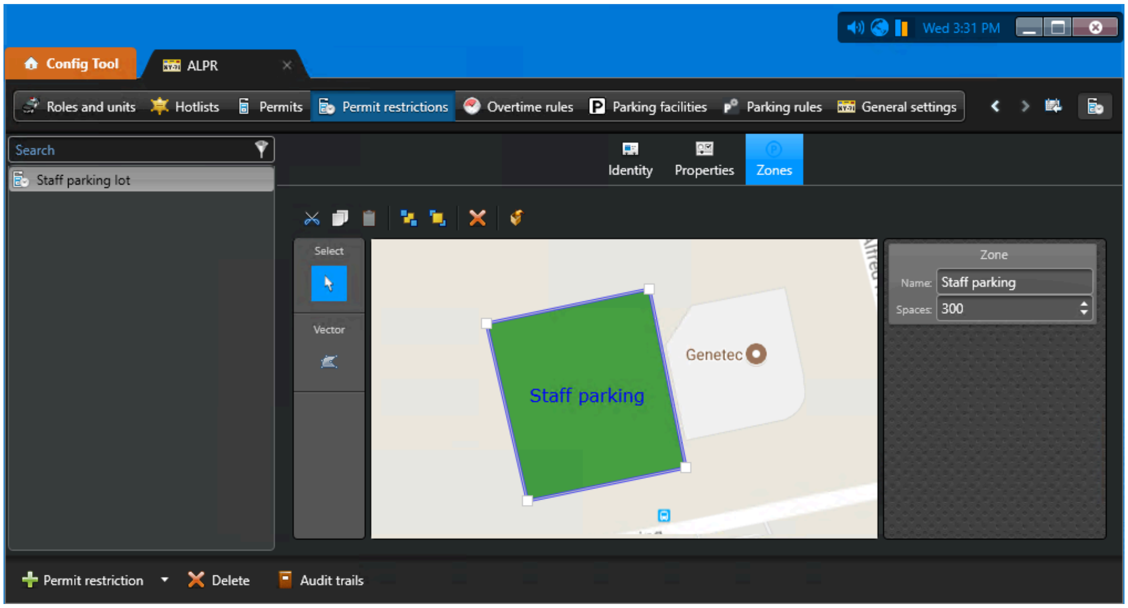
4 Click the **Vector** button, and place the cursor on the map.
The cursor changes to crosshairs.

5 On the map, click on each corner of the parking lot to create the polygon (click on the starting point to finish drawing).
A parking lot appears with the name **New zone 1**.

6 Click the **New zone 1** parking lot, and in the dialog that appears enter a new **Name** and the number of **Spaces** in the parking lot.

This name will appear in Patroller along with the *Permit*, *Overtime rule* or *Parking restriction* name, to display an enforcement zone.

TIP: Choose a name that describes where the parking lot is. This makes it easier to select the enforcement zone in Patroller when multiple zones are available.



Name: Staff parking
Spaces: 300

7 Click **Apply**.

The parking lot appears as a filled polygon with a thick blue border on the map. The name of the parking lot is displayed in the center.

8 (Optional) To resize a parking lot, select it in the map and use the handles to drag it to the desired size.

TIP: To select a parking lot, you can click directly on the parking lot, or click the Select button and then select the lot.

9 (Optional) To edit a parking lot, select the lot and use the buttons located at the top left of the map:

- **Cut :** Cut the selected parking lot from the current entity and paste it into another. For example, you may want to cut the parking lot from a permit entity and paste it into the map when creating a parking lot for an overtime rule.
- **Copy :** Copy the selected parking lot from the current entity and paste it into another. For example, you may want to use the same parking lot dimensions that were created for a permit parking lot in an overtime rule parking lot.
- **Paste :** Paste the selected parking lot into another entity.
- **Send to Back :** Send the selected parking lot to the background.
- **Bring to Front :** Send the selected parking lot to the background.
- **Remove :** Delete the parking lot.

Related Topics

Adding and configuring parking zones on page 1086

Importing KML files in Security Center

The **Zones** tab in Config Tool enables you to import Keyhole Markup Language (KML) files so you can easily create parking lots in Security Center.

Before you begin

Create a KML file for your map. This can be done using Google Earth or ArcGIS.

What you should know

- If the KML file you want to import is not supported or not valid, you will receive an error message.
- If you want update a KML lot in Security Center by reimporting an updated KML file, delete the original KML lot first so you don't get a duplicate.

To import a KML file:

1 From the Config Tool home page, click **ALPR** > **Permits**, **Permit restrictions**, or **Overtime rules**.

2 Select the permit, permit restriction, or overtime rule you want to configure, then click **Zones**.

The map appears.

3 Click **Import KML** ( ) and navigate to the folder that contains your KML file.

4 Select the KML file and click **Open**.

The parking lot appears in your map as a filled polygon with a thick blue border on the map. The name of the parking lot is written in the center.

5 Select the parking lot in the map. In the dialog box that appears, enter the number of **Spaces** the parking lot contains.

6 Click **Apply**.

Configuring advanced permit settings

The **Advanced** tab is where you configure the advanced properties of the permit such as the color and download frequency. These properties are not required for all permits, but allow you to customize certain permits for specific scenarios.

Before you begin

Create the permit.

To configure advanced permit settings:

1 From the Config Tool home page, click **ALPR** > **Permits**, and select the permit you want to configure.

2 Click the **Advanced** tab.

3 Beside **Color**, click the colored block and use the *Select color* dialog box to assign a new color to the permit.

The map symbol that marks the location of the permit hit in Security Desk and Genetec Patroller™ will appear in that color, as well as the Permit Hit and *Review Hits* screen in Patroller.

4 Turn on **Disable periodic transfer** if you only want permit changes to be downloaded to Patroller when the user logs on to the application. This option requires a wireless connection between Patroller and Security Center.

5 Turn on **Enable transfer modification** if you want to transfer permit modifications to Patroller as soon as they occur. For example, you can use this option on a permit to force Patroller to query for changes more frequently than the periodic transfer period (which applies to all permits). This option requires a continuous wireless connection between Patroller and Security Center.

6 Click **Apply**.

51

AutoVu Mobile License Plate Inventory systems

This section includes the following topics:

Mobile License Plate Inventory

Mobile License Plate Inventory (MLPI) is the Genetec Patroller™ software installation that is configured for collecting license plates and other vehicle information for creating and maintaining a license plate inventory for a large parking area or parking garage.

The inventory can be used to report the following:

- The number of days a vehicle has been parked in the facility.
- The location (sector and row) of the vehicle in the facility.
- All vehicles parked in the facility.
- All vehicles that have left or entered the facility.

License plate reads can be collected in three ways:

- Automatic reading using the Genetec Patroller™ application and a Sharp camera (or cameras).
- Manual entry using the *Manual capture* feature of the Patroller application.
- (Optional) Manual capture using the handheld computer approved by Genetec Inc. that is running the Patroller MLPI application.

License plate inventory

The license plate inventory includes license plate reads of all vehicles parked in the parking facility. It is created from the license plate collection offload data from Patroller and the handheld computer approved by Genetec Inc. (if applicable). The inventory can be used to monitor vehicle activity of the parking facility for a specific time period. For example, a patrol vehicle might collect license plate reads early in the morning and then do another collection in the evening to see how many vehicles have left the facility. The Security Desk *Inventory management* task is used to create the inventory from the offload data, and the Security Desk *Inventory Report* task is used to query any changes to an inventory.

For more information, see the *Inventory management* and *Inventory report* topics in the *Security Center User Guide*.

How reads are reconciled

Most reads from the offload data of a license plate collection are automatically reconciled (validated and added) to the license plate inventory by Security Center. However, some of them may require manual reconciliation if a conflict is detected. For example, a vehicle may have the same license plate numbers as another vehicle, but be from a different state. If this is the case, the Security Desk *Inventory Management* task will display a dialog box asking you to reconcile the read (confirm the plate number and state of the vehicle).

For more information on the *Inventory Management* task, see the *Security Center User Guide*.

About parking facilities

A parking facility entity defines a large parking area as a number of sectors and rows for the purpose of inventory tracking. It is used in the AutoVu™ *Mobile License Plate Inventory* (MLPI) application.

The license plate inventory is the list of vehicles present in a parking facility within a given time period.

Before AutoVu MLPI units (patrol vehicles and handheld devices) can collect license plates for the inventory, you must define their collection route as a sequence of sectors and rows configured in the parking facility. The sector and row where a license plate is read represents the location of the vehicle inside the parking facility.

Security Center collects *license plate reads* from the MLPI units and creates an inventory for the current date. Using Security Desk, you can find where a vehicle is parked (sector and row) and how long it has been parked there in the current inventory. You can also compare two inventories on different dates to view the vehicle movements (vehicles that were arrived, moved, or left).

Creating parking facilities

To track the location of vehicles in an AutoVu™ Mobile License Plate Inventory system, you must create a parking facility.

To create a parking facility:

1. From the Config Tool home page, click **ALPR** > **Parking facilities** and then click **Parking facility** (➕).
2. In the **Identity** tab, enter the required information:
   - **Name:** In Mobile License Plate Inventory, this name will appear in Genetec Patroller™ on the parking zone selection page.
   - **(Optional) Description:** You can add a longer description for the rule. This field does not appear in Patroller.
   - **(Optional) Logical ID:** Enter a Logical ID if applicable.
3. Click **Apply**.

The parking facility appears in a flat list view that displays all the facilities on your system.

After you finish

Define the parking facility for your parking scneario by creating sectors and rows.

Configuring parking facilities

After you have created a parking facility in Security Center, you must define the facility for your parking scenario by creating sectors and rows for the license plate collection route.

Before you begin

Create the parking facility.

What you should know

The parking space of a parking facility is divided into sectors (or levels in the case of a parking garage) for ease of reference. Each sector contains x number of rows, and each row contains x number of spaces. You can configure Genetec Patroller™ to trigger an alarm (sound or warning message) if the reads collected during your sweep of a row exceed the space count for that row.

The *route* is the license plate collection route followed by the MLPI units responsible for collecting the plates for the inventory. The route is downloaded by the patrol vehicles and handheld devices assigned to this parking facility.

NOTE: Only one route may be defined per parking facility, but each MLPI device can start its sweeping round at a different point in the route. The route forms a closed circuit.

To configure a parking facility:

1 From the Config Tool home page, click **ALPR** > **Parking facilities**, and select the facility you want to configure.

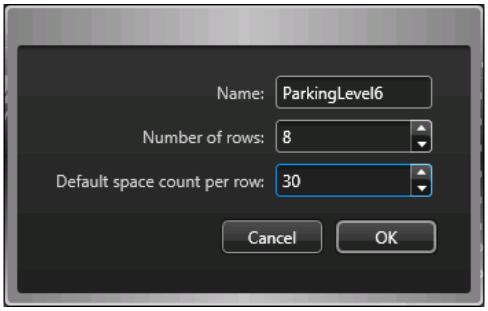
2 Click the **Properties** tab.

3 From the **ALPR Manager** list, select the ALPR Manager that will create and manage the license plate inventory for the selected parking facility.

Only offloads from MLPI patrol vehicles managed by the same ALPR Manager are used to build the inventory for this parking facility. An MLPI Patroller offload can include the vehicle inventory for multiple parking facilities, but only the reads tagged for this parking facility are used to build the inventory.

4 Under **Configuration**, click **Create** (+) to add a new sector.

The parking space of a parking facility is divided into sectors (or levels in the case of a parking garage) for ease of reference. Each sector contains x number of rows.



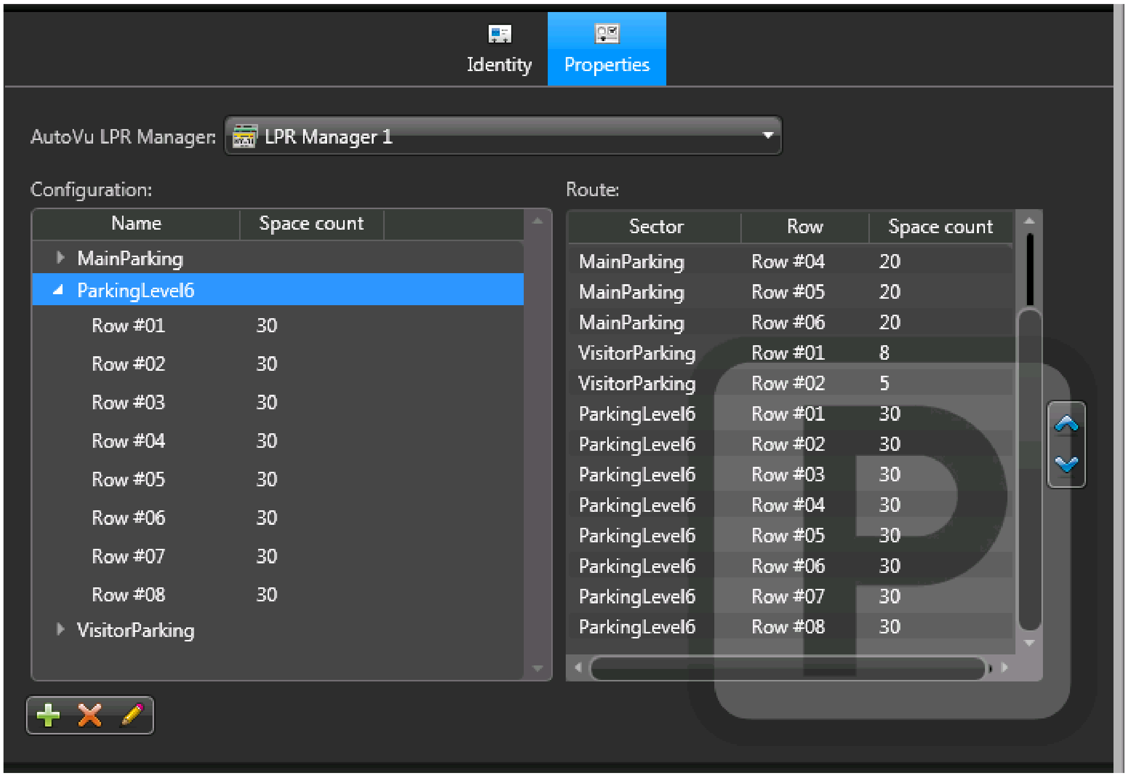
Name: ParkingLevel6
Number of rows: 8
Default space count per row: 30

5 Enter the **Name** of the sector, or level if you have a parking garage.

6 Enter the **Number of rows** in the sector.

7 Click **OK**.

The sector you created appears under the **Configuration** and **Route** sections.



AutoVu LPR Manager: LPR Manager 1

Configuration:

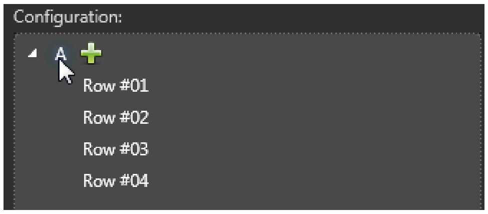
Name	Space count
MainParking	
ParkingLevel6	
Row #01	30
Row #02	30
Row #03	30
Row #04	30
Row #05	30
Row #06	30
Row #07	30
Row #08	30
VisitorParking	

Route:

Sector	Row	Space count
MainParking	Row #04	20
MainParking	Row #05	20
MainParking	Row #06	20
VisitorParking	Row #01	8
VisitorParking	Row #02	5
ParkingLevel6	Row #01	30
ParkingLevel6	Row #02	30
ParkingLevel6	Row #03	30
ParkingLevel6	Row #04	30
ParkingLevel6	Row #05	30
ParkingLevel6	Row #06	30
ParkingLevel6	Row #07	30
ParkingLevel6	Row #08	30

8 To add rows to a sector, do the following:

a) Under **Configuration**, mouseover the sector name, and then click the **Create** (➕).



Configuration:

A ➕
Row #01
Row #02
Row #03
Row #04

b) Enter the **Number of rows** to add, and then click **OK** > **Apply**.

9 (Optional) To rename a sector, do the following:

a) Under **Configuration**, click the sector name you want to rename, and then click **Edit** (✎).

b) Enter the new name, and then click **OK** > **Apply**.

10 (Optional) To delete a sector, click the sector name you want to delete under **Configuration**, and then click **Delete** (✖) > **Apply**.

11 To change the order of sectors and rows in the route, click the up (▲) and down (▼) arrows under **Route**.

After you finish

You must set the *Read retention period* of the ALPR Manager according to the period of time you want to keep your license plate inventories in the database. The default retention period is 90 days.

52

Federated reads matching

This section includes the following topics:

About federated reads matching

Federated reads matching is a feature that allows the live matching of license plate reads from federated sites against hotlists available on the Federation™ host. This feature makes it unnecessary to share hotlists with federated sites to raise hits.

The ALPR Manager role uses hotlists to raise hits against license plate reads by the ALPR units to identify vehicles of interest. These hotlists must be created and maintained locally in every Security Center installation. In a system without the federated read matching configured, if the Federation™ host needs to raise a hit against its hotlist, it would need to share its hotlist with every federated site.

Instead of having to share the hotlists between host and sites, the Federation™ host can configure the federated reads matching feature on every ALPR Manager role that has the matching property activated. With the federated reads matching feature, the ALPR Manager role on the Federation™ host can receive reads from federated sites and raise hits against hotlists defined on the Federation™ host in real-time.

Example

The state police department (PD) has implemented a Federation™ system that includes all the city police departments and local Sheriff's offices of that state. The state PD and local PDs have their own hotlists.

The state PD wants to keep its hotlists confidential, but also raise hits from federated sites. By enabling the federated reads matching feature, the state PD can assign a unique ALPR Manager role on the Federation™ host to receive reads from the corresponding federated entities. Every time a license plate is read by the federated site, it matches against both the Federation™ site and host hotlists, and raises hits accordingly.

Limitations of federated reads matching

The federated reads matching feature applies only for real-time reads.

The federated reads matching feature does not raise hits for the following:

- Stored reads, such as reads from a XML import module of a federated site
- Patroller offloads
- Reads over 5 minutes old on the federated site that are not sent to the Federation™ host

The *Source* column in a report displays only the federated site from where the read was received, and not the ALPR Manager role on the Federation™ host that raised the hit. To identify the role on the Federation™ host that raised the hit, you must include the role details in the hotlist name. For example, a hotlist named *Hotlist A* associated to a role running on the Federation™ host named *ALPR Manager 1* could be named to *Hotlist A on ALPR Manager 1*.

In the following scenarios, low-resolution images are displayed in the reports:

- The corresponding read or hit has been deleted at the federated site.
- The federated site is not accessible.

Outcomes in Read reports for federated read matching

The following scenarios lists all the possible outcomes in Read reports when the federated read matching feature is activated.

When you configure the federated reads matching feature on the Federation™ host, the Reads and Hits reports can display multiple outputs for a single incoming read. The following use cases demonstrate the different outputs that can be displayed in the reports:

When all entities are online

The number of reads or hits generated depends on which hotlists the incoming read raises a hit against. The following table summarizes how the reports displays the outcomes:

If the incoming plate read is a hit against	Reports display
• Federation™ host hotlist	• One read from the federated site • One hit from the Federation™ host
• Federation™ host hotlist • Federated site hotlist	• One read from the federated site • One hit from the Federation™ host • One hit from the federated site
• No hotlist	• One read from the federated site

When the federated role is offline or has been deleted

The Reads and Hits reports display federated reads and hits that meet the following criteria:

- Detected before the federated entity went offline or was deleted.
- Received within the retention period of the Federation™ host's Security Center.

The following table shows how retention periods affect the Reads report:

Retention periods

Retention period expired on host	Retention period expired on site	Reads report displays	Hits report displays
No	No	Reads from either the Federation™ host or federated site	Hits from either the Federation™ host or federated site
No	Yes	Reads from the Federation™ host	Hits from the Federation™ host
Yes	No	Reads from the Federation™	Hits from the Federation™
Yes	Yes	None	None

Configuring federated reads matching for Federation™ systems

To raise hits against hotlists defined on the Federation™ host, you must configure the ALPR Manager role on the host so that it can connect and receive reads from the federated sites.

Before you begin

- Configure your Security Center Federation™ system as needed.
- On the federated site, make sure the following configurations are set:
  - At least one ALPR Manager role is active.
  - All the required ALPR units and Genetec Patroller™ units have been added to ALPR Manager role.

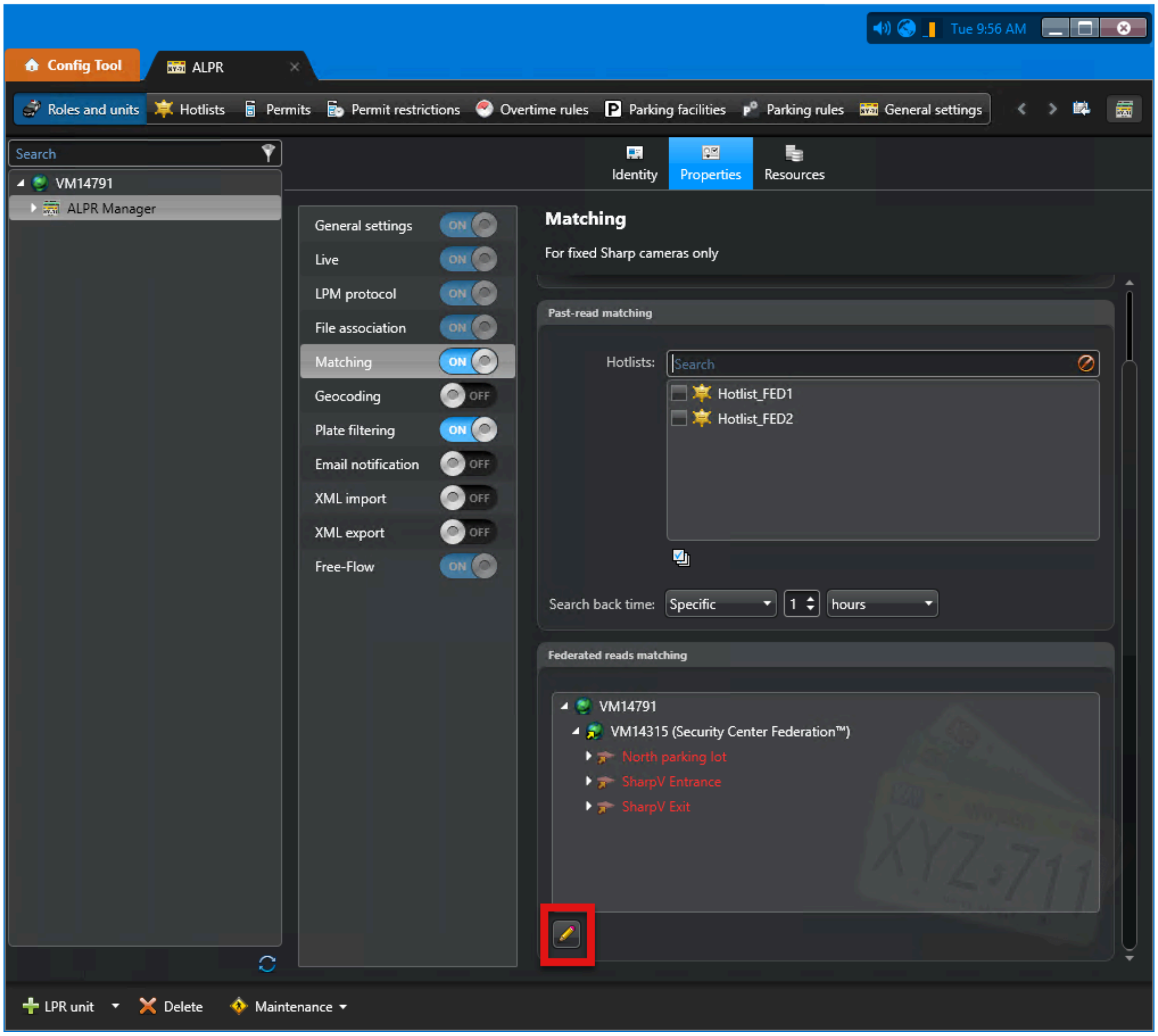
What you should know

IMPORTANT: To ensure optimal performance, configure a unique ALPR Manager role for every federated site that needs to be matched.

To configure the federated reads matching feature on the Federation™ host:

1. From the Config Tool home page, click **System** > **Roles**, and then select the ALPR Manager you want to configure.
2. Click the **Properties** tab, and then enable the **Matching** option.

3 In the *Federated reads matching* section, click ✎ to add federated ALPR or Patroller units.



General settings	ON
Live	ON
LPM protocol	ON
File association	ON
Matching	ON
Geocoding	OFF
Plate filtering	ON
Email notification	OFF
XML import	OFF
XML export	OFF
Free-Flow	ON

Matching

For fixed Sharp cameras only

Past-read matching

Hotlists: Search
□ Hotlist_FED1
□ Hotlist_FED2

Search back time: Specific 1 hours

Federated reads matching

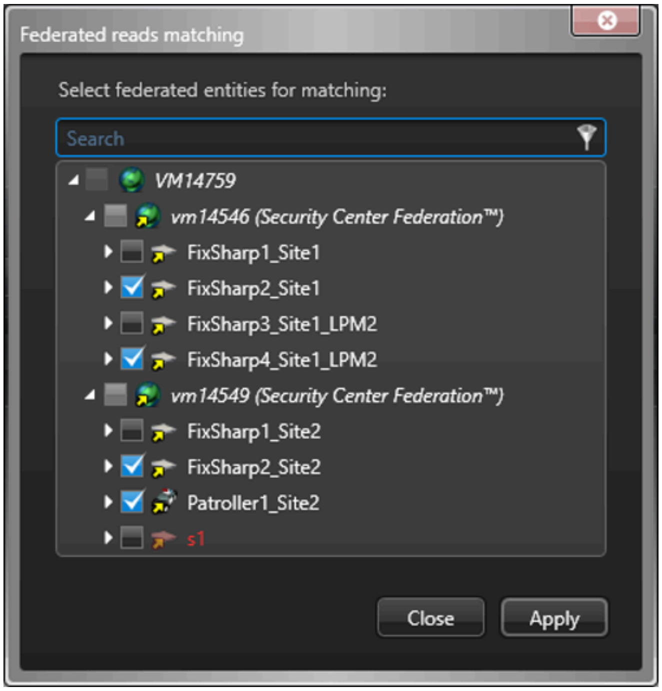
- VM14791
  - VM14315 (Security Center Federation™)
    - North parking lot
    - SharpV Entrance
    - SharpV Exit

4. In the *Federated reads matching* dialog box, select the entities for matching.

   You can select entities by doing either of the following:

   - Click a federated role.

     NOTE: This selects all the corresponding child ALPR units. Also, any future units added to this role are automatically selected.
   - Click individual ALPR and Patroller units under a federated role.



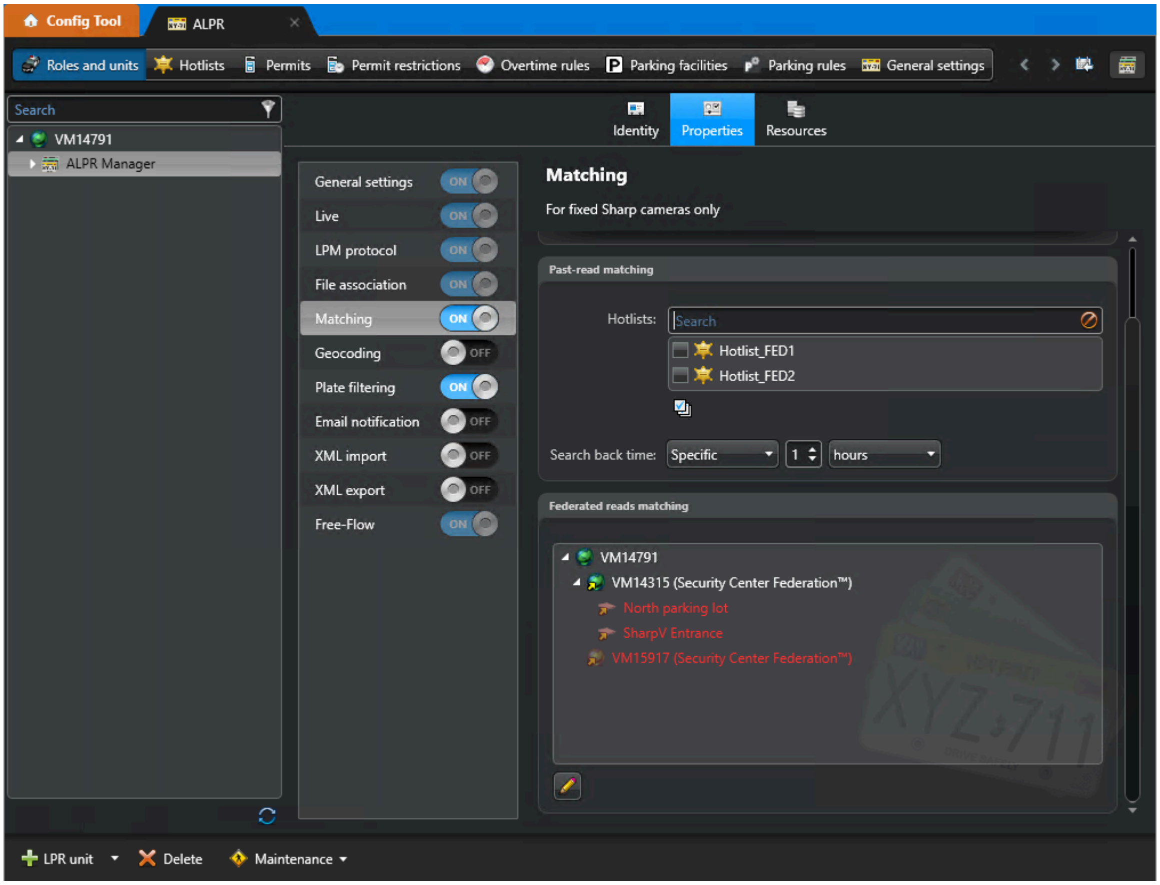
Federated reads matching

Select federated entities for matching:

- □ VM14759
  - □ vm14546 (Security Center Federation™)
    - □ FixSharp1_Site1
    - ☑ FixSharp2_Site1
    - □ FixSharp3_Site1_LPM2
    - ☑ FixSharp4_Site1_LPM2
  - □ vm14549 (Security Center Federation™)
    - □ FixSharp1_Site2
    - ☑ FixSharp2_Site2
    - ☑ Patroller1_Site2
    - □ s1

5. Click **Apply**.

6 Click **Apply** on the *Properties* page.



To turn off the federated reads matching feature:

1 In the *Federated reads matching* section, click ✏ to add federated ALPR or Patroller units.

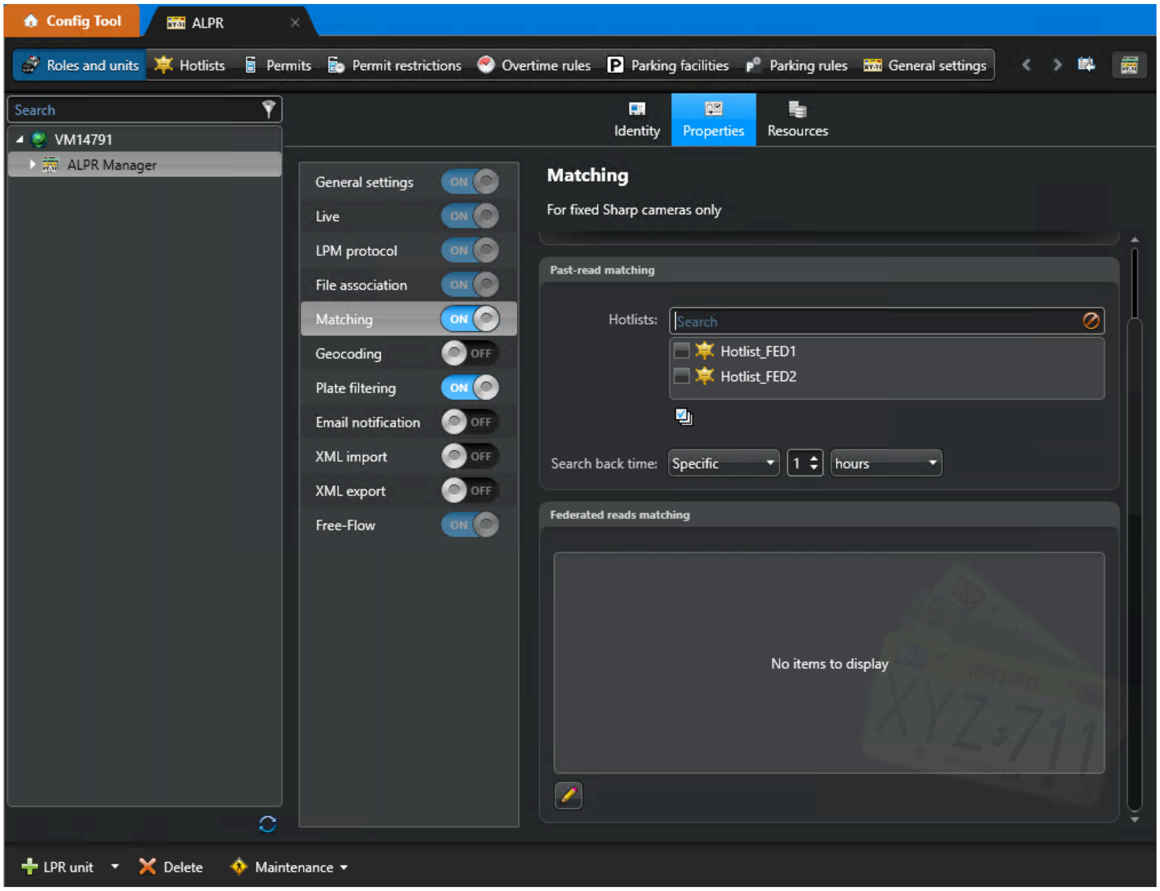
2 Click the **Properties** tab, and then turn on the **Matching** option.

3 In the *Federated reads matching* section, click ✏ to edit federated ALPR or Patroller units.

4 In the *Federated reads matching* dialog box, clear all the selected federated entities and then click **Apply**.

IMPORTANT: If the **Matching** option on the ALPR Manager role is disabled without removing the selected entities from the *Federated reads matching* section, the federated site continues to forward reads. This can negatively impact system performance.

5 Click **Apply** on the *Properties* page.



General settings ON
Live ON
LPM protocol ON
File association ON
Matching ON
Geocoding OFF
Plate filtering ON
Email notification OFF
XML import OFF
XML export OFF
Free-Flow ON

Matching

For fixed Sharp cameras only

Past-read matching

Hotlists: Search

□ Hotlist_FED1

□ Hotlist_FED2

Search back time: Specific 1 hours

Federated reads matching

No items to display

53

Troubleshooting ALPR

This section includes the following topics:

Moving Patroller or ALPR units to a different ALPR Manager

If you want a different ALPR Manager role to manage and control an ALPR or Genetec Patroller™ unit, for load balancing or another purpose, you can move the unit to another ALPR Manager using the *Move unit* tool. After the unit is moved, the old ALPR Manager continues to manage the unit data collected before the move.

What you should know

After you move a unit in Config Tool, you need to update the unit's network settings in Patroller Config Tool and in the Sharp Portal so that the unit can communicate with its new ALPR Manager. Specific unit settings (for example, unit name, logical ID, and so on) are automatically carried over to the new ALPR Manager.

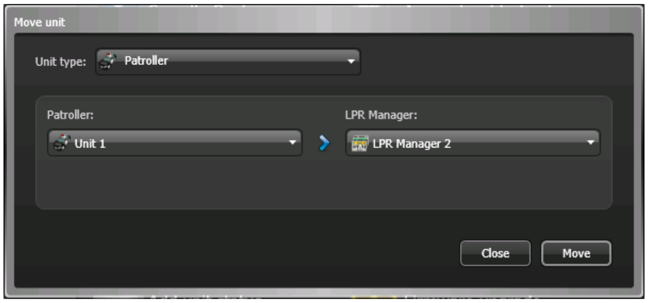
For example, if you move a Patroller unit from *ALPR Manager* to *ALPR Manager 2*, you must configure the Patroller unit to communicate with *ALPR Manager 2* the same way you did when you originally added the unit to *ALPR Manager*. This requires changing network settings in Patroller Config Tool so that they match the network settings for *ALPR Manager 2* in Security Center Config Tool.

To move an ALPR or Patroller unit to a different ALPR Manager:

1 From the Config Tool home page, click **Tools** > **Move unit**.

2 From the **Unit type** list in the *Move unit* dialog box, select the Patroller or ALPR unit you want to move.

A Patroller unit is shown as an example.



3 Select the unit you want to move.

4 From the **ALPR Manager** list, select the new ALPR Manager to control the unit.

5 Click **Move** > **Close**.

The unit is now added to the new ALPR Manager

After you finish

Make sure the unit can communicate with the new ALPR Manager, as follows:

- For hotlists, permit lists, and Patroller user groups, do the following:
  1. From the home page, click **System** > **Roles**, and then select the ALPR Manager that is now controlling the unit you moved.
  2. Click **Properties** > **File association**.
  3. Activate the hotlists and permit lists, and assign a Patroller user group for this ALPR Manager.
- Update the network settings of Patroller units to communicate with the new ALPR Manager (see the *Genetec Patroller™ Administrator Guide*).
- Update the network settings of ALPR units to communicate with the new ALPR Manager. For more information, see the *Sharp Administrator Guide*.

Troubleshooting: Federated read matches the host hotlist but does not generate a hit

If a read from a federated site matches the Federation™ host hotlist but does not raise a hit, the corresponding ALPR Manager role on the host must be investigated.

To troubleshoot why a hit is not raised when a read matches the hotlist on a Federation™ host:

1. Make sure the matching property is enabled for the corresponding ALPR Manager role on the Federation™ host.
2. Make sure the correct hotlist is linked to the ALPR Manager on the Federation™.
3. Make sure the ALPR unit that generated the read is in the *Federated reads matching* list of the corresponding ALPR Manager role on the Federation™ host.
4. Inspect the ALPR Manager database on the Federation™ host to verify that the read was saved.

Migrating ALPR images to another server

If the server hosting the ALPR images fails, or has limited disk space, you must manually transfer the ALPR images and the corresponding Archiver role to a new or more adequate server.

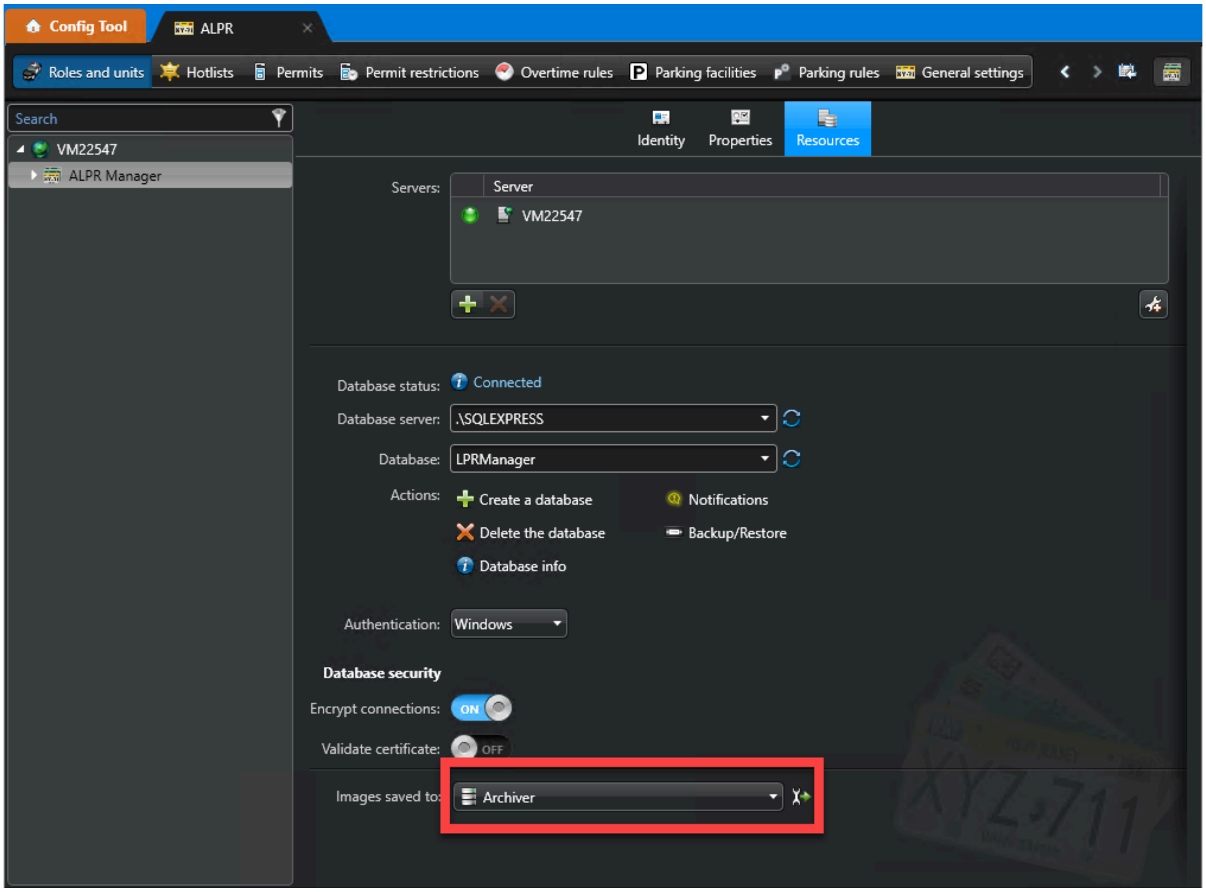
Before you begin

Make sure you have another server configured and ready to accept a new role.

What you should know

- Depending on the amount of data being re-indexed, and depending on your hardware, ALPR image migration might take several hours.
- The ALPR images are managed by an Archiver role assigned to the ALPR Manager. The images are stored as G64 files in the *VideoArchives* folder on the server. The ALPR images must be transferred manually as the Archive transfer task does not yet support the G64 files containing ALPR images.

  WARNING: If you change the Archiver entity in **ALPR Manager** > **Resources** > **Images saved to** tab without completing the following steps, you will lose all the images.



Servers: Server: VM22547

Database status: Connected

Database server: .\SQLEXPRESS

Database: LPRManager

Authentication: Windows

Encrypt connections: ON

Validate certificate: OFF

Images saved to: Archiver

To transfer the old ALPR images:

1 Back up the Archiver SQL database.

2. Deactivate the Archiver role on the old server:
   a) In the Config Tool *Video* task, select the Archiver.
   b) At the bottom of the *Video* task, click **Maintenance** > **Deactivate role** (🚦).
   c) In the confirmation dialog box, click **Continue**.

      The Archiver and all video units controlled by the role turn red.
3. Manually move the video archives from *C:\VideoArchives\Archiver* to the desired location on the new server.
4. On the new server, transfer the files to the desired location.
5. If the location of the G64 files on the new server is the same as that on the original server, restore Archiver SQL Database.
6. If the location of the G64 files on the new server is different from that of the original server, re-index these files in the Archiver database using the VideoFileAnalyzer.exe tool.
7. Activate the Archiver role on the new server:
   a) In the Config Tool *Video* task, select the Archiver.
   b) At the bottom of the *Video* task, click **Maintenance** > **Activate role** (🚦).
   c) In the confirmation dialog box, click **Continue**.
8. Click the **Resources** tab.
9. In the **Server** list, select the new server.

Upgrading SharpV unit firmware

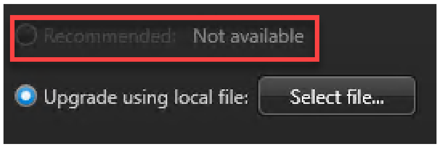
You can upgrade the firmware or perform maintenance updates to one or more fixed ALPR units directly from Config Tool.

Before you begin

Upgrading your ALPR unit requires the following:

- Config Tool is running on the same system that hosts the *ALPR manager* role.
- Your Security Center user has the *Upgrade ALPR units* privilege.
- The unit you want to upgrade has a supported upgrade path to the new version.
- The SharpV units support upgrades using Config Tool. This requires the units to have a SharpOS 13.3 or later, depending on the unit you want to upgrade.
- Download a supported firmware version for the unit from GTAP.

  NOTE: You need to manually download the firmware file only if the **Recommended** option is *not available*.

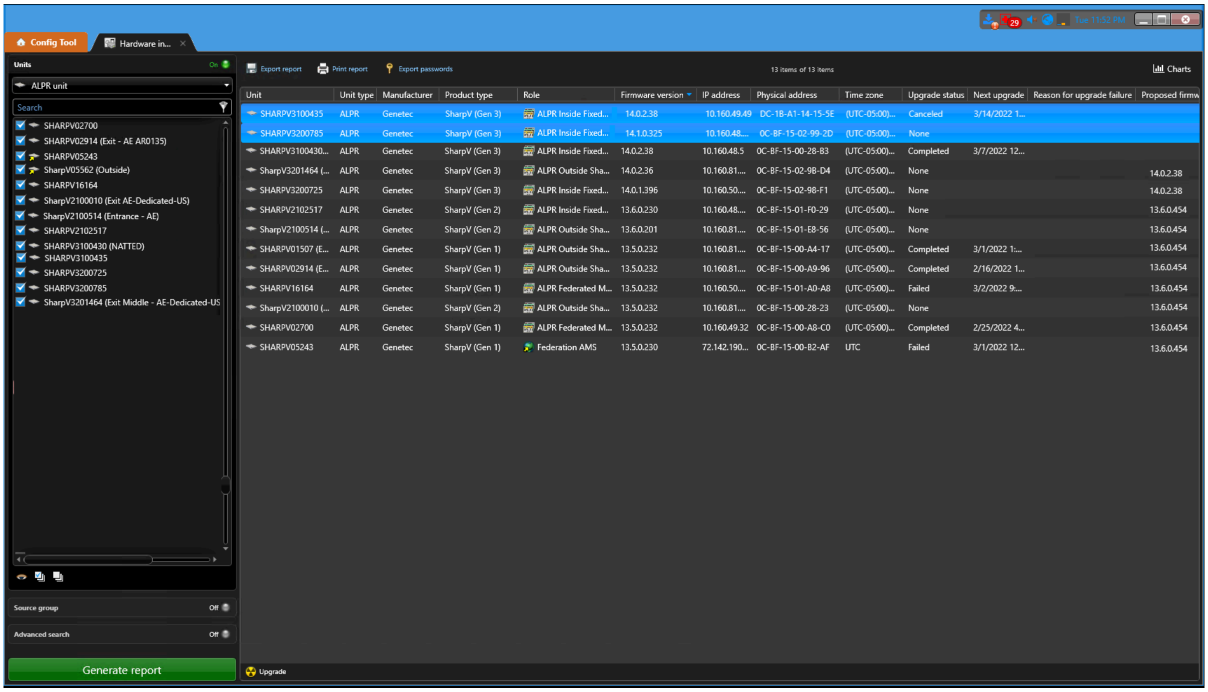


○ Recommended: Not available

● Upgrade using local file:

IMPORTANT: It is recommended to schedule upgrades outside of core business hours.

What you should know



Units On

ALPR unit

Search

☑ SHARPV02700
☑ SHARPV02914 (Exit - AE AR0135)
☑ SHARPV05243
☑ SharpV05562 (Outside)
☑ SHARPV16164
☑ SharpV2100010 (Exit AE-Dedicated-US)
☑ SharpV2100514 (Entrance - AE)
☑ SHARPV2102517
☑ SHARPV3100430 (NATTED)
☑ SHARPV3100435
☑ SHARPV3200725
☑ SHARPV3200785
☑ SharpV3201464 (Exit Middle - AE-Dedicated-US

Source group Off

Advanced search Off

13 items of 13 items

Unit	Unit type	Manufacturer	Product type	Role	Firmware version	IP address	Physical address	Time zone	Upgrade status	Next upgrade	Reason for upgrade failure	Proposed firmw
SHARPV3100435	ALPR	Genetec	SharpV (Gen 3)	ALPR Inside Fixed...	14.0.2.38	10.160.49.49	DC-1B-A1-14-15-5E	(UTC-05:00)...	Canceled	3/14/2022 1...		
SHARPV3200785	ALPR	Genetec	SharpV (Gen 3)	ALPR Inside Fixed...	14.1.0.325	10.160.48....	0C-BF-15-02-99-2D	(UTC-05:00)...	None			
SHARPV3100430...	ALPR	Genetec	SharpV (Gen 3)	ALPR Inside Fixed...	14.0.2.38	10.160.48.5	0C-BF-15-00-28-B3	(UTC-05:00)...	Completed	3/7/2022 12...		
SharpV3201464 (...	ALPR	Genetec	SharpV (Gen 3)	ALPR Outside Sha...	14.0.2.36	10.160.81....	0C-BF-15-02-9B-D4	(UTC-05:00)...	None			14.0.2.38
SHARPV3200725	ALPR	Genetec	SharpV (Gen 3)	ALPR Inside Fixed...	14.0.1.396	10.160.50....	0C-BF-15-02-98-F1	(UTC-05:00)...	None			14.0.2.38
SHARPV2102517	ALPR	Genetec	SharpV (Gen 2)	ALPR Inside Fixed...	13.6.0.230	10.160.48....	0C-BF-15-01-F0-29	(UTC-05:00)...	None			13.6.0.454
SharpV2100514 (...	ALPR	Genetec	SharpV (Gen 2)	ALPR Outside Sha...	13.6.0.201	10.160.81....	0C-BF-15-01-E8-56	(UTC-05:00)...	None			13.6.0.454
SHARPV01507 (E...	ALPR	Genetec	SharpV (Gen 1)	ALPR Outside Sha...	13.5.0.232	10.160.81....	0C-BF-15-00-A4-17	(UTC-05:00)...	Completed	3/1/2022 1:...		13.6.0.454
SHARPV02914 (E...	ALPR	Genetec	SharpV (Gen 1)	ALPR Outside Sha...	13.5.0.232	10.160.81....	0C-BF-15-00-A9-96	(UTC-05:00)...	Completed	2/16/2022 1...		13.6.0.454
SHARPV16164	ALPR	Genetec	SharpV (Gen 1)	ALPR Federated M...	13.5.0.232	10.160.50....	0C-BF-15-01-A0-A8	(UTC-05:00)...	Failed	3/2/2022 9:...		13.6.0.454
SharpV2100010 (...	ALPR	Genetec	SharpV (Gen 2)	ALPR Outside Sha...	13.5.0.232	10.160.81....	0C-BF-15-00-28-23	(UTC-05:00)...	None			13.6.0.454
SHARPV02700	ALPR	Genetec	SharpV (Gen 1)	ALPR Federated M...	13.5.0.232	10.160.49.32	0C-BF-15-00-A8-C0	(UTC-05:00)...	Completed	2/25/2022 4...		13.6.0.454
SHARPV05243	ALPR	Genetec	SharpV (Gen 1)	Federation AMS	13.5.0.230	72.142.190...	0C-BF-15-00-B2-AF	UTC	Failed	3/1/2022 12...		13.6.0.454

NOTE: You can schedule multiple consecutive upgrades for the same SharpV unit. However, it is recommended that a sufficient interval is maintained between the upgrades to ensure that every upgrade is successful.

You can also update individual SharpV units from the respective Sharp Portal.

To upgrade the SharpV unit:

1 In Config Tool, generate a hardware inventory report for the SharpV units you want to upgrade.

2 Select the units that you want to upgrade.

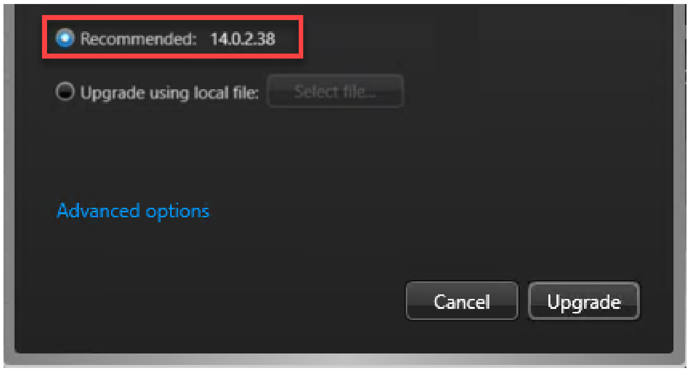
NOTE: You can select different generations of SharpV units to be upgraded simultaneously. However, if the firmware version of *.gpack* selected is not compatible, the upgrade button is not displayed.

3 Click **Upgrade** (☢).

NOTE: If a unit has a firmware upgrade running, and you select another firmware upgrade for that unit, you might need to manually cancel the previous upgrades through the sharp portal.

4 In the pop-up window, you can select from one of the following options for the firmware file:

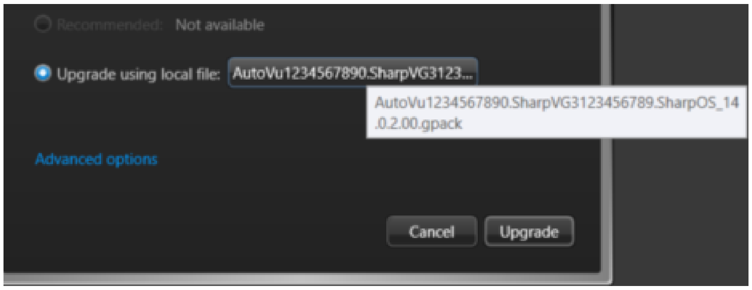
- Recommended: The file is automatically downloaded through Genetec Update Service (GUS).



● Recommended: 14.0.2.38

○ Upgrade using local file:

- Upgrade using local file: In the file browser, select the file that you downloaded from GTAP, and click **Open**.

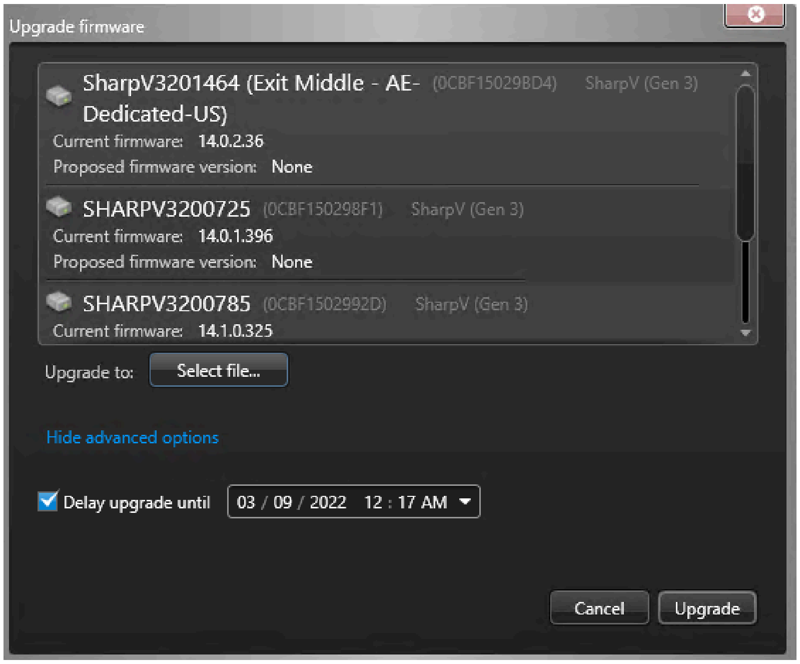


○ Recommended: Not available

● Upgrade using local file: AutoVu1234567890.SharpVG3123...

AutoVu1234567890.SharpVG3123456789.SharpOS_14.0.2.00.gpack

5 (Optional) To delay the upgrade, click **Advanced options**, and select **Delay upgrade until**, and enter the upgrade date and time.



Upgrade firmware

SharpV3201464 (Exit Middle - AE-Dedicated-US) (0CBF15029BD4) SharpV (Gen 3)
Current firmware: 14.0.2.36
Proposed firmware version: None

SHARPV3200725 (0CBF150298F1) SharpV (Gen 3)
Current firmware: 14.0.1.396
Proposed firmware version: None

SHARPV3200785 (0CBF1502992D) SharpV (Gen 3)
Current firmware: 14.1.0.325

Upgrade to: Select file...

Hide advanced options

☑ Delay upgrade until 03 / 09 / 2022 12 : 17 AM

6 Click **Upgrade**.

When the upgrade starts, the *Upgrade status* column displays the current status of the ALPR unit firmware update. You can monitor the percentage of the progress in *Upgrade progression* column.

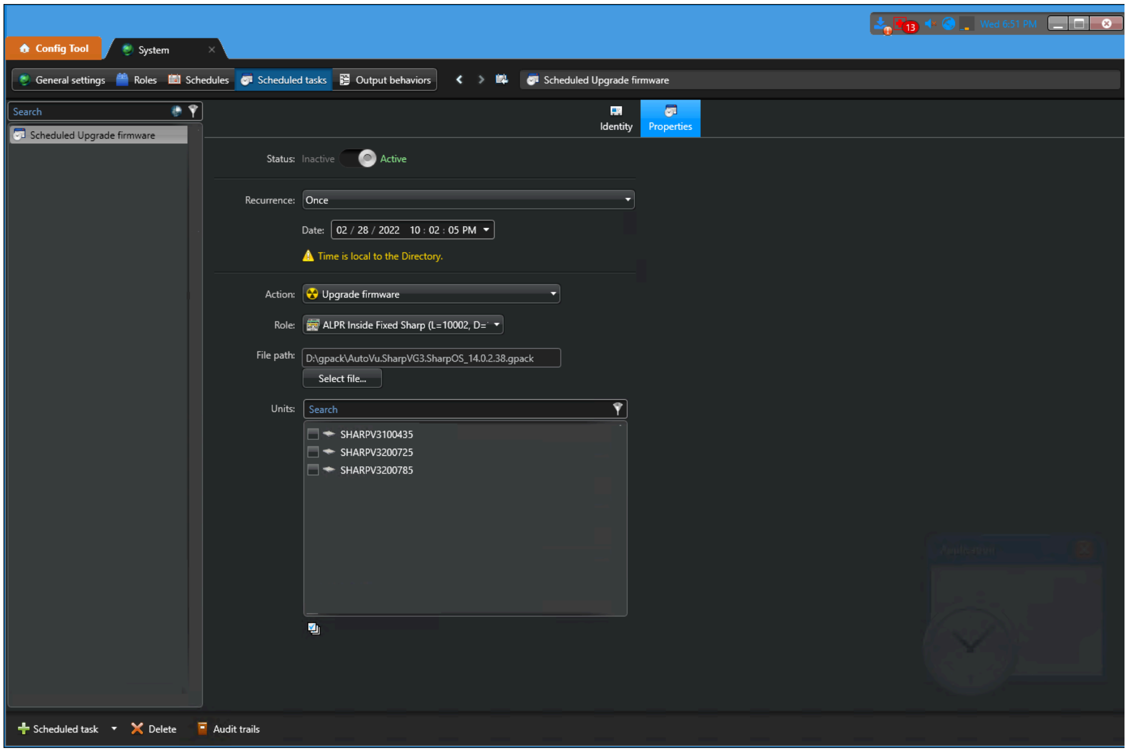
NOTE: To add the *Upgrade progression* column to your report, right-click the column title, click **Select columns**, and select the *Upgrade progression*.

Status	Displayed when
Started	The firmware upgrade starts.
Transfer started	The file transfer starts.
Upgrading	The upgrade starts.
Canceled	The upgrade was canceled by the user.
Failed	The upgrade failed.
Completed	The upgrade is successfully completed.

After you finish

- When the update is complete, generate another *Hardware inventory* report and the *Proposed firmware version* column should display the next version that the unit needs to be upgraded to or *up to date*. You can also view the status of the upgrade from the report.

- You can view, modify, or delete the upgrade task in the following way:
  1. From the Config Tool homepage, open **System** > **Scheduled tasks**.
  2. From the left-hand pane, click the required *scheduled task*.



Status: Inactive Active

Recurrence: Once

Date: 02 / 28 / 2022 10 : 02 : 05 PM

⚠ Time is local to the Directory.

Action: Upgrade firmware

Role: ALPR Inside Fixed Sharp (L=10002, D=

File path: D:\gpack\AutoVu.SharpVG3.SharpOS_14.0.2.38.gpack

Units:

□ SHARPV3100435
□ SHARPV3200725
□ SHARPV3200785

NOTE: You can only modify details such as selected units, file path, and so on, until the firmware upgrade begins. To modify details after upgrade has started, you need to cancel the task and create a task with the correct details.

Part VII

Alarms and critical events

This part includes the following chapters:

54

Alarms

This section includes the following topics:

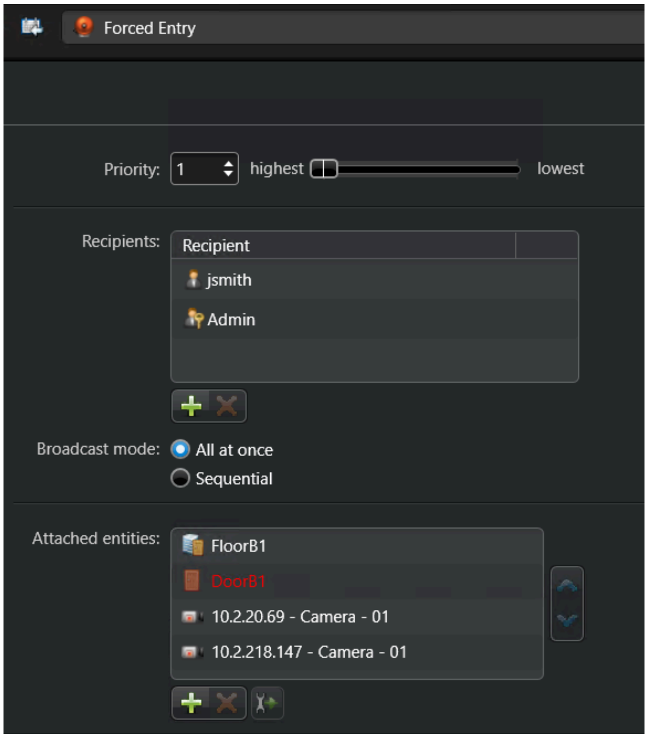
About alarms

An alarm entity describes a particular type of trouble situation that requires immediate attention and how it can be handled in Security Center. For example, an alarm can indicate which entities (usually cameras and doors) best describe the situation, who must be notified, how it must be displayed to the user, and so on.

The basic properties of an alarm are:

- **Name:** Alarm name.
- **Priority:** Priority of the alarm (1-255), based on the urgency of the situation. Higher priority alarms are displayed first in Security Desk.
- **Recipients:** Users, user groups, and analog monitor groups who are notified when the alarm occurs, and are responsible for responding to the alarm situation.
- **Broadcast mode:** How the alarm recipients are notified about the alarm.
  - **All at once:** (Default) All recipients are notified at the same time, immediately after the alarm is triggered.
  - **Sequential:** The recipients are notified individually, each after a specified delay (in seconds) calculated from the time the alarm is triggered. If the recipient is a user group, all members of the user group are notified at the same time.
- **Attached entities:** Entities that help describe the alarm situation (for example, cameras, area, doors, alarm procedure, and so on). When the alarm is received in Security Desk, the attached entities can be displayed one after another in a sequence or all at once in the *canvas*, to help you review the situation. If a composite entity is attached to the alarm, the entities that compose it are also attached to the alarm. For example, if a door entity is attached to the alarm, the cameras associated to the door are also attached to the alarm.

For information about monitoring, acknowledging, and investigating alarms in Security Desk, see the *Security Center User Guide*.



Forced Entry

Priority: 1 highest lowest

Recipients:

Recipient
jsmith
Admin

Broadcast mode: ● All at once ○ Sequential

Attached entities:
FloorB1
DoorB1
10.2.20.69 - Camera - 01
10.2.218.147 - Camera - 01

Alarm priority

In Security Desk, alarms are displayed in the *Alarm monitoring* task and the *Monitoring* task by order of priority (this is evaluated every time a new alarm is received). The highest priority alarm is displayed in tile #1, followed by the second highest in tile #2, and so on. When two alarms have the same priority value, priority is given to the newest one.

When a new alarm is received in Security Desk with a priority level identical or higher than the current alarms displayed, it pushes the other alarms down the tile list.

When an alarm is *acknowledged* in Security Desk, it frees a tile for lower priority alarms to move up.

Video recording on alarms

When an alarm is triggered that has cameras attached to it, you can make sure that the video related to the alarm is recorded and available for future alarm investigations.

The amount of time that the video is recorded for (called the *guaranteed recording span*) is defined by two settings:

- **The alarm recording duration:** Number of seconds that the Archiver records video for after the alarm is triggered. This option (*Automatic video recording*) is set in the alarm *Advanced* tab.
- **The recording buffer:** Number of seconds that the Archiver records video for before the alarm was triggered, to make sure that whatever triggered the alarm is also recorded. This option (*Time to record before an event*) is set in the Archiver *Camera default settings* tab, or for each camera individually.

If an alarm is triggered from a camera event (for example *Object removed*), the camera that caused the event is also attached to the alarm and starts recording.

IMPORTANT: The recordings are dependent on the archiving schedules. If recording is disabled when the alarm is triggered, no video is recorded.

Related Topics

Archiver: Camera default settings tab on page 1338

Differences between threat levels and alarms on page 1190

Creating alarms

For alarms to be triggered in your system, you must create an alarm entity and set up its properties.

What you should know

As a best practice, give names to alarms that best describe the situation, so it is easy to determine what happened when the alarm is triggered.

To create an alarm:

1. From the Config Tool home page, open the *Alarms* task, and click the **Alarms** view.
2. Click **Alarm** (➕).

   A new alarm entity (●) appears in the **Alarms** view.
3. Type a name for the alarm, and press Enter.
4. Click the **Properties** tab.
5. In the **Priority** option, set the priority of the alarm, based on the urgency of the situation.

   Higher priority alarms are displayed first in Security Desk.
6. To add recipients for the alarm, click **Add an item** (➕) under the **Recipients** section, select the users, user groups, or analog monitor groups, and click **Add**.

   Recipients are notified when the alarm occurs, and are responsible for responding to the alarm.
7. If you chose more than one recipient, select how they are notified about the alarm from the **Broadcast mode** option:
   - **All at once:** All recipients are notified at the same time, immediately after the alarm is triggered.
   - **Sequential:** The recipients are notified individually, each after a specified delay (in seconds) calculated from the time the alarm is triggered. If the recipient is a user group, all members of the user group are notified at the same time.
8. To add entities to help describe the alarm, click **Add an item** (➕) under the **Attached entities** section, select the entities, and click **Select**.

   Attached entities help users react to the alarm situation. When the alarm is received in Security Desk, the attached entities (cameras, doors, areas, alarm procedure, and so on), are displayed in the canvas in the Alarm monitoring task.
9. From the **Video display option** list, select the video display options when the alarm is triggered.
10. To automatically rotate the attached entities inside a tile in the *Alarm monitoring* task when the alarm is triggered, switch the **Content cycling** option to **ON**, and set the number of seconds each entity is displayed for.

    NOTE: The order of the entities in the list is the order they are displayed in Security Desk. When the alarm is triggered by an event, the entity that caused the event is also attached to the alarm, and is displayed first.
11. Click **Apply**.
12. Click the **Advanced** tab, and configure the optional alarm settings.

After you finish

Do the following:

- Make sure the alarm recipients have the *Acknowledge alarms* and *Alarm monitoring* user privileges.
- Test the alarm you just created.

Selecting video display options for alarms

If a camera is attached to an alarm, you must configure how the video is shown when the alarm is triggered and displayed in the canvas of the Alarm monitoring task.

What you should know

The default video display option is live video. You can select live video, playback video, a series of still frames before, during, or after the alarm is triggered, or a combination of the three. The video or still frames are displayed for the number of seconds set in the **Content cycling** option in the alarm **Properties** tab.

The options you set are applied to all cameras that are attached to the alarm.

To select the video display options for an alarm:

1 Open the *Alarms* task and click the **Alarms** view.

2 Select the alarm to configure, and click the **Properties** tab.

3 From the **Video display option** list, select one of the following:

- **Live:** Display live video.
- **Playback:** Display playback video.
- **Live and playback:** Cycle between displaying live and playback video. When you unpack the tile, one tile displays live video and the other displays playback. You can also click Properties (⚙) and configure **Picture-in-picture** so you can view the live and playback video in the same tile.
- **Live and still frames:** Cycle between displaying live video and a series of still frames. When you unpack the tile, one tile displays live video and the other displays still frames. You can also click Properties (⚙) and configure **Picture-in-picture** so you can view the live and still frames video in the same tile.

  NOTE: Still frames are not supported when the camera is encrypted.
- **Still frames:** Display a series of still frames. See previous note.

4 If you select a display option that includes playback video, select how many seconds before the alarm was triggered to start the playback.

NOTE: To ensure that playback video is available for the length of time you set, the recording buffer for events must be an equal or larger value.

5 If you select a display option that includes still frames, click Properties (⚙).

6 In the *Still frames* dialog box, select whether you want each still frame to be displayed for the same duration or an independent duration of time (**Same durations** or **Independent durations**).

7 If you select **Same durations**, set the following options:

- **Number of frames:** Select the number of still frames to display within total content cycling duration.
- **Play:** Select how many seconds before the alarm was triggered to start the first still frame.

8 If you select **Independent durations**, do the following:

a) Click **Add an item** (➕).

b) In the **Relative time** option, select how many seconds before or after the alarm was triggered the still frame displays.

c) In the **Duration** option, select how long the still frame is displayed for.

d) Click **Add**.

e) Add additional still frames.

The duration of all the still frames cannot exceed the **Total duration** value.

9 If you select the **Live and Playback** or **Live and still frames** option, you can configure picture-in-picture to display both live and playback video or live and still frame video in the same tile.

   a) Click Properties (⚙).

   b) In the *Video display configuration* dialog box, from the **Picture-in-picture** list, choose what type of video you would like to be displayed in the inset window.

   c) From the **Displayed at** list, select where you would like the inset window to be displayed.

10 Click **OK** > **Apply**.

Setting optional alarm properties

After you create an alarm and configure its basic properties, there are additional properties you can set.

To set optional properties for an alarm:

1 Open the *Alarms* task and click the **Alarms** view.

2 Select the alarm to configure, and click the **Advanced** tab.

3 Set the following options:

- **Reactivation threshold:** The minimum time Security Center needs to wait after triggering this alarm before it can be triggered again. This option prevents the system from repeatedly triggering the same alarm before it is resolved.
- **Alarm procedure (URL):** Enter the URL or the web page address corresponding to the *alarm procedure*, which provides alarm handling instructions to the operators. The web page is displayed when the user clicks *Show alarm procedure* (▤) in the alarm widget in Security Desk.
- **Schedule:** Assign schedules to define when this alarm is in operation. You can assign more than one schedule. Outside the periods defined by these schedules, triggering this alarm has no effect.
- **Automatic acknowledgment:** Turn this option on to let the system automatically acknowledge this alarm if no one acknowledges it before the specified time (in seconds). This option is recommended for low-priority alarms that serve to alert the security operator, but do not require any action. When this option is turned off, the system follows the **Auto ack alarms after** option configured at the system level in Server Admin.

  NOTE: Automatic acknowledgment does not apply to alarms that have an active condition attached. To acknowledge those alarms, you need to forcibly acknowledge them (which requires the *Forcibly acknowledge alarms* privilege). For more information on acknowledging alarms, see the *Security Center User Guide*.
- **Create an incident on acknowledgment:** Turn this option on to prompt the Security Desk user to report an *incident* every time they acknowledge an alarm.

  NOTE: Turning this option on turns the *automatic acknowledgment* option off.
- **Automatic video recording:** Turn this option off (default=on) if you do not want to start recording video when the alarm is triggered.
- **Protect recorded video:**
- **Alarm sound:** Select the sound to play when a new alarm occurs. This sound overrides the default sound configured in **Security Desk** > **Options** > **Alarms**.

  NOTE: For a sound to play when an alarm is triggered, you must click **Security Desk** > **Options** > **Alarms** and enable the **Play a sound** option.
- **Color:** Select a color for the alarm. The color is used for the overlay of the alarm video when it is displayed in a tile in the *Alarm monitoring* or *Monitoring* task, as well as when the alarm is triggered on a map.

4 Click **Apply**.

Related Topics

Archiver: Camera default settings tab on page 1338

Protecting video files from deletion on page 678

Server Admin - Main server page on page 102

Hiding alarms without source entities

You can hide alarms from users who do not have permission to view the alarm source entity by setting **HideAlarmsWithoutSource** to true in the *Advanced settings* page under **Config Tool** > **System** > **General settings**.

Before you begin

You need the *Modify advanced settings* privilege to view the *Advanced settings* page under **Config Tool** > **System** > **General settings**.

What you should know

The alarm source is the entity that triggered the alarm. It is the event source if the alarm is triggered by an event-to-action, or the user, if the alarm is triggered manually. The alarm source is not displayed if the user who receives the alarm does not have permission to view the source entity. This happens when the source entity belongs to a partition to which the user does not have access.

To hide alarms from users who do not have access to the alarm source:

1 Open the *System* task and click **General settings** > **Advanced settings**

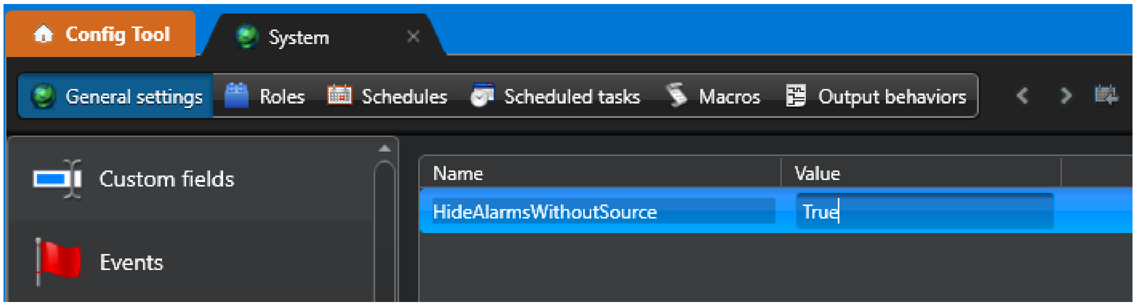
2 Click **Add an item** (➕).

An empty row is added to the advanced parameter list.

3 In the **Name** field, enter `HideAlarmsWithoutSource`.

The parameter name must be written exactly as indicated.

4 In the **Value** field, enter `True`.



Name	Value
HideAlarmsWithoutSource	True

The parameter value is not case sensitive but must spell the word True in English. Any other word is equivalent to False.

5 Click **Apply**.

The new setting immediately applies to all new alarms. If existing alarms are already displayed in an *Alarm monitoring* task, you must close and reopen the task to refresh and filter out the alarms with blank source entities.

Testing alarms

To test if an alarm that you just created works, you can trigger it manually from Config Tool, and make sure that you receive it in Security Desk.

Before you begin

Log on to Security Desk as one of the alarm recipients.

What you should know

You can configure the *Alarm monitoring* task in Security Desk to open automatically when an alarm is triggered. For information about customizing alarm behavior, see the *Security Center User Guide*.

To test an alarm:

1. In Config Tool, open the *Alarms* task.
2. Click the **Alarms** view, and select the alarm to test.
3. In the toolbar at the bottom of the workspace, click **Trigger alarm** (🚨).

   The alarm should appear in the Security Desk notification tray, and in the alarm list in the *Alarm monitoring* task.
4. If the *Alarm monitoring* task does not open automatically, double-click the alarm icon (🚨) in the Security Desk notification tray.
5. In the *Alarm monitoring* task, make sure the alarm appears in the alarm list.

After you finish

If you did not receive the alarm, then you can troubleshoot the alarm.

Troubleshooting: Alarms not received

If you do not receive an alarm in Security Desk, you can troubleshoot the cause of the issue.

To troubleshoot why an alarm is not received:

1 Make sure the user who is trying to receive the alarm is a recipient of the alarm, as follows:
   a) Open the *Alarms* task and click the **Alarms** view.
   b) Select the alarm, and click the **Properties** tab.
   c) Make sure the user, or the user group they are a member of, is in the **Recipients** list.

2 Make sure the alarm schedule is not preventing you from triggering the alarm at this moment, as follows:
   a) Click the **Advanced** tab of the alarm.
   b) Make sure the schedule listed in the **Schedule** list applies at this time.

3 Make sure the alarm recipient has the correct user privileges to receive alarms, as follows:
   a) From the Config Tool home page, open the *User management* task.
   b) Select the user to configure, and click the **Privileges** tab.
   c) Make sure the *Alarm monitoring* and *Acknowledge alarms* user privileges are set to **Allow**.
   d) Click **Apply**.

4 If you use partitions in your system, make sure that the alarm belongs to a partition to which the user has access.

5 If your system is configured to hide alarms from users who do not have permission to view the alarm source, make sure the source entity of the alarm belongs to a partition to which the user has access.

Related Topics

About partitions on page 423

About privileges on page 438

Hiding alarms without source entities on page 1180

Setting up alarms using event-to-actions

You can configure alarms so that they are triggered when an event occurs, using event-to-actions.

To set up an alarm using an event-to-action:

1 Open the *System* task, and click the **General settings** view.

2 Go to the *Actions* page.

3 (Optional) From the **Domain** list, select a subject domain.

Selecting a domain limits the configured actions displayed on this page to the ones associated to an event in that domain. The same filter also applies to all subsequent event selection drop-down lists.

You can select the following domains:

- All
- Access control
- ALPR
- Intrusion detection
- Video

4 Click **Add an item** (✚).

5 From the **When** list in the *Event-to-action* dialog box, select an event type.

a) (Optional: ALPR only) If you select **License plate read**, you can specify a condition for LicensePlateRead events.

b) (Optional: Custom events only) If you select a custom event, you can specify a text string in the **and** field, which must be included in the macro that triggers the event-to-action.

6 In the **From** option, click **Any entity**, and then select an entity that triggers the event.

The *source entity* is the entity that the event is attached to. Only events related to the selected entity type are listed.

7 From the **Action** list, select **Trigger alarm**.

8 From the **Alarm** list, select an alarm to trigger.

9 In the **Effective** option, click **Always**, and select a schedule when this event-to-action is active.

The schedule determines when the event triggers the action. For example, you might want to trigger an alarm only if a window is opened during the weekend. By default, *Always* is selected. If the event occurs outside of the defined schedule, the action is not triggered.

10 (Optional) Enable the **Use source time zone** option to configure the schedule's start and end using the time zone of the source entity's server.

NOTE: This option is only available for cameras, video units, access control units, and doors.

11 (Optional) From the **Acknowledgment condition** list, select an event that must be triggered before the alarm can be acknowledged.

This option is only available for some event types.

12 To require a user to acknowledge the alarm after the acknowledgment condition is cleared, select the **User acknowledgment required** option.

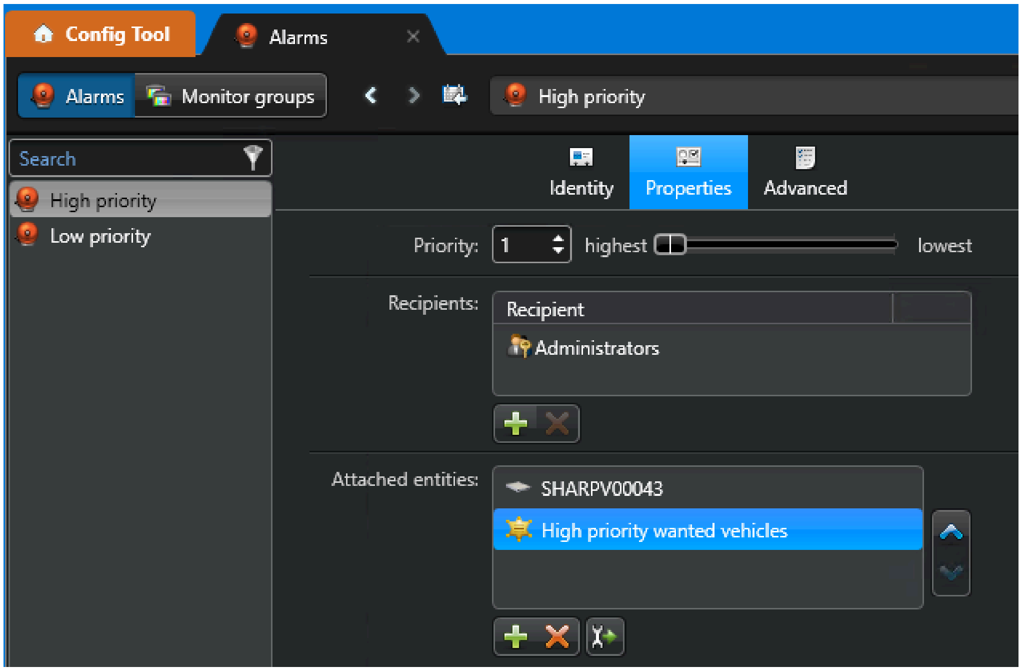
If you clear this option, the alarm is automatically acknowledged when the acknowledgment condition is cleared.

13 Click **Save**.

The **Save** button is only available when all the arguments required by the event-to-action type are specified.

After you finish

If you are using alarms to monitor *ALPR* hits, you must add the associated ALPR rule (hotlist, overtime rule, permit, or shared permit) as an attached entity in the **Properties** tab of the alarm.



Priority: 1

Recipients: Administrators

Attached entities: SHARPV00043, High priority wanted vehicles

Related Topics

Creating event-to-actions on page 212

Event types on page 1410

Event types that can require acknowledgment conditions

You can configure some event-to-actions with a second event that must be triggered before the triggered alarm can be acknowledged. The second event is the *acknowledgment condition*.

For example, you can configure a *Signal lost* event to trigger an alarm, and specify that the alarm can only be acknowledged after the *Signal recovered* event is generated.

To configure an acknowledgment condition that must be cleared before the alarm can be acknowledged, you can use the following event types:

Source event type	Entity type	Acknowledgment condition
AC fail	Access control unit, intrusion detection unit	AC ready
Application lost	Roles	Application online
Asset offline	Asset	Asset online
Asset online	Asset	Asset offline
Battery fail	Access control unit, intrusion detection unit	Battery ready

Source event type	Entity type	Acknowledgment condition
Deadbolt locked, Deadbolt unlocked	Zone	Input (*Normal* or *Active*)
Door closed	Door, Zone	Input (*Normal* or *Active*)
Door forced open	Door, Zone	Door closed Input (*Normal* or *Active*)
Door locked or unlocked	Door, Zone	Input (*Normal* or *Active*)
Door manually unlocked	Door, Zone	Input (*Normal* or *Active*)
Door opened	Door, Zone	Door closed Input (*Normal* or *Active*)
Door open too long	Door	Door closed
Door unsecured	Door	Door secured
Doorknob in place, Doorknob rotated	Zone	Input (*Normal* or *Active*)
Entity warning	Any entity that has an input	Input (*Normal* or *Active*)
Glass break	Zone	Input (*Normal* or *Active*)
Hardware tamper	Access control unit, intrusion detection unit, Zone	Tamper normal Input (*Normal* or *Active*)
Intrusion detection area alarm activated	Intrusion detection area	Disarmed (not ready) Disarmed (ready to arm) Perimeter armed Master armed
Intrusion detection area input bypass activated	Intrusion detection area	Input normal
Intrusion detection unit tamper	Intrusion detection unit	Tamper normal
Lock released, Lock secured	Zone	Input (*Normal* or *Active*)
Manual station activated	Door, Zone	Manual station normal Input (*Normal* or *Active*)
Manual station reverted to normal state	Door, Zone	Input (*Normal* or *Active*)
Motion off, Motion on	Zone[1]	Input (*Normal* or *Active*)
Record updated	Record type, Zone	Input (*Normal* or *Active*)

Source event type	Entity type	Acknowledgment condition
Recording problem	Camera	Recording problem resolved (corresponds to *Recording on* or *Recording off*)
Signal lost	Camera	Signal recovered
Unit lost	Access control unit, intrusion detection unit, ALPR unit, Video unit	Unit online
Window closed, Window opened	Zone	Input (*Normal* or *Active*)
Zone armed, Zone disarmed	Zone	Input (*Normal* or *Active*)
Zone maintenance completed, Zone maintenance started	Zone	Input (*Normal* or *Active*)
Zone offline	Zone	Input (*Normal* or *Active*)

[1] Only *Motion on* and *Motion off* events associated to zone input states can have an acknowledgment condition.

Triggering alarms manually

To test an alarm that you just created, or if something critical occurs and you want to activate an alarm, you can trigger the alarm manually.

Before you begin

- The alarm must be configured in Config Tool.
- The alarm cannot be set to maintenance mode.
- If you want to trigger alarms from the *Monitoring* task, you must enable alarm monitoring.

To trigger an alarm manually:

- Do one of the following:
  - In the Config Tool **Alarms** task, select an alarm, and then click **Trigger alarm** (●) in the toolbar at the bottom of the workspace.
  - In the Security Desk notification tray, click **Hot actions (📢)** > **Manual action** . Click **Trigger alarm** (●), select an alarm, and then click **OK**.
  - In the Security Desk *Alarm monitoring* task or *Monitoring* task, click **Trigger alarm** (▶), select an alarm, and click**Trigger alarm**.

All pre-configured alarm recipients receive the alarm if they are logged on to Security Desk.

Related Topics

Setting entities to maintenance mode on page 366

55

Threat levels

This section includes the following topics:

About threat levels

A *threat* is a potentially dangerous situation, such as a shooting or an infectious disease, that requires immediate response from the system and the security personnel.

Each threat level is characterized by a name and a color, and is associated with two lists of actions that dictate the behavior of the system. One list is executed when the threat level is set, and the other list is executed when the threat is cleared. You can choose from any Security Center actions to define the threat level, plus some additional actions that are unique to threat levels, such as denying certain cardholders access to areas in your system or forcing certain users to log off from the system.

Threat levels are set by Security Desk users who have the *Set threat level* privilege when a dangerous situation occurs. Operators can set a threat level on an area or on the entire system (includes all areas).

Unlock schedules during an active threat level

Areas are configured with a security clearance level ranging from 0 to 7 (0 = highest security, 7 = lowest). A security clearance of 7 is the default value, usually meaning that the area does not require a special clearance. Unlock schedules for areas configured with a security clearance level different than seven are bypassed for the duration of the threat. The moment the threat level is cleared, the unlock schedules for these areas resume.

Setting a threat level has no effect on the following:

- *Manual Override unlock schedule* commands from Security Desk
- *Manual Unlock* commands for specific doors from the Security Desk door widget
- *Temporarily override unlock schedule* event-to-action
- REX activation, meaning the REX activation can still unlock the door
- Unlocking doors from inside the area, meaning that access rules for exiting the area are not affected
- Captive doors inside the area
- Hardware zone I/O linking

Limitations of threat levels

The following limitations apply when using the threat level feature:

- Threat levels work independently of partitions. Therefore, a threat level set at the system level by the users of one partition might affect the entities belonging to another partition, if the actions have a generic scope (applied to *All entities*).
- Threat levels cannot be applied directly to federated areas. This means that when the Federation™ host sets a threat level on a federated area, only the threat level actions are sent to the federated site, not the threat level itself. Local users on the federated site cannot see that a threat level has been set by the Federation™ host.
- Trigger output actions on door locks are blocked when the security clearance for the area is not 7.

Threat level actions

Normally, actions are applied to a specific entity. However, the actions that you configure for a threat level can be applied to all entities of the entity type related to that action.

For example, the action *Start recording* normally applies to one camera. However, when you are configuring a threat level, you can select *All entities* so that all the cameras start recording when the threat level is set.

NOTE: If you apply your action to a specific entity, the action is applied to the specified entity regardless whether the entity is found under the area where the threat level is set or not.

Actions exclusive to threat levels

The following actions are unique to threat level configuration.

Action name	Target entity	Description
Set minimum security clearance	area (Location)	Sets the minimum security clearance level required from cardholders to enter the area on top of the restrictions imposed by the access rules. Perimeter doors in the area go into the locked state if they were previously unlocked because of an unlock schedule. You need the *Set minimum security clearance* privilege to configure this action. Additional parameter: • **Security clearance:** The minimum security clearance level required to enter the selected area. (0=highest level, 7=lowest level or no special clearance required). This action only works with door controllers that support this feature. The range of supported values might vary, depending on the access control hardware. **NOTE:** For this action to be applied to a federated area, the Federation™ user must also have the *Set minimum security clearance* privilege.
Set minimum user level	N/A	Logs out users with a lower user level than the one you specify when a threat level is set, and prevents them from logging back on. You need to be an administrative user to configure this action. Additional parameter: • **User level:** The minimum user level (1=highest level, 254=lowest level) required to log on to the system, or to stay logged on to the system. This action is only executed when the threat level is set at the system level. If the user setting the threat level has a user level below the required minimum, that user is logged off the system the moment the threat level is set.
Set reader mode	area, door (Location)	Sets the reader mode for accessing doors. Additional parameter: • **Reader mode:** Select whether access is granted using *Card and PIN*, or *Card or PIN*, for the selected areas. This action only works with door controllers and readers that support this feature.

Differences between threat levels and alarms

There are key differences between threat levels and alarms, such as why they are triggered, how they are activated, and so on.

The following table highlights the differences between threat levels and alarms.

Characteristics	Alarm	Threat level
Purpose	Deals with localized events, such as a forced entry or an object being left unattended in a public area.	Deals with widespread events affecting an whole area or the entire system, such as a fire or a shooting.
Configuration privileges	• Config Tool • Modify alarms • Add/delete alarms	• Config Tool • Modify threat levels • Add/delete threat levels
Activation	Typically triggered by an event-to-action. Can also be triggered by a manual action.	Typically set manually by a Security Desk operator. Can also be set by an event-to-action.
System response on activation	Recording starts automatically on cameras associated to the alarm.	The threat level activation action list is automatically executed.
Notification method	The alarm icon turns red in the Security Desk notification tray. Depending on your Security Desk configuration, the *Alarm monitoring* task might be brought to the foreground.	The threat level icon turns red in the Security Desk notification tray. When a threat level is set at the system level, the background of Security Desk turns to the color of the threat level.
Recipients	Security Desk users configured as alarm recipients.	All Security Desk users.
Event ranking	Alarms are ranked according to their priority level (1=highest, 255=lowest). Higher priority alarms are displayed first. When the priority level is the same, the most recent is displayed first.	Threat levels are independent of each other. Only one threat level can be set on an area at any given time. The last threat level set overrides the previous one.
Deactivation	A Security Desk user (alarm recipient) must acknowledge the alarm. Alarms can also be automatically acknowledged by the system after a specified delay or when the acknowledgment condition is met.	A Security Desk user must manually clear the threat level or set a different threat level. A threat level can also be automatically cleared using an event-to-action (*Set threat level* to *None*).
System response on deactivation	The acknowledged alarm is removed from all active alarm list (*Alarm monitoring* task in Security Desk).	The threat level deactivation action list is automatically executed.
Related events	• *Alarm triggered* • *Alarm being investigated* • *Alarm condition cleared* • *Alarm acknowledged* • *Alarm acknowledged (alternate)* • *Alarm forcibly acknowledged*	• *Threat level set* • *Threat level cleared*

Characteristics	Alarm	Threat level
Operator privileges	• Security Desk (Application) • Alarm monitoring (Task) • Alarm report (Task) • Trigger alarms (Action) • Snooze alarms (Action) • Forward alarms (Action) • Acknowledge alarms (Action)	• Security Desk (Application) • *Set threat level* (Action) The same privilege is used for both setting and clearing threat levels. To clear a threat level is to set it to *None*. **NOTE:** The threat level activation and deactivation actions are carried out by the system, independently of the operator's privileges.
Exclusive actions	None.	• Set minimum security clearance • Set minimum user level

Related Topics

About alarms on page 1174
Threat level actions on page 1189

Defining threat levels

To help your security personnel quickly respond to a threatening situation, you can define threat levels.

What you should know

CAUTION: The system does not automatically revert to the state it was in before the threat level was set. You must explicitly define the actions that are triggered when the threat is cleared.

To define a threat level:

1. Open the *System* task, click the **General settings** view, and click the **Threat levels** tab.
2. At the bottom of the threat level list, click **Add an item** (➕).
3. In the *Threat level configuration* dialog box, enter the **Name**, **Description**, **Logical ID** (optional), and **Color** of the threat level.

   TIP: Choose a distinctive color for each threat level, so that when the threat level is set at the system level and the Security Desk background turns that color, the users can easily identify the threat.
4. Configure the threat level **Activation actions**.

   These actions are executed by the system when the threat level is set, independently of the privileges and permissions of the user who set the threat level.
5. Configure the threat level **Deactivation actions**.

   These actions are executed by the system when the threat level is cleared or overwritten by another one, independently of the privileges and permissions of the user who cleared the threat level.
6. Click **OK**.

   A new threat level (🚨) appears in the threat level list.
7. Click **Apply**.

After you finish

For all users who need to set threat levels, make sure that they are part of the *public partition*, and make sure that they are assigned the *Set threat level* user privilege.

- To view which threat levels and security clearance are set on each area, use the *System status* task.
- To find out when threat levels were set and cleared, and who did it, use the *Activity trails* task.

Related Topics

Threat level actions on page 1189

Monitoring the status of your Security Center system on page 389

Investigating user-related activity on your Security Center system on page 392

Threat level scenario: Fire

A scenario for creating threat levels is in case of a fire.

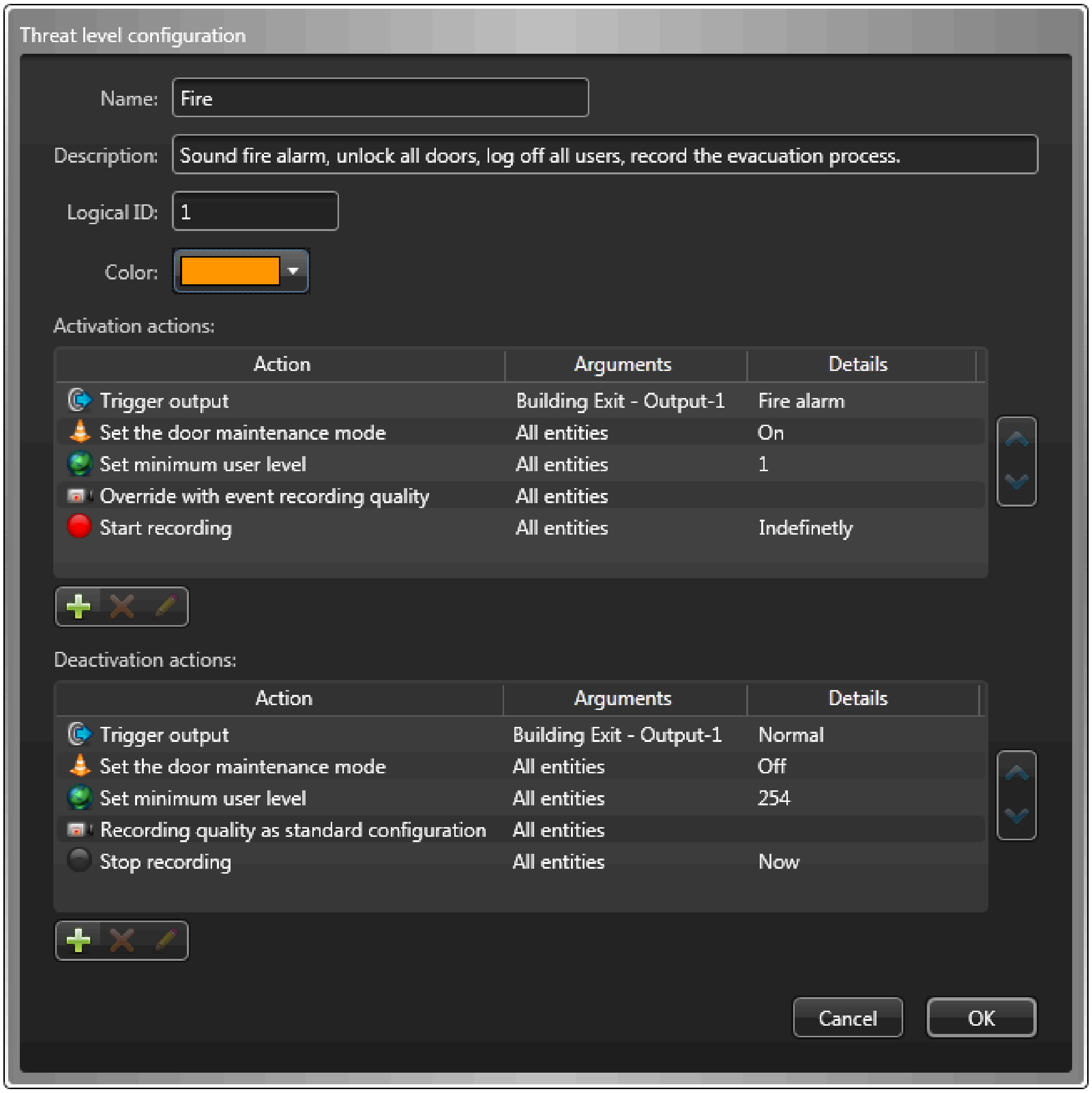
If a fire breaks out, some actions that you want the system to respond with are the following:

- Sound the fire alarm.

  NOTE: For the sake of illustration only. Not a recommended practice.
- Unlock all doors to let people evacuate.

  NOTE: For the sake of illustration only. Not a recommended practice.
- Log off all low priority users to free up your resources (especially network bandwidth), for high priority users to manage the current threat.
- Record the entire evacuation process at high video quality for as long as it lasts.

A threat level for responding to a fire could be configured as follows:



Threat level configuration

Name: Fire

Description: Sound fire alarm, unlock all doors, log off all users, record the evacuation process.

Logical ID: 1

Color: 🟧

Activation actions:

Action	Arguments	Details
Trigger output	Building Exit - Output-1	Fire alarm
Set the door maintenance mode	All entities	On
Set minimum user level	All entities	1
Override with event recording quality	All entities	
Start recording	All entities	Indefinetly

Deactivation actions:

Action	Arguments	Details
Trigger output	Building Exit - Output-1	Normal
Set the door maintenance mode	All entities	Off
Set minimum user level	All entities	254
Recording quality as standard configuration	All entities	
Stop recording	All entities	Now

When an operator sets this threat level, the following actions are executed by the system:

- **Trigger output:** Sounds the fire alarm by sending the *Fire alarm* output behavior to the output relay *Building Exit - Output-1*, assuming that this is where the alarm bell is connected.

- **Set the door in maintenance mode:** Sets all doors within the area where the threat level is set to maintenance mode, effectively unlocking all of them for an indefinite period of time. This is better than using the *Unlock door explicitly* action which only unlocks the doors for a few seconds.
- **Set minimum user level:** Immediately logs off all users with a user level lower than 1, basically every one that is not an administrator, encouraging them to leave their desk at once, as well as stopping all unnecessary activity on the network, so the administrators can have as much bandwidth as possible at their disposal to deal with the situation.

  NOTE: This action is only executed if the threat level is set at the system level. So if the fire is limited to one area, we do not want to log off everyone from the system.
- **Override with event recording quality:** Boosts the recording quality of all cameras within the area where the threat level is set to event recording quality.
- **Start recording:** Starts recording on all cameras within the area where the threat level is set for an infinite duration, or until it the *Stop recording* command is issued.

When an operator clears this threat level, the following actions are executed by the system:

- **Trigger output:** Stops the fire alarm by sending the *Normal* output behavior to the output relay *Building Exit - Output-1*.
- **Set the door maintenance mode:** Turns off the maintenance mode on all doors within the area where the threat level is set. This effectively restores all doors to their normal behavior.
- **Set minimum user level:** Resets the minimum user level to 254 (the lowest value), allowing all users to log back on.
- **Recording quality as standard configuration:** Restores the standard recording quality on all cameras within the area where the threat level is set.
- **Stop recording:** Stops recording on all cameras within the area where the threat level is set. This action will not stop the recording on cameras that are on a continuous recording schedule.

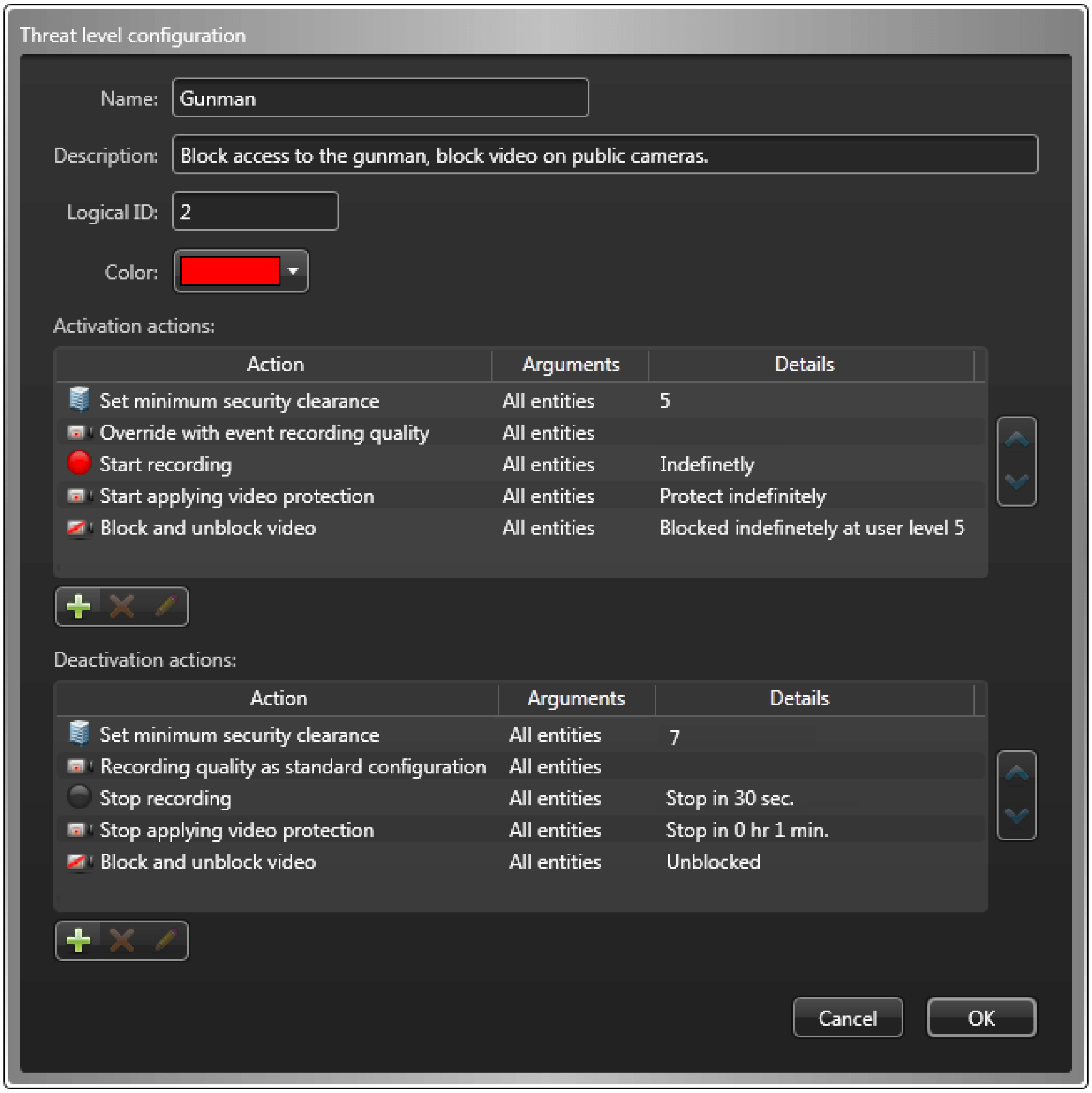
Threat level scenario: Gunman

A scenario for creating threat levels is in case of a gunman.

If a gunman or shooter is spotted, some actions that you want the system to respond with are the following:

- Block access to where the gunman/shooter is from innocent bystanders.
- Record the shooting incident in high quality video as evidence in court.
- Protect the video recordings of the whole event against accidental deletion.
- Block the sensitive video footage from the public eye in case some of the video streams are shown on public websites.

A threat level for responding to a gunman or shooter could be configured as follows:



Name: Gunman

Description: Block access to the gunman, block video on public cameras.

Logical ID: 2

Color: 🟥

Activation actions:

Action	Arguments	Details
Set minimum security clearance	All entities	5
Override with event recording quality	All entities	
Start recording	All entities	Indefinetly
Start applying video protection	All entities	Protect indefinitely
Block and unblock video	All entities	Blocked indefinetely at user level 5

Deactivation actions:

Action	Arguments	Details
Set minimum security clearance	All entities	7
Recording quality as standard configuration	All entities	
Stop recording	All entities	Stop in 30 sec.
Stop applying video protection	All entities	Stop in 0 hr 1 min.
Block and unblock video	All entities	Unblocked

When an operator sets this threat level, the following actions are executed by the system:

- **Set minimum security clearance:** Reduces the mobility of the gunman, assuming the credential he holds has a security clearance lower than 5 (between 6-7).

NOTE: This configuration assumes that only armed security personnel have a clearance level higher than 5 (between 0-5), and that security operators continue to monitor all doors so they can open them when necessary to allow innocent people to hide in secured areas where the gunman cannot access.

- **Override with event recording quality:** Boosts the recording quality of all cameras within the area where the threat level is set to event recording quality.
- **Start recording:** Starts recording on all cameras within the area where the threat level is set for an infinite duration, or until it the *Stop recording* command is issued.
- **Start applying video protection:** Starts protecting the videos recorded from the cameras within the area where the threat level is set, from now until the *Stop applying video protection* command is issued, for an unlimited period of time.
- **Block and unblock video:** Block all users with a user level lower than 5 from viewing the video from the cameras within the area where the threat level is set, from now until the video blocking is explicitly stopped, for an unlimited period of time.

  NOTE: This configuration assumes that all security personnel have a user level higher than 5 and can continue to monitor the scene.

When an operator clears this threat level, the following actions are executed by the system:

- **Set minimum security clearance:** Restore normal access to the area to all cardholders by setting the security clearance to 7 (the lowest level).
- **Recording quality as standard configuration:** Restores the standard recording quality on all cameras within the area where the threat level is set.
- **Stop recording:** Stops recording on all cameras within the area where the threat level is set after 30 seconds. This action will not stop the recording on cameras that are on a continuous recording schedule.
- **Stop applying video protection:** Stops protecting the videos recorded from the cameras within the area where the threat level is set, after one minute.
- **Block and unblock video:** Unblock all cameras within the area where the threat level is set. The video recorded during the time when the threat level was active will remain blocked for playback to the users whose user level is lower than 5.

56

Zones and intrusion detection

This section includes the following topics:

About zones

A zone is an entity that monitors a set of inputs and triggers events based on their combined states. These events can be used to control output relays.

The concept of a zone is borrowed from the world of *alarm panels*, where electric inputs are associated with zones to trigger specific alarms. In Security Center, electrical inputs are associated with zones to trigger events. Using *event-to-actions*, these events can be used to not only trigger outputs, but also to trigger alarms, send emails, start camera recordings, and so on.

TIP: You can also define custom events to correspond to each of the special input combinations.

A zone can be armed (triggers activated), or disarmed (triggers deactivated) using a key switch, a software command, or on a schedule. A zone can be armed by software (using an action command or according to a schedule), or by hardware (for units that support this feature).

I/O linking

I/O linking is the control of specific output relays based on the combined result of a specific set of electric inputs. Each input can be connected to a specific monitoring device, such as a motion sensor, a smoke detector, a door or window contact, and so on.

For example, if a window shatters, the *glass break* sensor on a window connected to an input on a *unit*, can be linked to an output that triggers a buzzer.

CAUTION: On HID VertX units, some inputs, such as *AC Fail* and *Bat Fail*, must be configured for something other than their initial purpose (leave the checkboxes empty) before they can be used for I/O linking. However, other inputs, such as *Door Monitor*, can only be used for their designated purpose. If you use a specific purpose input as general purpose, your configuration will not work. Do not exceed 20 inputs per zone with HID VertX units. Exceeding this limit may lead to unit synchronization problems.

Zone states

Zone states are determined by a combination (AND/OR) of inputs associated with the zone.

The following zone states are available:

- **Normal:** When the combination of inputs yields a zero (0).
- **Active:** When the combination of inputs yields a one (1).
- **Trouble:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.

Hardware zones

A hardware zone is a zone entity in which the I/O linking is executed by a single access control unit. A hardware zone works independently of the Access Manager, and consequently, cannot be armed or disarmed from Security Desk.

Hardware zones are recommended when quick responses and offline operations are crucial for your security system. The *access control unit* controlling the zone must not be operated in *server mode*. Once the unit is configured in Security Center, it must be able to act on its own without being connected to, or controlled by Security Center.

Hardware zones can be armed using a key switch (input), or on schedules.

Virtual zones

A virtual zone is a zone entity where the I/O linking is done by software. The input and output devices can belong to different units of different types. A virtual zone is controlled by the Zone Manager and only works when all the units are online. It can be armed and disarmed from Security Desk.

Virtual zones are recommended when flexibility is required, and when access control units are not available.

I/O zones

An I/O zone is a zone entity in which the I/O linking can be spread across multiple Synergis™ units, while one unit acts as the master unit. All Synergis™ units involved in an I/O zone must be managed by the same Access Manager. The I/O zone works independently of the Access Manager, but ceases to function if the master unit is down. An I/O zone can be armed and disarmed from Security Desk as long as the master unit is online.

I/O zones are recommended when quick responses, offline operation, and I/O linking across multiple units are required.

Differences between the types of zone

The following table lists the differences between a hardware zone, a virtual zone, and an I/O zone, and can help you decide which type of zone you need to create.

Characteristics	Hardware zone	Virtual zone	I/O zone
Recommended use	Hardware zones are recommended when quick responses and offline operations are crucial for your security system.	Virtual zones are recommended when flexibility is required, and when access control units are not available.	I/O zones are recommended when quick responses, offline operation, and I/O linking across multiple units are required.
Role	Access Manager	Zone Manager	Access Manager
Required unit type	HID or Synergis™ unit	Any type of unit with inputs and outputs[1]	Synergis units[2]
Unit operation mode	Online and Offline	Online	Online and Offline
I/O linking execution	Access control unit	Zone Manager	Master unit[3]
I/O linking (inputs)	All inputs must be from the same unit	Can combine inputs from any unit of any type	Can combine inputs from any unit
Logical operator (inputs)	**OR**/AND	**OR**/AND	OR
I/O linking (outputs)	All outputs must be from the same unit as the inputs	Can trigger outputs on any unit of any type	Can trigger outputs on any unit
I/O linking configuration	Zone configuration + event-to-actions	Zone configuration + event-to-actions	Zone configuration alone
Peer-to-peer	No	No	Yes[4]
Arm/disarm from Security Desk	No	Yes	Yes[5]

Characteristics	Hardware zone	Virtual zone	I/O zone
Arm/disarm using actions	No	Yes	Yes[5]
Arm/disarm using key switch	Yes[6]	No	No
Arm/disarm on schedule	Yes[7]	Yes[8]	Yes[9]
Arming delay	**OFF**/ON (mm:ss)	**OFF**/ON (mm:ss)	No
Entry delay	**OFF**/ON (mm:ss)	**OFF**/ON (mm:ss)	No
Maintenance mode	No	No	Yes

[1] Using zones to monitor the inputs of intrusion detection units is not recommended.

[2] Requires Synergis™ Softwire 10.2 and later.

[3] The master unit is the Synergis unit that you select to do I/O linking.

[4] Up to 15 Synergis units can communicate directly with each other, as long as they are all under the same Access Manager.

[5] The master unit must be online.

[6] The key switch must be wired to an input on the same access control unit.

[7] Only one schedule at a time, and cannot be combined with the key switch approach.

[8] Supports multiple schedules.

[9] Supports multiple schedules, including exception schedules.

About Zone Managers

The Zone Manager role manages virtual zones and triggers events or output relays based on the inputs configured for each zone. It also logs the zone events in a database for zone activity reports.

Multiple instances of this role can be created on the system.

About output behaviors

An output behavior is an entity that defines a custom output signal format, such as a pulse with a delay and duration.

Some examples of output behaviors can include controlling a parking gate, flashing a light in a warehouse, and so on.

Output behaviors are used to control output relays on access control units, video units, and zones that are not being used to control door locks. They can be triggered automatically through event-to-actions, manually through *hot actions* in Security Desk, or through *I/O linking*.

Creating hardware zones

To have a zone that can operate on its own even when the access control unit is not connected to the Access Manager, you must create a hardware zone in Security Center.

Before you begin

Do the following:

- Configure the Access Manager role that will manage the zone.
- Add the access control unit that will control the zone in your system.

What you should know

A *hardware zone* allows you to program the I/O linking behavior on an access control unit so it can operate on its own. Hardware zones can only be controlled by a single access control unit.

To create a hardware zone:

1. Open the *Area view* task.
2. Click **Add an entity** (✚) > **Zone**.
3. In the zone creation wizard, enter a name and description for the zone.
4. Select the area this zone is part of in **Location**, and click **Next**.
5. On the *Zone information* page, click **Zone**.
6. From the dialog box, select the access control unit to control this zone and click **OK**.
7. Click **Create** > **Close**.

After you finish

Configure the hardware zone.

Related Topics

About zones on page 1199

Configuring hardware zone settings

To monitor and set up I/O linking for hardware zones in Security Center, you must decide how the zone state is evaluated, which events are triggered based on the inputs associated with the zone, and when the zone is armed.

Before you begin

- To arm the zone on a schedule, a schedule must already be created.
- To arm the zone using a key switch, one of the inputs from the access control unit must be wired to the key switch.

What you should know

All input points and output relays configured for this zone must belong to the same access control unit that is controlling the zone.

You cannot arm or disarm a hardware zone from Security Desk, or by using a software command (event-to-actions).

To configure hardware zone settings:

1. Open the *Area view* task.
2. Select the hardware zone to configure, and click the **Properties** tab.
3. From the list, select the inputs to determine the state of the zone.
4. Turn the **Operator** switch to the desired position.
   - **AND:** Combine the input states with the logical AND operator.
   - **OR:** (Default) Combine the input states with the logical OR operator

   Example: If you select the **AND** operator, the zone is considered to be in a *Active* state when all selected inputs are in the *Active* state. If you select the **OR** operator, the zone is considered to be in a *Active* state if one of the selected inputs is in the *Active* state.
5. In the **Associated events** section, select which events to trigger when the zone state changes, from the following drop-down lists:

   These events are only triggered when the zone is armed. Select *None* if a zone state should be ignored.
   - **Normal:** When the combination of inputs yields a zero (0).
   - **Active:** When the combination of inputs yields a one (1).
   - **Trouble:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.
6. Enter in **Reactivation threshold**, how many milliseconds must pass before the event associated to the zone state can be re-triggered, and click **Apply**.

   NOTE: The reactivation threshold does not apply if the zone state transitions to or from the *Trouble* state.
7. Click the **Arming** tab, and configure how the zone is armed.
8. In the *Arming source* section, select whether the zone is armed using a key switch, or on a schedule:
   - **Schedule:** Select a predefined schedule for arming the zone.
   - **Input point:** Select the input that is wired to the key switch.

9 (Optional) To give people more time to leave a zone they just armed, or disarm a zone they entered, turn the following options **ON**:

- **Arming delay:** Duration (mm:ss) you want between the time the zone is armed and the time the event triggers become active.
- **Entry delay:** Duration (mm:ss) you want between the time the entry sensor is tripped and the time the events are triggered. This option allows you to disarm the zone before triggering the output relays.

10 (Optional) Select a **Countdown buzzer** to use for the duration of the arming delay, as follows:

NOTE: This option is only available when the zone is armed using a key switch.

a) From the **Countdown sounder** list, select an output relay.

b) From the **Output behavior** list, select an output behavior entity to determine the pattern of the signal to send to the buzzer.

11 Click **Apply**.

After you finish

- Test your zone by verifying that the generated events show up in the *Zone activities* report in Security Desk. For more information, see the *Security Center User Guide*.
- For each associated event configured for this zone, create event-to-actions to trigger the desired output relays to complete the I/O linking configuration.

  NOTE: For the hardware zone to work, the output relays must be among the peripherals of the unit controlling the zone.

Related Topics

HID I/O linking considerations on page 1487

Hardware zone configuration tabs on page 1272

Creating virtual zones

To monitor input devices (sensors, switches, and so on) using Security Desk, and to use them to trigger events, you must create a virtual zone in Security Center.

Before you begin

Configure the Zone Manager role that will manage the zone.

What you should know

A virtual zone allows you to turn monitoring on/off in the various input devices (sensors, switches, and so on) on your system using Security Desk, and to use them to trigger events.

To create a virtual zone:

1 Open the *Area view* task.

2 Click **Add an entity** (➕) > **Zone**.

3 In the zone creation wizard, enter a name and description for the zone.

4 Select the area this zone is part of in **Location**, and click **Next**.

5 On the *Zone information* page, click **Virtual zone**.

If you have multiple Zone Manager roles, you are prompted to select one.

6 Click **Create** > **Close**.

After you finish

Configure the virtual zone.

Related Topics

About zones on page 1199

Configuring virtual zone settings

To monitor input devices and use them to trigger events for virtual zones in Security Center, you must decide how the zone state is evaluated, which events are triggered based on the inputs associated with the zone, and when the zone is armed.

Before you begin

To arm the zone on a schedule, a schedule must already be created.

What you should know

A virtual zone can be armed at any time by a Security Desk operator, or by the *Arm zone* action. Arming schedules is optional and is only necessary if you want the zone to be armed automatically at a certain time. An armed virtual zone can be disarmed at any time by a Security Desk user, or by the *Disarm zone* action triggered by an event.

To configure virtual zone settings:

1 Open the *Area view* task.

2 Select the virtual zone to configure, and click the **Properties** tab.

3 Under the **Inputs** list, click **Add an item** (➕), select the inputs that will determine the state of the zone, and click **Select**.

TIP: Hold **Ctrl** or **Shift** to select multiple inputs.

4 Turn the **Operator** switch to the desired position.

- **AND:** Combine the input states with the logical AND operator.
- **OR:** (Default) Combine the input states with the logical OR operator

Example: If you select the **AND** operator, the zone is considered to be in a *Active* state when all selected inputs are in the *Active* state. If you select the **OR** operator, the zone is considered to be in a *Active* state if one of the selected inputs is in the *Active* state.

5 In the **Associated events** section, select which events to trigger when the zone state changes, from the following drop-down lists:

These events are only triggered when the zone is armed. Select *None* if a zone state should be ignored.

- **Normal:** When the combination of inputs yields a zero (0).
- **Active:** When the combination of inputs yields a one (1).
- **Trouble:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.

6 Enter in **Reactivation threshold**, how many milliseconds must pass before the event associated to the zone state can be re-triggered, and click **Apply**.

NOTE: The reactivation threshold does not apply if the zone state transitions to or from the *Trouble* state.

7 Click the **Arming** tab, and configure how the zone is armed.

8 Under the *Arming source* section, click **Add an item** (➕), select a predefined schedule for when the zone is armed, and click **Select**.

9 (Optional) To give people more time to leave a zone they just armed, or disarm a zone they entered, turn the following options **ON**:

- **Arming delay:** Duration (mm:ss) you want between the time the zone is armed and the time the event triggers become active.
- **Entry delay:** Duration (mm:ss) you want between the time the entry sensor is tripped and the time the events are triggered. This option allows you to disarm the zone before triggering the output relays.

10 Click **Apply**.

After you finish

- Test your zone by verifying that the generated events show up in the *Zone activities* report in Security Desk. For more information, see the *Security Center User Guide*.
- For each associated event configured for this zone, create event-to-actions to trigger the desired output relays to complete the I/O linking configuration.

Related Topics

Virtual zone configuration tabs on page 1303

Creating I/O zones

To have the inputs on one Synergis™ unit trigger output relays on other Synergis units (even when some, or none of them are connected to the Access Manager), you must create an I/O zone in Security Center.

Before you begin

- Configure the Access Manager role that will manage the zone.
- Add the Synergis units that will be linked by the zone.
- Make sure all units are running Synergis™ Softwire version 10.2 or later.

What you should know

An *I/O zone* allows you to program the I/O linking behavior on multiple Synergis units, with one unit designated as the master unit. All units must be managed by the same Access Manager. An I/O zone can be armed and disarmed from Security Desk as long as the master unit is online.

To create a hardware zone:

1 Open the *Area view* task.

2 Click **Add an entity** (✚) > **Zone**.

3 In the zone creation wizard, enter a name and description for the zone.

4 Select the area this zone is part of in **Location**, and click **Next**.

5 On the *Zone information* page, click **I/O zone**.

6 From the dialog box, select the Synergis unit that will play the role of *master unit* among its peers, and click **OK**.

The master unit is the Synergis unit that you select to do I/O linking. Once your choice is made, it cannot be changed after the I/O zone is created.

7 Click **Create** > **Close**.

After you finish

Configure the I/O zone.

Related Topics

About zones on page 1199

Configuring I/O zone settings

To monitor and set up I/O linking for I/O zones in Security Center, you must decide how the zone state is evaluated, which output relays are triggered based on the inputs associated with the zone, and when the zone is armed.

Before you begin

- To arm the zone on a schedule, a schedule must already be created.
- To trigger an output relay, an output behavior must already be created.

What you should know

All input points and output relays configured for this zone must belong to Synergis™ units that are managed by the same Access Manager.

You can configure the I/O linking from the I/O zone's **Properties** tab. You do not need to create *event-to-actions* in order to trigger output relays.

IMPORTANT: If the inputs and outputs configured for this zone do not belong to the same Synergis unit, you must enable the **Activate peer-to-peer** option on the Access Manager.

To configure I/O zone settings:

1. Open the *Area view* task.
2. Select the I/O zone to configure, and click the **Properties** tab.
3. From the **Arming schedule** list, select a predefined schedule for when the zone is armed.

   To add more predefined schedules for defining the arming schedule, click **Advanced** (⊕) and then click **Add an item** (✚).
4. (Optional) Click **Exceptions** to define periods within the arming schedule when the zone should not be armed.
5. Under the **Inputs** list, click **Add an item** (✚), and select inputs to determine the state of the zone.

   The zone is considered to be in a *Trouble* state if one of the inputs is in the Trouble state.
6. Under the **Outputs** list, click **Add an item** (✚), and select the output relays that you want to send the configured output behavior to, when the zone is armed and in the *Active* state, or when the zone is in the *Trouble* state.

   BEST PRACTICE: As much as possible, use the output relays on the master unit. This allows the I/O zone to continue to function when one or more slave units are down.
7. From the **Output behavior** list, select the output behavior to send to the output relays.
8. Select **Activate output on trouble when the zone is disarmed** if you want the output relays to be triggered when the zone is in the *Trouble* state.
9. From the **Revert to** list, select the output behavior to send to the output relays when the zone returns to the *Normal* state.
10. In the **Associated events** section, select which events to trigger when the zone state changes, from the following drop-down lists:

    These events are only triggered when the zone is armed. Select *None* if a zone state should be ignored.

    - **Normal:** When the combination of inputs yields a zero (0).
    - **Active:** When the combination of inputs yields a one (1).
    - **Trouble:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.

11 Enter in **Reactivation threshold**, how many milliseconds must pass before the event associated to the zone state can be re-triggered, and click **Apply**.

   NOTE: The reactivation threshold does not apply if the zone state transitions to or from the *Trouble* state.

After you finish

Test your zone by verifying that the generated events show up in the *Zone activities* report in Security Desk. For more information, see the *Security Center User Guide*.

Related Topics

I/O zone - Properties tab on page 1275

Intrusion panel integration

Intrusion panels (also known as *alarm panels* or *control panels*) can be integrated to Security Center using the Intrusion Manager role.

Intrusion panels allow you to monitor the status of any zone (or group of sensors) in real time, generate detailed activity reports, and arm and disarm zones (or partitions) defined on the intrusion panels in Security Desk.

Security Center supports intrusion systems from many manufacturers, including; Bosch, DSC PowerSeries, Honeywell, DMP, and more. For a list of supported manufacturers and links to our integration guides for each, see the *Supported plugins in Security Center*.

How Intrusion panel integration works

The Intrusion Manager role receives events from the panel over an IP network or serial connection, reports them live in Security Desk, and logs them in a database for future reporting. The role also relays user commands to the panel (such as arming and disarming the intrusion detection areas), and triggers the outputs connected to the panel through event-to-actions (for example, an *Intrusion detection area master armed* event in Security Center can trigger an output on the panel).

Working with intrusion detection units in Security Desk

Using Security Desk, operators can monitor, investigate, and control the intrusion detection units. For more information, read the following topics in the *Security Center User Guide*. You can access this guide by pressing **F1** in Security Desk.

- Monitoring events.
- Monitoring alarms.
- Monitoring intrusion detection units.
- Using intrusion detection area widget.
- Triggering hot actions.
- Monitoring the status of entities in your system using the *System status* task.
- Investigating past events from the entities in your system using the *Intrusion detection area activities* or *Intrusion detection unit events* tasks.

About Intrusion Managers

The Intrusion Manager role monitors and controls intrusion detection units. It listens to the events reported by the units, provides live reports to Security Center, and logs the events in a database for future reporting.

The Intrusion Manager also relays user commands to intrusion panels such as arming the *intrusion detection areas* (or zones), and triggering outputs connected to the panel using *event-to-actions*.

Multiple instances of this role can be created on the system.

Limitations of Intrusion Manager roles

For purposes of *failover*, the Intrusion Manager can be assigned to more than one server. However, the Intrusion Manager only supports failover when the intrusion panels are connected via IP. Failover is not supported if your intrusion panel is directly connected to your server via serial port, failover is not supported.

Creating the Intrusion Manager role

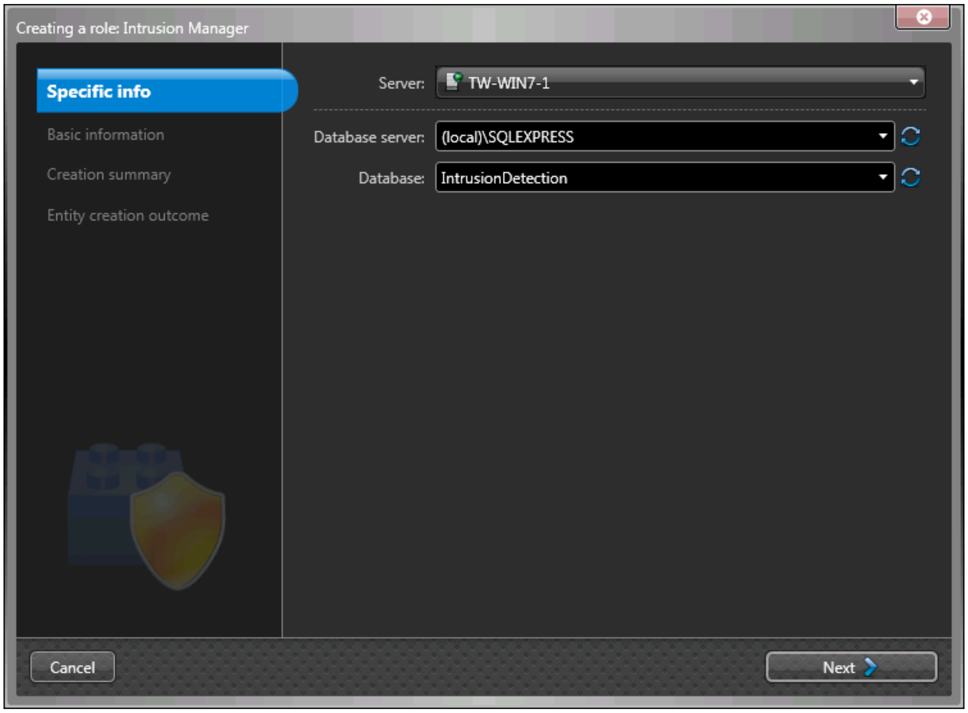
You must create an Intrusion Manager role in Config Tool to manage the intrusion detection units.

To create an Intrusion Manager role:

1 From the Config Tool home page, open the *System* task, click **Roles**.

2 Click **Add an entity** (+), and then **Intrusion Manager**.

The *Creating a role: Intrusion Manager* window opens.



Server: TW-WIN7-1

Database server: (local)\SQLEXPRESS

Database: IntrusionDetection

3 On the *Specific info* page, do the following:

a) From the **Server** list, select the server assigned to this role.

NOTE: If no expansion server is present, this option is not available.

b) In the **Database server** field, select or type the name of the database server.

c) In the **Database** field, select or type the name of the database (for example, **IntrusionDetection**).

d) Click **Next**.

4 On the *Basic information* page, do the following:

a) Type the **Entity name** (**Intrusion Manager**).

b) Type an **Entity description** for the role.

c) Click **Next**.

5 On the *Creation summary* page, do the following:

a) Verify the information you entered.

b) If everything is correct, click **Create**, or click **Back** to modify your settings.

When the role is created, you see the following message: *The operation was successful.*

6 Click **Close**.

After you finish

Add the intrusion detection units in Security Center.

About intrusion detection units

An intrusion detection unit entity represents an intrusion device (intrusion panel, control panel, receiver, and so on) that is monitored and controlled by the Intrusion Manager role.

An *intrusion panel* (also known as *alarm panel* or *control panel*) is a wall-mounted unit where the alarm sensors (motion sensors, smoke detectors, door sensors, and so on) and wiring of the intrusion alarms are connected and managed.

For a list of intrusion detection panels supported in Security Center, see the "Intrusion detection" section in Supported plugins in Security Center.

To monitor and control intrusion detection areas (zones or partitions) in Security Desk, you must enroll the intrusion panel that controls them by adding an intrusion detection unit. For information about creating intrusion detection units in Security Center, see the corresponding Intrusion Panel Extension Guide.

Limitations in monitoring intrusion panel inputs

We recommend that you use intrusion panels only for intrusion monitoring.

Intrusion panels are not designed to capture rapid consecutive changes to their input states, such as doors being opened and closed rapidly, or motion sensors that detect constant movements.

The main purpose of an input on an intrusion panel is to trigger an alarm when its state changes. When the input becomes active while its intrusion detection area is armed, the panel raises an alarm. Security Center uses this alarm to trigger an *Intrusion detection area alarm activated* event.

- Intrusion panels are limited in the number of events they can report; they are also limited in how fast they can transmit them.
- It might take a few minutes to receive the changes to the input states in Security Center.
- Some of the changes to the input states might not be reported in Security Center even though the panel raises intrusion alarms.

About intrusion detection areas

An intrusion detection area entity represents a zone (sometimes called an area) or a partition (group of sensors) on an intrusion panel.

Intrusion detection areas might be created automatically by the Intrusion Manager role when the intrusion panels on which they are configured are enrolled in your system.

You can assign cameras to intrusion detection areas and intrusion detection inputs for monitoring purposes in Security Desk and you can configure the mapping of an output relay to an input pin for virtual alarms. Intrusion detection areas are automatically updated when the zones they correspond to are updated on the intrusion panels.

Users can perform the following actions on intrusion detection areas:

NOTE: You might not be able to perform some of these actions, depending on the type of intrusion panel you are using.

- **Master arm:** Master arm is arming an intrusion detection area in such a way that all sensors attributed to the area would set the alarm off if one of them is triggered. Some manufacturers call this arming mode “Away arming”.
- **Perimeter arm:** Perimeter arm is arming an intrusion detection area in such a way that only sensors attributed to the area perimeter set the alarm off if triggered. Other sensors, such as motion sensors inside the area, are ignored.
- **Disarm:** Disarm the area, by causing all sensors attributed to the selected intrusion detection area to be ignored by the intrusion panel.
- **Trigger intrusion alarm:** Trigger an intrusion alarm on the selected intrusion detection area.
- **Silence alarm:** If there is an active alarm on the selected intrusion detection area, stop the siren on the intrusion panel from beeping. Depending on your intrusion panel and the type of alarm, clicking **Silence alarm** might also acknowledge the alarm.
- **Acknowledge alarm:** Acknowledge the intrusion alarm on the selected intrusion detection area.

Creating intrusion detection areas

If the intrusion detection areas were not automatically created after the intrusion detection unit was enrolled, you must create them manually, so the areas can be armed, disarmed, and so on.

Before you begin

Add the intrusion detection unit to control the areas.

To create an intrusion detection area:

1. Open the *Intrusion detection* task.
2. Click **Add an entity** (➕) > **Show all** > **Intrusion detection area**.
3. On the *Basic information* page, enter a name and description for the area.
4. Select the **Partition** this area is a member of, and click **Next**.

   Partitions determine which Security Center users have access to entities. Only users that are part of the partition can view or modify the intrusion detection area.
5. From the **Intrusion detection unit** list, select the intrusion detection unit to control this area.
6. Under **Intrusion detection area unique ID**, enter the ID or name of the area as it is configured on the intrusion panel.
7. Click **Next** > **Create** > **Close**.

Related Topics

About intrusion detection areas on page 1218

Assigning cameras to intrusion detection areas

To display a camera feed in a Security Desk monitoring tile when an intrusion area event occurs, such as *Intrusion detection area disarmed*, you can assign cameras to intrusion detection area entities.

What you should know

When cameras are associated to the intrusion detection area and related intrusion detection inputs and an event occurs, only the relevant cameras are shown, and the most relevant is shown first. For example, when an area event occurs, only the cameras assigned to the area are shown in the monitoring tile. When an input event occurs, the camera assigned to the input is displayed first, and the cameras assigned to the area are displayed in the other tiles. You can cycle or unpack the tile to display the video from the other cameras.

To assign cameras to an intrusion detection area:

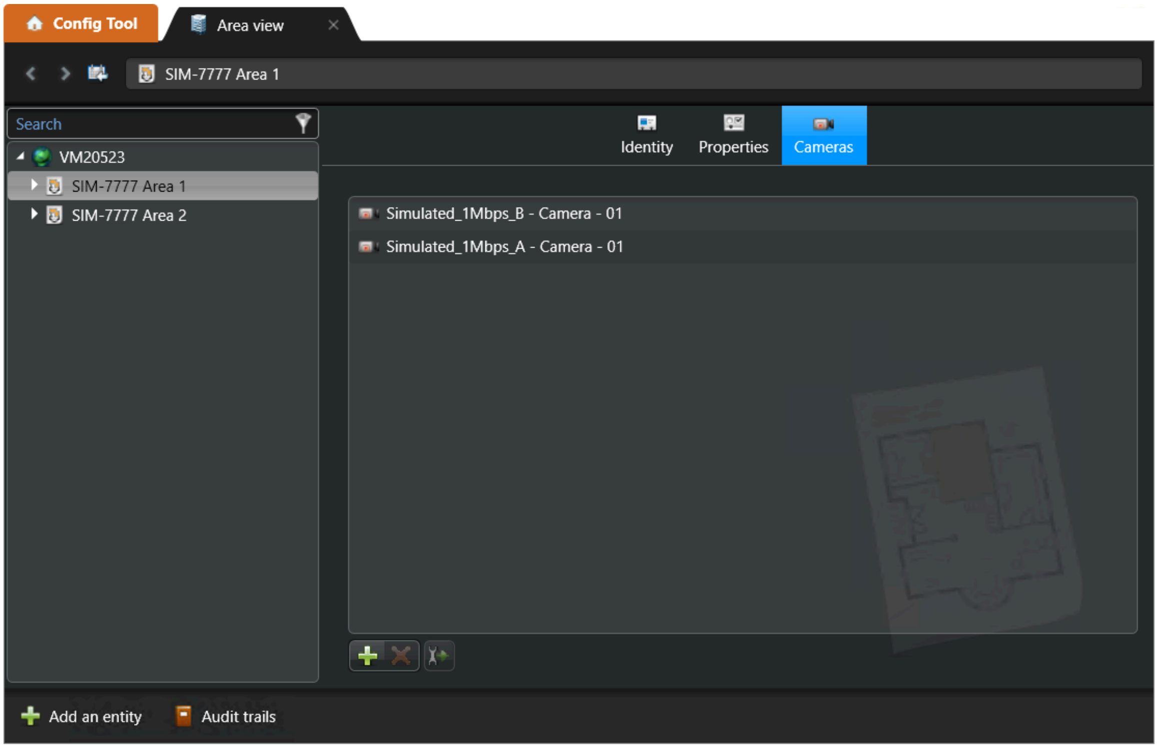
1 From the Config Tool home page, open the *Area view* task.

2 Select the intrusion detection area to configure, and then click the **Cameras** tab.

3 Click **Add an item** (➕).

4 In the dialog box that opens, select a camera, and then click **OK**.

The camera is added to the **Cameras** list.



Simulated_1Mbps_B - Camera - 01
Simulated_1Mbps_A - Camera - 01

5 Click **Apply**.

Assigning cameras to intrusion detection inputs

To display a camera feed in a Security Desk monitoring tile when an intrusion input event occurs, such as *Glass break*, you can assign cameras to intrusion detection inputs.

What you should know

You can assign a camera to an intrusion detection input either from the *Intrusion detection* task or from the *Area view* task.

When you associate cameras to an intrusion detection area and related inputs and an event occurs, the system shows the most relevant camera first. For example, when an input event occurs, such as a motion detected, the camera assigned to the input is displayed in the first tile and the cameras assigned to the area are shown next. However, when an area event occurs, such as area disarmed, only the cameras assigned to the area are displayed. When there are multiple videos attached to an event, you can cycle or unpack the tile to see them.

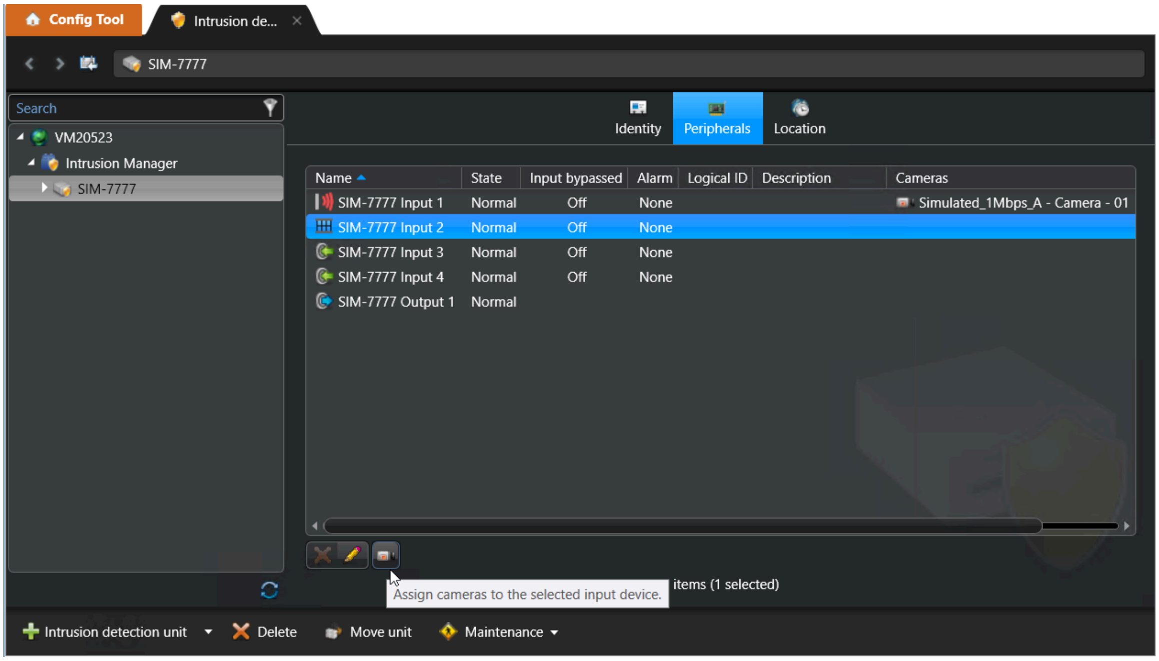
To assign cameras to an intrusion detection input from the *Intrusion detection* task:

1 From the Config Tool home page, open the *Intrusion detection* task, expand the **Intrusion Manager** role, and then select an intrusion detection unit from the list.

2 On the *Peripherals* page, click the camera button ().

3 Click **Add a camera** (), select a camera from the list, and click **OK**.

4 Click **OK** > **Apply**.



Name	State	Input bypassed	Alarm	Logical ID	Description	Cameras
SIM-7777 Input 1	Normal	Off	None			Simulated_1Mbps_A - Camera - 01
SIM-7777 Input 2	Normal	Off	None			
SIM-7777 Input 3	Normal	Off	None			
SIM-7777 Input 4	Normal	Off	None			
SIM-7777 Output 1	Normal					

Assign cameras to the selected input device.

items (1 selected)

To assign cameras to an intrusion detection input from the *Area view* task:

1 From the Config Tool home page, open the *Area view* task.

2 Select the intrusion detection area to configure, and click the **Properties** tab.

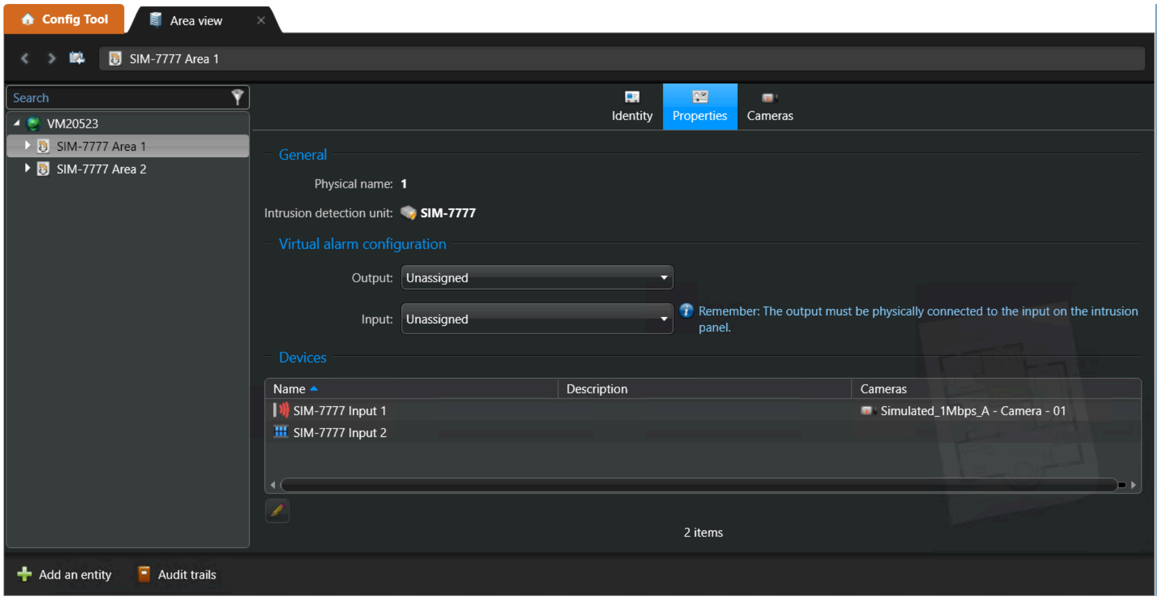
3 From the **Devices** list, select an input, and then click **Edit the item** ().

The *Assign cameras to inputs* dialog box opens.

4 If you have cameras associated to the intrusion detection area, select a camera, then click **OK**.

5 To add a camera that is not associated to the area, click **Add an item** (➕), select a camera, and then click **OK**.

6 Click **OK** > **Apply**.



General

Physical name: **1**

Intrusion detection unit: **SIM-7777**

Virtual alarm configuration

Output: Unassigned

Input: Unassigned

Remember: The output must be physically connected to the input on the intrusion panel.

Devices

Name	Description	Cameras
SIM-7777 Input 1		Simulated_1Mbps_A - Camera - 01
SIM-7777 Input 2		

2 items

Configuring Security Center to trigger intrusion alarms on any intrusion panel

You can configure Security Center to trigger alarms on intrusion panels, regardless of their model. This is done by physically connecting the input pin associated to an alarm to an output relay on the panel, and configuring the pair as a *virtual alarm* in Config Tool.

Before you begin

Do the following preparation on the intrusion panel:

- Associate an input pin to an alarm on the intrusion panel. You might need a proprietary software.
- Physically connect that input pin to an output relay on the same panel.

What you should know

We use the *Trigger intrusion alarm* action to activate alarms on intrusion detection areas. But not all intrusion panel models support the alarm activation from an external source. For panels that do not support this feature, a workaround exists. The solution is to physically connect an output to an alarm input on the intrusion panel. We call this configuration, a *virtual alarm*, and the input that you physically connected to the output, a *virtual input*. When the virtual alarm is configured, Security Center sends a signal to the output that is physically connected to the alarm input when the *Trigger intrusion alarm* action is used, thus activating the intrusion alarm.

To configure Security Center to raise virtual alarms:

1 From the Config Tool home page, open the *Area view* task.

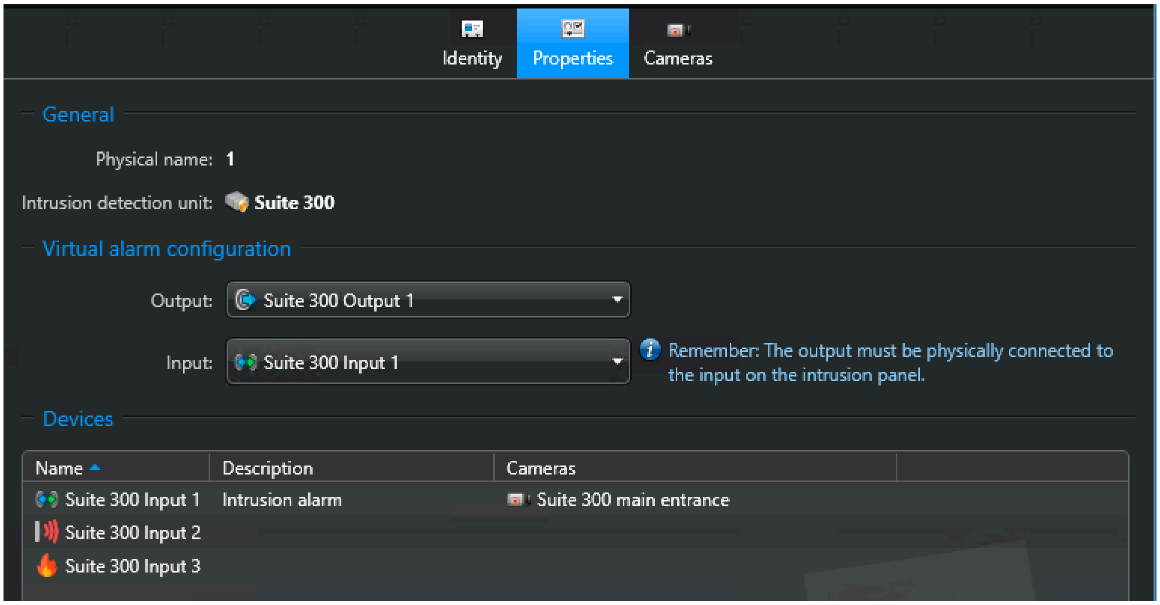
2 Select the intrusion detection area ( ) to configure, and click the **Properties** tab.

3 From the **Output** list, select the output relay that is physically connected to the input pin.

4 From the **Input** list, select the input pin that is physically connected to the output relay.

5 Click **Apply**.

The input icon changes to , meaning that it is now a virtual input.



Physical name: 1

Intrusion detection unit: Suite 300

Output: Suite 300 Output 1

Input: Suite 300 Input 1

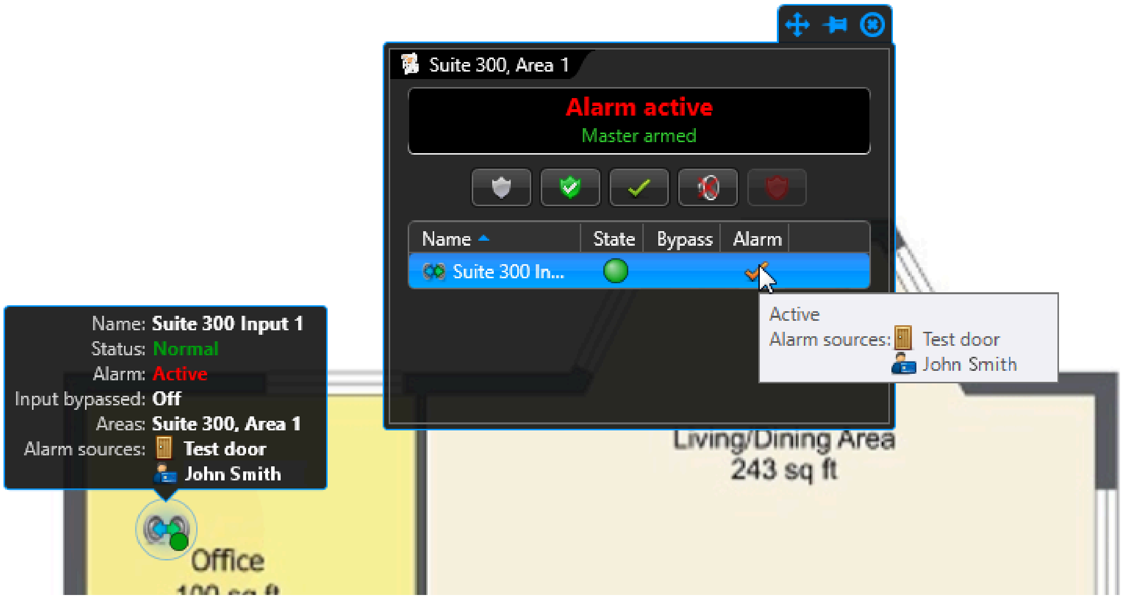
Remember: The output must be physically connected to the input on the intrusion panel.

Name	Description	Cameras
Suite 300 Input 1	Intrusion alarm	Suite 300 main entrance
Suite 300 Input 2		
Suite 300 Input 3		

Now, you can configure event-to-actions to trigger the action *Trigger intrusion alarm* on this intrusion detection area. The source entity of the event used to trigger the intrusion alarm will be shown as the alarm source on a map if you monitor this intrusion detection area on a map, and as the initiator of the *intrusion detection area alarm activated* event in the *Intrusion detection area activities* report.

Example

Suppose you create an event-to-action to trigger the *Trigger intrusion alarm* action on *Access denied (at a door)* event, the door where access is being denied would be shown as the alarm source in your *Monitoring* task and on the map. If on top of that, you configure a second event-to-action to trigger the same action on *Access denied (to cardholder)* event, the cardholder would also be shown as the alarm source when the event occurs.



Suite 300, Area 1

Alarm active

Master armed

Name	State	Bypass	Alarm
Suite 300 In...	●		✓

Active
Alarm sources: Test door
John Smith

Name: Suite 300 Input 1
Status: Normal
Alarm: Active
Input bypassed: Off
Areas: Suite 300, Area 1
Alarm sources: Test door
John Smith

Moving intrusion detection units to a different Intrusion Manager

If you want a different Intrusion Manager role to manage and control an intrusion detection unit, for load balancing or another purpose, you can move the unit to another Intrusion Manager using the *Move unit* tool.

Before you begin

- The Intrusion Manager role must be on the same LAN as the intrusion detection unit it controls.
- If the unit extension is not created automatically, you must add it.
- If the intrusion panel is physically connected to a serial port on the server hosting the original role, make sure you do the same with the server hosting the new role.

To move an intrusion detection unit to a different Intrusion Manager:

1. From the homepage, click **Tools** > **Move unit**.
2. From the **Unit type** list, select **Intrusion detection unit**.
3. Select the units you want to move.
4. Under **Intrusion Manager**, select the new Intrusion Manager role to control the unit.
5. Click **Move** > **Close**.

Related Topics

Intrusion Manager configuration tabs on page 1363

Part VIII

Config Tool reference

This part includes the following chapters:

- Chapter 57, " Entity types " on page 1227
- Chapter 58, " Role types " on page 1304
- Chapter 59, " Administration tasks " on page 1394
- Chapter 60, " Events and actions " on page 1409

57

Entity types

This section includes the following topics:

- "ALPR unit - Properties tab" on page 1278
- "Macro configuration tabs" on page 1279
- "Monitor group - Monitors tab" on page 1280
- "Network - Properties tab" on page 1281
- "Output behavior - Properties tab" on page 1282
- "Overtime rule configuration tabs" on page 1283
- "Parking facility - Properties tab" on page 1284
- "Partition - Properties tab" on page 1285
- "Patroller - Properties tab" on page 1286
- "Permit - Properties tab" on page 1287
- "Permit restriction configuration tabs" on page 1288
- "Schedule - Properties tab" on page 1289
- "Scheduled task - Properties tab" on page 1290
- "Server - Properties tab" on page 1291
- "Tile plugin - Properties tab" on page 1292
- "User configuration tabs" on page 1293
- "User group configuration tabs" on page 1296
- "Video unit - Identity tab" on page 1298
- "Video unit - Properties tab" on page 1299
- "Video unit - Peripherals tab" on page 1301
- "Virtual zone configuration tabs" on page 1303

Common configuration tabs

Some of the configuration tabs are commonly used by most Security Center entities.

Identity tab

The **Identity** tab provides descriptive information about the entity, such as its name, description, logical ID, and lets you jump to the configuration page of related entities.

- **Type:** Entity type.
- **Icon:** Icon assigned to the entity in the *Area view*, **Identity** tab, on maps, and so on.

  Click the **Change icon** drop-down to change the icon settings:

  - Click **Browse...** to navigate to and select your own preferred custom icon.
  - Click **Reset** to restore the default icon.

  NOTE: Doors have two icons to indicate if they are open or closed.
- **Name:** Name for the entity Security Center. It is recommended to create a unique and descriptive name for each entity. In some cases, a default name is created, which you can change. Entity names are editable, except in the following cases:
  - **Server entities:** The entity name corresponds to the machine name and cannot be changed.
  - **Federated entities:** The entity name is defined on the original system and cannot be changed on the federation.
- **Description:** Optional information about the entity.
- **Logical ID:** Unique number assigned to the entity to easily identify them in the system (mainly for CCTV keyboard operations).
- **Relationships:**

  List of relationships between this entity and other entities on the system.

  You can use the command buttons found at the bottom of the list to manage the relationship between this entity and other entities in the system.

  - To add a new relationship, click ➕.
  - To remove a relationship, select a related entity, and click ✖.
  - To jump to a related entity's configuration page, select the entity, and click ➡.
- **Specific information:** Certain entity types, such as video units, might show additional information in this tab.

Cameras tab

The **Cameras** tab allows you to associate cameras to the entity so that when it is viewed in Security Desk, the cameras are displayed instead of the entity icon.

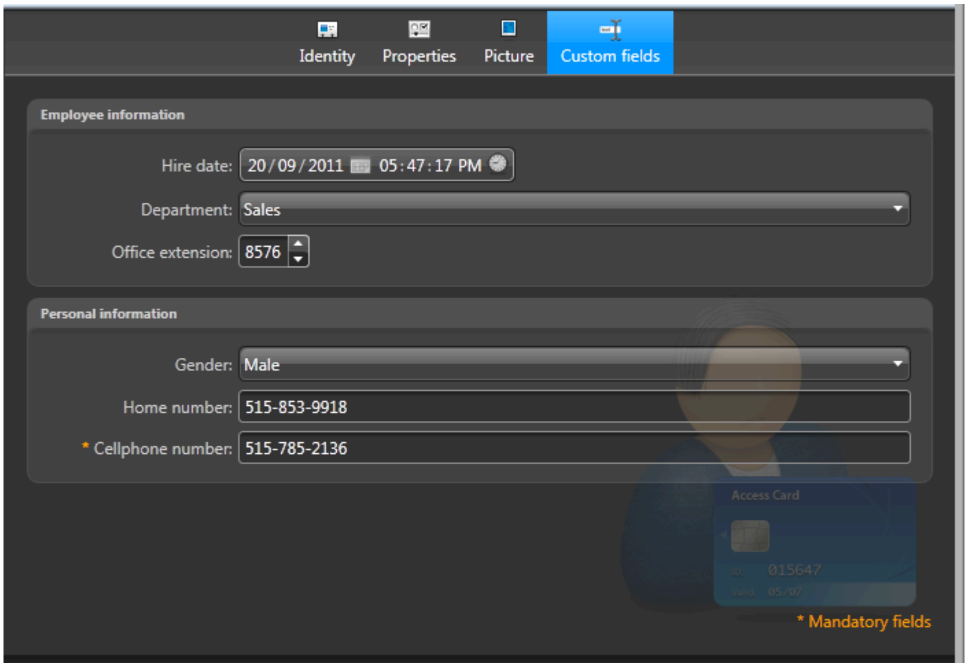
From this tab you can perform the following actions:

- To add a camera, click ➕.
- To remove the selected camera, click ✖.

Custom fields

The **Custom fields** tab lets you view and modify the custom fields defined for the entity. The sample screen capture below is that of a *cardholder* entity.

This tab only appears when custom fields are created for that type of entity.



Employee information

Hire date: 20/09/2011 05:47:17 PM

Department: Sales

Office extension: 8576

Personal information

Gender: Male

Home number: 515-853-9918

* Cellphone number: 515-785-2136

* Mandatory fields

In the above example, five custom fields have been defined for the cardholder entity, separated in two groups:

- Employee information
  - Hire date
  - Department
  - Office extension
- Personal information
  - Gender
  - Home number
  - Cellphone number (flagged as mandatory)

Location tab

The **Location** tab provides information regarding the time zone and the geographical location of the entity. It does not affect the actual location of entities on maps.

- **Time zone:** The time zone is used to display the entity events in the entity’s local time zone. In Security Center, all times are stored in UTC in the *databases*, but are displayed according to the local time zone of the entities. The local time of the entity is displayed below the time zone selection.
- **Location:** The geographical location (latitude, longitude) of the entity. This location setting is only used for the following types of entities:
  - For video units, the location is used for the automatic calculation of the time the sun rises and sets on a given date.
  - For fixed ALPR units that are not equipped with a GPS receiver, the geographical location is used to plot the ALPR events (*reads* and *hits*) associated to the ALPR unit on the map in Security Desk.

Access control unit - HID - Identity tab

This section lists the settings found in the HID access control unit **Identity** tab, in the *Access control* task. This tab lets you view hardware-specific information, in addition to the standard entity information (name, description, logical ID, and so on).

- **Manufacturer:** Manufacturer of the access control unit.
- **Product type:** Model of the access control unit.
- **MAC address:** MAC address of the access control unit.
- **Firmware version:** Current firmware version installed on the access control unit.

  NOTE: The **Upgrade** (☢) button only appears if it is an HID EVO unit.
- **Proposed:** Displays the recommended firmware version. If the firmware version is the same as the proposed version, it will display *Up to date*.
- **Number of credentials:** (Only when **Secure mode** is enabled) Number of credentials stored on the unit.

  (When **Secure mode** is disabled) Number of credentials stored on the unit versus the total number of credentials the unit can store, based on the available memory and the average number of bytes per credential.
- **Main memory:** (Only when **Secure mode** is disabled) Available memory on the unit.
- **Secondary memory:** (Only when **Secure mode** is disabled) Available secondary memory on the unit (when it applies).

Access control unit - HID - Properties tab

This section lists the settings found in HID access control unit **Properties** tab, in the *Access control* task. This tab lets you update the connection parameters after the HID unit has been discovered, such as the logon credentials, and the usage of certain specific inputs.

Connection settings

This section shows the connection parameters for the Access Manager to communicate with the unit. These settings are initialized when the HID unit is added to your system. Do not change these settings unless you changed them on the unit through the unit's web page or using the HID Discovery GUI after the unit was enrolled, or one or our representatives instructs you to do so.

- **Username and password:** Username and password used to log on to the HID unit.
- **Use translated host address:** Select this option when there is a NAT router between the unit and its Access Manager. The NAT router's IP address that is visible from the unit would be set here.
- **Static IP:** Select this option and configure the IP address, Gateway and Subnet mask manually if the HID unit uses a fixed IP address (recommended).
- **Use DHCP:** Select this option if the HID unit will be assigned its IP configuration by a DHCP server. When using the DHCP option, the DHCP server must be configured to always assign the same IP address to the unit.

General settings

This section displays the general settings of the HID unit.

- **Server mode:** This option is always greyed out because HID units do not support *server mode*.
- **Secure mode:** Enabling secure mode disables the insecure protocols FTP and Telnet. It also makes the connection between the Access Manager and HID units less susceptible to network impairments. This option is only available if the HID unit meets the firmware requirement for secure mode.
- **Monitor AC Fail :** Select this option if the *AC fail* input is being used to monitor AC failures or for some other general purpose.
- **Monitor battery fail :** Select this option if the *Battery fail* input is being used to monitor the backup battery or for some other general purpose.
- **Reader supervision:** Select this option to enable reader supervision (ability to detect reader disconnection or power loss in Security Desk and Config Tool). For this feature to work, all readers connected to this HID unit must be configured for supervision. You must also enable the supervision mode on each physical reader by presenting the HID configuration card.
- **Timeout:** (Only if *Reader supervision* is selected) Timeout used to detect that the reader is offline. We recommend that you set the timeout value to be at least three times the cycle time of the *I'm alive* signal (default=10 seconds) configured on the reader.

Related Topics

Enabling reader supervision on HID VertX controllers on page 773

Access control unit - HID - Synchronization tab

This section lists the settings found in HID access control unit **Synchronization** tab, in the *Access control* task. This tab lets you configure the type of synchronization you want between the unit and its Access Manager.

- **Last update:** Indicates the date and time of the last successful synchronization with the unit.
- **Next update:** Date and time of the next scheduled synchronization with the unit.
- **Configuration expires on:** Depends on whether temporary access rules are used or not.
    - If no temporary access rules are used: Indicates the date and time when the unit can no longer fully function independently of the Access Manager. This is due to the limited scheduling capability of the

      HID access control unit. You need to synchronize before the expiration date to ensure that the unit works properly on its own.
    - If temporary access rules are used: Indicates the date and time the next synchronization should happen based on the rule activation and expiration date and time of the temporary access rules.

  CAUTION: HID VertX units expire after one year. Past the expiration date, the unit stops working properly.
- **Synchronize:** Click this button to send everything that changed since the last synchronization to the unit. This operation may cause a short service disruption if there are changes to door unlock schedules.
- **Synchronize and restart:** Click this button to send the full configuration to the unit and restart the unit. This operation will cause service disruption.

Synchronization options

You can select how frequently you want the unit synchronization to occur.

- **Automatically:** This is the recommended setting.

  Any configuration change is sent to the access control unit 15 seconds after the change is saved by the Config Tool, Web Client, Genetec Web App, or Security Desk. Only configurations that affect that particular unit are sent.
- **Daily:** The unit is synchronized daily, at the specified times.
- **Every:** The unit is synchronized weekly, at the specified day and time.
- **Manual:** The unit is only synchronized when you click **Synchronize now**.

  Make sure you synchronize the unit before the configuration expires.

Access control unit - HID - Peripherals tab

This section lists the settings found in HID access control unit **Peripherals** tab, in the *Access control* task. In this tab, you can view and change the name and settings of the peripherals (readers and I/O devices) controlled by the unit.

The informations displayed on this page are:

- **Name:** Name of the interface module or peripheral. The peripherals are displayed in a hierarchical view by default.

  Click **Viewing mode** () to select the *Flat view* if it is your preference.
- **Type:** Peripheral type: *In* (Input), *Out* (Output), *Reader*. Blank if it is not a peripheral.

  (Output relays only) Click **Trigger output** () at the bottom of the list to send an output behavior (*Active*, *Normal*, or *Pulse*) to the selected device.
- **State:** Live peripheral state: *Active*, *Normal*, *Shunted* (inputs only), *Trouble* (inputs only), or *Unknown*.

  Use this column to test the connected interface modules and validate the wiring configuration of the I/O devices.
- **Additional info:** Settings specific to the type of peripheral.

  Double-click a peripheral, or click **Edit** () at the bottom of the list to edit the settings of the selected peripheral.
- **Controlling:** Entity (door, elevator, zone) controlled by this peripheral.

  Click **Jump to** () at the bottom of the list to view the configuration tabs of the entity controlled by the selected peripheral.
- **Logical ID:** (Hidden by default) Logical ID assigned to this peripheral for ease of reference in macros and SDK programs.
- **Physical name:** (Hidden by default) Static name assigned to this peripheral by the system.

TIP: Information on this page is also available to Security Desk users through the *System status* task, when monitoring peripherals.

Editable reader settings

The editable reader settings are:

- **Name:** Reader name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Shunted:** This feature is not supported by HID units.
- **Type of reader:** Select one of the following.
  - *Wiegand*
  - *Clock & Data*
  - *Wiegand (Dorado)*
  - *Clock & Data (Dorado)*

Discover interfaces

If the HID unit is operating with **Secure mode** enabled, the new interfaces you attach to the unit will not appear automatically in the **Peripherals** tab after rebooting the unit. To show them, click the **Discover interfaces** () button at the bottom of the page. Note that clicking this button causes the unit to go offline briefly.

Editable input settings

The editable input settings are:

- **Name:** Input device name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Shunted:** Select this option to ignore the inputs. Once shunted, the state of the input remains at *Normal*, regardless how you trigger it.
- **Debounce:** The amount of time an input can be in a changed state (for example, changed from *Active* to *Normal*) before the state change is reported. This option filters out signals that are unstable.
- **Contact type/ Presets:** Set the normal state of the input contact and its supervision mode.
  - **Not supervised / Normally closed:** The normal state of the input contact is closed, and the access control unit does not report if the input is in the trouble state.
  - **Not supervised / Normally open:** The normal state of the input contact is open, and the access control unit does not report if the input is in the trouble state.
  - **4-state supervised / Normally closed:** The normal state of the input contact is closed, and the access control unit reports when the input is in the trouble state.
  - **4-state supervised / Normally open:** The normal state of the input contact is open, and the access control unit reports when the input is in the trouble state.
- **Contact type/ Manual:** Manual settings. Allows you to set your custom range of values for *Active* and *Normal* input states.

Editable output settings

The editable reader settings are:

- **Name:** Output device name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Minimum time (Action):** If a relay is being used as part of a zone (either hardware or virtual), set a minimum number of seconds the relay stays closed when triggered by an event (for example, *Request to exit*).

Access control unit - Synergis - Identity tab

This section lists the settings found in the Synergis™ access control unit **Identity** tab, in the *Access control* task. This tab lets you view hardware-specific information, in addition to the standard entity information (name, description, logical ID, and so on).

- **Manufacturer:** Manufacturer of the access control unit.
- **Product type:** Model of the access control unit.
- **MAC address:** MAC address of the access control unit.
- **Discovery port:** Port used by the Access Manager to talk to this unit. It must match one of the discovery ports configured for the Genetec™ Synergis extension of the Access Manager.
- **Firmware version:** Current firmware version installed on the access control unit.
- **Platform version:** Current platform (cumulative security rollup) version installed on the unit.
- **Number of cardholders:** Number of cardholders (distinct credentials) stored on the unit.

Access control unit - Synergis - Properties tab

This section lists the settings found in Synergis™ access control unit **Properties** tab, in the *Access control* task. This tab lets you update the connection parameters after the Synergis unit has been discovered, such as its logon credentials.

Connection settings

The connection settings are initialized when the Synergis unit is enrolled in your system. Do not change these settings unless you changed the unit's settings with the Synergis™ Appliance Portal after the unit has been enrolled, or one of our representatives instructs you to do so.

- **Web address:** Web address for contacting the Synergis unit's portal. If you change the web address to use the unit's IP address after it has been enrolled using its hostname, make sure to delete the IPV6 address from the **Accepted Access Manager connections** list on the *Network* page of the unit's portal. If the IPV6 address is not removed from the list, the next time the unit is disconnected, it will not reconnect.
- **Username and Password:** Logon username and password.
- **Change unit password:** Click to update the password.
- **Unit password history:** Displays the details of the five previous password change attempts made through Security Center, including the date, the previous password, and the new password.
- **Use DHCP:** Do not change this parameter unless asked by a Genetec Technical Assistance representative. This parameter is reset every time the Access Manager reconnects to the Synergis unit.
- **Ignore web proxy:** Select this option to instruct the Access Manager to ignore the Proxy Server settings on the server currently hosting the role. Clear this option to instruct the Access Manager to follow the Proxy Server settings (default=cleared).
- **Thumbprint:** The thumbprint of the certificate on the Synergis unit. This field is automatically updated to reflect the new certificate when you click the **Reset trusted certificate** button.
- **Reset trusted certificate:** (Only enabled when the unit is offline) Click this button to make the Access Manager forget the trusted certificate for this unit so that the new one can be accepted. Use this feature when you changed the digital certificate of the unit after it has been enrolled.

Access control unit - Synergis - Portal tab

Clicking the Synergis™ unit **Portal** tab in the *Access control* task opens the Synergis unit's web-based interface (Synergis™ Appliance Portal), which allows you to configure and maintain the unit.

For more information about the Synergis™ Appliance Portal and what tasks you can perform in it, see the *Synergis™ Appliance Configuration Guide*.

Related Topics

Access control unit - Synergis - Hardware tab on page 1239

Access control unit - Synergis - Hardware tab

The Synergis™ unit *Hardware* page in the *Access control* task allows you configure the interface modules connected to the Synergis unit.

For more information about the integrations supported by the Synergis unit, see the *Synergis™ Softwire Integration Guide*.

Related Topics

Access control unit - Synergis - Portal tab on page 1238

Access control unit - Synergis - Synchronization tab

This section lists the settings found in the Synergis™ access control unit **Synchronization** tab, in the *Access control* task. This tab lets you manually trigger the synchronization between the unit and its Access Manager.

- **Last update:** Indicates the day and time of the last successful synchronization between the unit and its Access Manager.
- **Next update:** Does not apply. Changes affecting the Synergis unit are always sent automatically the moment they are saved.
- **Configuration expires on:** The synchronized data of the Synergis unit never expires because it understands the scheduling scheme used in Security Center.
- **Synchronize:** Click this button to send everything that changed since the last synchronization to the unit.

  This action always performs a full synchronization. A Synergis unit synchronization does not cause any service disruption.

Access control unit - Synergis - Peripherals tab

This section lists the settings found on the Synergis™ access control unit *Peripherals* page in the *Access control* task. This page displays in a hierarchical view, all the interface modules attached to the unit, along with any downstream panels attached to them.

From the *Peripherals* page, you can add and delete interface modules, and change the name and settings of the peripherals (readers and I/O devices) attached to the unit.

The information displayed on this page are:

- **Name:** Name of the interface module or peripheral. The peripherals are displayed in a hierarchical view by default.

  Click **Viewing mode** (👁) to select the *Flat view* if it is your preference.
- **Type:** Peripheral type: *In* (Input), *Out* (Output), *Reader*. Blank if it is not a peripheral.

  (Output relays only) Click **Trigger output** (➡) at the bottom of the list to send an output behavior (*Active*, *Normal*, or *Pulse*) to the selected device.
- **State:** Live peripheral state: *Active*, *Normal*, *Shunted* (inputs and readers only), *Trouble* (inputs only), or *Unknown*.

  Use this column to test the connected interface modules and validate the wiring configuration of the I/O devices.
- **Additional info:** Settings specific to the type of peripheral.

  Double-click a peripheral, or click **Edit** (✏) at the bottom of the list to edit the settings of the selected peripheral.
- **Controlling:** Entity (door, elevator, zone) controlled by this peripheral.

  Click **Jump to** (➡) at the bottom of the list to view the configuration tabs of the entity controlled by the selected peripheral.
- **Logical ID:** (Hidden by default) Logical ID assigned to this peripheral for ease of reference in macros and SDK programs.
- **Physical name:** (Hidden by default) Static name assigned to this peripheral by the system.

TIP: Information on this page is also available to Security Desk users through the *System status* task, when monitoring peripherals.

Interface modules you can add and delete

You can only add and delete Mercury controllers (EP, LP, and M5-IC) attached to your Synergis unit from the *Peripherals* page. For all other types of interface modules, you must add them either through the *Hardware* page in Config Tool or in the Synergis™ Appliance Portal.

Editable reader settings

The editable reader settings are:

- **Name:** Reader name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Shunted:** Select this option to ignore the reads.

  This action can also be issued from Security Desk.
- **Type of reader:** Select the type corresponding to your reader. The list of available reader types depends on the type of interface module you have. Selecting the *Custom* reader type allows you to configure all the reader options manually.

Editable input settings

The editable input settings are:

- **Name:** Input device name.
- **Description:** (Read only) Input description.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Shunted:** Select this option to ignore the inputs. Once shunted, the state of the input remains at *Normal*, regardless how you trigger it.

  NOTE: Input Tamper and Input PowerMonitor cannot be configured. These inputs only support normally closed (NC) switch contacts and are unsupervised. To make sure unused inputs are not seen as active in Security Center, connect the terminals with a short piece of wire.
- **Debounce:** The amount of time an input can be in a changed state (for example, changed from *Active* to *Normal*) before the state change is reported. This option filters out signals that are unstable.
- **Contact type:** Set the normal state of the input contact and its supervision mode.
  - **Not supervised/Normally closed:** The normal state of the input contact is closed, and the access control unit does not report that the input is in the trouble state.
  - **Not supervised/Normally open:** The normal state of the input contact is open, and the access control unit does not report if the input is in the trouble state.
  - **4-state supervised/Normally closed:** The normal state of the input contact is closed, and the access control unit reports when the input is in the trouble state.
  - **4-state supervised/Normally open:** The normal state of the input contact is open, and the access control unit reports when the input is in the trouble state.
  - **Custom:** Allows you to set your custom range of values for *Active* and *Normal* input states. The actual values are set in the Mercury controller Advanced settings.

Editable output settings

The editable reader settings are:

- **Name:** Output device name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.

Access rule - Properties tab

This section lists the settings found in the Access rule **Properties** tab, in the *Access control* task.

In the *Properties* tab, you can link the 3 W’s for an access rule: the “Who”, “When” and “What”. For example, “All Employees”, “Office Hours”, and “Access Granted”.

- **Schedule:** Choose when this access rule is active.
- **Activation:** (Only for temporary access rules) Activation date and time, or when the rule schedule starts to apply.
- **Expiration:** (Only for temporary access rules) Expiration date and time, or when the rule schedule stops to apply.
- **When the schedule is active:** Select what the rule does (grant or deny access to cardholders) when it is active.
- **Cardholders affected by this rule:** Select the cardholders and cardholder groups affected by this rule.

Alarm configuration tabs

This section lists the settings found in Alarm configuration tabs, in the *Alarm* task.

Alarm - Properties tab

In the *Properties* tab, you can define the essential alarm properties.

- **Priority:** Priority of the alarm (1-255), based on the urgency of the situation. Higher priority alarms are displayed first in Security Desk.
- **Recipients:** Users, user groups, and analog monitor groups who are notified when the alarm occurs, and are responsible for responding to the alarm situation.
- **Broadcast mode:** How the alarm recipients are notified about the alarm.
  - **All at once:** (Default) All recipients are notified at the same time, immediately after the alarm is triggered.
  - **Sequential:** The recipients are notified individually, each after a specified delay (in seconds) calculated from the time the alarm is triggered. If the recipient is a user group, all members of the user group are notified at the same time.
- **Attached entities:** Entities that help describe the alarm situation (for example, cameras, area, doors, alarm procedure, and so on). When the alarm is received in Security Desk, the attached entities can be displayed one after another in a sequence or all at once in the *canvas*, to help you review the situation. If a composite entity is attached to the alarm, the entities that compose it are also attached to the alarm. For example, if a door entity is attached to the alarm, the cameras associated to the door are also attached to the alarm.
- **Video display option:** If cameras are attached to the alarm, select whether to display live video, playback video, a series of still frames, or a combination of the three when the alarm is triggered.
  - **Live:** Display live video.
  - **Playback:** Display playback video.
  - **Live and playback:** Rotate between displaying live and playback video.
  - **Live and still frames:** Rotate between displaying live video and a series of still frames.
  - **Still frames:** Display a series of still frames.
- **Still frame durations:** Select whether you want each still frame to be displayed for the same duration or an independent duration of time.
  - **Same durations:** Display each still frame for the same duration of time.
    - **Number of frames:** Select the number of still frames to display within total content cycling duration.
    - **Play:** Select how many seconds before the alarm was triggered to start the first still frame.
  - **Independent durations:** Display each still frame for an independent duration of time.
    - **Relative time:** Select how many seconds before or after the alarm was triggered the still frame displays.
    - **Duration:** Select how long the still frame is displayed for.
- **Content cycling:** Turn this option on to automatically rotate the entities that are attached to the alarm in a display tile for an equal amount of time. The attached entities are listed in the order that they are displayed in Security Desk.

Alarm - Advanced tab

In the *Advanced settings* tab, you can configure the optional alarm properties.

- **Reactivation threshold:** The minimum time Security Center needs to wait after triggering this alarm before it can be triggered again. This option prevents the system from repeatedly triggering the same alarm before it is resolved.
- **Alarm procedure (URL):** Enter the URL or the web page address corresponding to the *alarm procedure*, which provides alarm handling instructions to the operators. The web page is displayed when the user clicks *Show alarm procedure* (📋) in the alarm widget in Security Desk.
- **Schedule:** Assign schedules to define when this alarm is in operation. You can assign more than one schedule. Outside the periods defined by these schedules, triggering this alarm has no effect.
- **Automatic acknowledgment:** Turn this option on to let the system automatically acknowledge this alarm if no one acknowledges it before the specified time (in seconds). This option is recommended for low-priority alarms that serve to alert the security operator, but do not require any action. When this option is turned off, the system follows the **Auto ack alarms after** option configured at the system level in Server Admin.

  NOTE: Automatic acknowledgment does not apply to alarms that have an active condition attached. To acknowledge those alarms, you need to forcibly acknowledge them (which requires the *Forcibly acknowledge alarms* privilege). For more information on acknowledging alarms, see the *Security Center User Guide*.
- **Create an incident on acknowledgment:** Turn this option on to prompt the Security Desk user to report an *incident* every time they acknowledge an alarm.

  NOTE: Turning this option on turns the *automatic acknowledgment* option off.
- **Automatic video recording:** Turn this option off (default=on) if you do not want to start recording video when the alarm is triggered.
- **Protect recorded video:**
- **Alarm sound:** Select the sound to play when a new alarm occurs. This sound overrides the default sound configured in **Security Desk** > **Options** > **Alarms**.

  NOTE: For a sound to play when an alarm is triggered, you must click **Security Desk** > **Options** > **Alarms** and enable the **Play a sound** option.
- **Color:** Select a color for the alarm. The color is used for the overlay of the alarm video when it is displayed in a tile in the *Alarm monitoring* or *Monitoring* task, as well as when the alarm is triggered on a map.

Analog monitor - Properties tab

This section lists the settings found in the Analog monitor **Properties** tab, in the *Video* task.

The *Properties* tab lets you configure the video stream usage (or function) and specific network settings for the analog monitor.

Video

In the *Video* section, you can configure settings that affect the quality the video.

- **Stream usage:** Select the video stream to use for cameras displayed in the analog monitor. This option is only available for decoders capable of generating multiple video streams. The stream usage options are the following:
- **Live:** Default stream used for viewing live video in Security Desk.
- **Recording:** Stream recorded by the Archiver for future investigation.
- **Remote:** Stream used for viewing video when the bandwidth is limited.
- **Low resolution:** Stream used instead of the *Live* stream when the tile used to view the stream in Security Desk is small.
- **High resolution:** Stream used instead of the *Live* stream when the tile used to view the stream in Security Desk is large.
- **Analog format:** Select NTSC (National Television System Committee) or PAL (Phase Alternating Line) analog format for the video signal. PAL format generally streams video at a lower frame rate, but at a higher resolution.
- **Display camera name:** Turn this option on if you want the camera name to be shown when it is displayed in the analog monitor in a Security Desk tile.

Network settings

In the *Network settings* section, you can configure the connection type used by the video decoder.

- **UDP port:** Port number used when the connection type is unicast *UDP*. If the encoder supports multiple video streams, this parameter is different for each stream.
- **Connection type:** Defines how communication is established between the Archiver and the unit for sending or receiving video streams. Each device on the same unit could support different connection types.
- **Best available:** Lets the Archiver select the best available connection type for the stream. The best available types rank in this order, according to availability: *Multicast*, *UDP*, and *TCP*. When the stream is requested for recording only, multicast is removed from the list, so the best available types start with UDP.
  - **Multicast:** Communication between a single sender and multiple receivers on a network. This is the preferred connection type. In this mode, multiple users in multiple locations can receive the same video transmission simultaneously from a same source, using the bandwidth only once. Most video units are capable of multicast transmissions.
  - **UDP:** Forces the stream to be sent in UDP to the Archiver. The stream must be formatted using the RTP protocol.
  - **TCP:** Forces the stream to be sent in *TCP* to the Archiver. Here, TCP is taken in the broad sense. For some types of cameras, the Archiver establishes a TCP connection to the unit and receives the stream in a proprietary protocol. For others, the stream is sent over HTTP. Typically, the stream is not formatted according to the RTP protocol by the unit. The Archiver has to convert the stream to the RTP protocol to be archived or retransmitted to the system.

Hardware

In the *Hardware* section, you can associate other hardware devices (PTZ motor, Speaker, Microphone, and so on) to this analog monitor. When the decoder is added to the system, all hardware devices belonging to the same unit are configured by default. You can manually associate the analog monitor to other devices, according to how they are physically connected.

Area configuration tabs

This section lists the settings found on the configuration pages of areas in the *Area view* task.

Area - Identity

On the *Identity* page, you can configure whether or not the area is used for access control, in addition to the standard entity information (name, description, logical ID, and so on).

- **Access control:** When this option is on, the **Properties** and **Advanced** tabs are shown, and you can configure the area as a *secured area*. When this option is off, the area is ignored by the Access Manager role.

  Adding a door to the area automatically sets the **Access control** option to **ON** and makes it read-only. If

  you only configure elevators for the area, the option is automatically set to **ON**, but can still be turned off. **NOTE:** This option is only visible when Synergis™ is enabled as a feature in your license.

Area - Properties

On the *Properties* page, you can define who has access to the area through its perimeter doors.

NOTE: This page is only visible when Synergis is enabled as a feature in your license, and the **Access control** option on the *Identity* page of the area is set to **ON**.

- **Access rules:** Define who has access to the area and when. Each rule can be applied to one or both sides of the doors.
  - **Access rules:** Add access rules to grant or deny access to the area to cardholders and cardholder groups based on a schedule.
  - **Cardholders:** Add cardholders and cardholder groups to define who has access to the area at all times.

    NOTE: Only grant access directly to cardholders for temporary situations or exceptions. If a group of cardholders should be allowed to access the area at all times as a regular setup, define an access rule with the *Always* schedule.
- **Doors:** Define the *Perimeter* and *Captive* doors of the area. Perimeter doors are used to enter and exit an area, and help to control access. Captive doors are doors inside the area. By correctly setting the door sides, people counting and antipassback are properly tracked. A door’s Entrance and Exit sides are relative to the area being configured.

  NOTE: Access rules assigned to the area apply to all perimeter doors of the area, even though the access rules are not listed on the *Access rules* page of the perimeter doors. If each perimeter door must be governed by its own set of rules, configure the access rules on each door.

Area - Advanced

On the *Advanced* page, you can define the advanced access control behaviors for the area.

NOTE: This page is only visible when Synergis is enabled as a feature in your license, and the **Access control** option on the *Identity* page of the area is set to **ON**. Depending on your license options, some properties might not be visible.

- **Antipassback:** Antipassback is the access restriction placed on a secured area that prevents the same cardholder from entering an area they have not yet exited, and vice versa.
  - **Status:** Turn the antipassback feature on or off.
  - **Schedule:** Select *Always* if you want antipassback to be applied at all times.
  - **Type:** Type of antipassback to apply.

        - **Soft:** Soft antipassback only logs the passback events in the database. It does not restrict the door from being unlocked due to the passback event.
        - **Hard:** Hard antipassback logs the passback event in the database and prevents the door from being unlocked due to the passback event.
    - **Presence timeout:** Set how many minutes a cardholder’s presence in the area is remembered for the purpose of passback detection (not used for counting people). Past that period, a cardholder who never left the area can re-enter without triggering a passback event. The default value of zero (0) minutes means that a cardholder's presence never times out.
      NOTE: When global antipassback is enabled, the presence of a cardholder in an area is forgotten after seven days if no entry or exit from this area is reported for that cardholder during that period. This means that cardholders can re-enter an area that they never left, or leave an area they never entered, without triggering a passback event if no movement was registered for these cardholders on that area for seven days. This applies even if the **Presence timeout** is set to infinite (=0).
    - **Strict:** Turn on this option to generate passback events for both types of access violations: when cardholders try to re-enter an area that they never left, and when cardholders try to exit an area that they never entered. Otherwise, the default is turn it off and antipassback logic is only verified on area entrances, and passback events are only generated when cardholders try to re-enter an area that they never left.
      BEST PRACTICE: If you choose to enable *strict* and *hard* antipassback on an area that is not controlled with turnstiles or similar devices that only allow one person through at a time, grant the *Forgive antipassback violation* privilege to the operators responsible for monitoring this area.
      NOTE: With strict antipassback turned off, you can have Card-In/REX-out perimeter doors, but the **Presence timeout** parameter must be configured (> 0). With strict antipassback turned on, all perimeter doors must be configured as Card-In/Card-Out, **Presence timeout** must be set to infinite (= 0), and no REX can be configured.
- **Max occupancy:** The *max occupancy* feature monitors the number of people in an area, up to a configured limit. Once the limit is reached, the rule will either deny access to additional cardholders (if set to *Hard*) or trigger events while allowing further access (*Soft*).
    - **Status:** Set it to **ON** to enable the max occupancy feature. Enabling a *Max occupancy* limit on an area generates the following events:
        - *Max occupancy reached* when the area reaches the configured limit. This event sends the area into a warning state.
        - *Max occupancy exceeded* when additional cardholders enter the area.
        - *Below max occupancy* when the number of occupants drops below the configured limit.
    - **Type:** Select from the following:
        - *Hard*: When the max occupancy limit is reached, it will deny the next access request on the area's perimeter door.
        - *Soft*: Will not deny subsequent access requests.
    - **Max occupancy limit:** Enter the number of people the area can hold before triggering the limit.

      NOTE: Cardholders with the **Bypass antipassback rules** option active are granted access even if the area's occupancy limit is reached or exceeded.
- **Interlock:** Security Center supports the interlocking of the perimeter doors for an area by allowing only one perimeter door to be open at one time.

  - **Status:** Turn the interlock feature on or off. When this feature is on, only one perimeter door of the area can be open at any given time. To open a door, all others must be closed.
  - **Priority:** When both the *override* and *lockdown* inputs are configured, select which one has priority when both inputs are active.
  - **Override:** Select the input that is wired to the *override* key switch or flip switch. When the switch in on, the interlock feature is disabled.
  - **Lockdown:** Select the input that is wired to the *lockdown* key switch or flip switch. When the switch is on, all perimeter doors remain locked until the switch is back to its normal position.

- **First-person-in rule:** The *first-person-in* rule is the access restriction placed on a secured area that prevents anyone from entering the area unless a supervisory cardholder is on site. The first-person-in rule can be enforced on door unlock schedules, access rules, or both.
  - **Enforce on door unlock schedules:** Set to **ON** to ignore all door unlock schedules until a supervisor is granted access to the area. The first-person-in rule has no effect on elevator unlock schedules.
  - **Enforce on access rules:** Set to **ON** to ignore access rules until a supervisor is present in the area. You specify when the first-person-in rule applies with a schedule.
  - **Supervisors:** List of cardholders who can act as area supervisors.
  - **Exemption list:** List of cardholders who continue to follow the access rules even when the first-person-in rule is in effect.
- **Visitor escort rule:** The *visitor escort* rule is the additional access restriction placed on a secured area that requires visitors to be escorted by a cardholder during their stay. Visitors who have a host are not granted access through access points until both they and their assigned host (cardholder) present their credentials within a certain delay.

  NOTE: The hosts are configured in the *Visitor management* task. The maximum delay granted to the host to present their credential after the visitor has presented theirs is configured individually for each door.
  - **Enforce visitor escort rule:** Set to **ON** to require the host to present their credential after the visitor, if the visitor has a mandatory host assigned.
- **Duress PIN:** The *Duress PIN* function helps to ensure a cardholder's safety in a situation where they are being coerced into unlocking a door by an intruder. When the option is on, the cardholder can use their duress PIN to unlock the door, which triggers a *Duress PIN entered* event without alerting the intruder.

Area - Threat levels

On the *Threats levels* page, you can configure specific actions to be executed by the system when a threat level is activated or deactivated on the area.

NOTE: This page is only visible when the *Threat level* license option is enabled, and at least one threat level is configured in your system.

Badge template - Badge designer tab

This section lists the settings found in the Badge template **Badge designer** tab, in the *Access control* task.

In the *Badge designer* tab, you can design and modify badge templates. In the Badge designer, there are different tools you can use to edit a template.

- **Tools:** In the *Tools* section, there are six graphical tools you can use to edit the template:
  - **Select tool:** Use to click and select an object on the template.
  - **Rectangle tool:** Use to draw a square/rectangle on the template.
  - **Ellipsis tool:** Use to draw circles/ovals on the template.
  - **Text tool:** Use to insert text on to the template.
  - **Image tool:** Use to insert a picture on to the template.
  - **Barcode tool:** Use to insert barcodes on to the template.
- **Image:** In this widget, you can choose whether the image displayed on the badge uses a cardholder picture or an image from a file, and whether the image should be stretched or not.
- **Text:** In this widget, you can add cardholder fields, as well as edit the text, the text color, and the text alignment.
- **Color and border:** In this widget, the following options are available:
  - **Fill:** Use to modify the fill color of an inserted object like a square or oval.
  - **Opacity:** Use to modify the opacity of an inserted object.
  - **Border:** Use to modify the border color of an inserted object.
  - **Border thickness:** Use to modify the thickness of the inserted object’s border.
- **Size and position:** In this widget, you can choose where the text or image is located on the badge, and its width and height.
- **Properties (⚙):** Opens the *Format* dialog box, where you can select from the following card sizes and orientation.
  - CR70
  - CR80
  - CR90
  - CR100
  - Custom card size
  - Orientation. You can choose *Landscape* or *Portrait* orientation.
- **Import (📦):** Import a badge design that was previously exported from Config Tool as a badge template (BDG formats only).
- **Export (📦):** Save the current badge design to a BDG file so it can be imported to another system.
- **Cut (✂):** Delete the selected item on the badge template.
- **Copy (⧉):** Copy the selected item on the badge template.
- **Paste (📋) :** Paste the copied item onto the badge template.
- **Send to back (⧉):** Send the selected item to the background of the badge template. This option is helpful if you want to have a background image on the badge.
- **Bring to front (⧉):** Bring the selected item to the foreground of the badge template.

Camera - Video tab

This section lists the settings found in the Camera **Video** tab, in the *Video* task.

The *Video* tab allows you to define multiple video quality (resolution, frame rate, and so on) configurations for each video *stream* generated by your video encoder. For each stream, you can also specify its usage (or function) and specific network settings.

Video quality

In the *Video quality* section, you can configure settings that affect the quality of the video (image resolution, bit rate, frame rate, and so on). Multiple video quality configurations can be defined for the same stream on different schedules.

Video quality settings might vary from one manufacturer to another. No manufacturer supports them all.

NOTE: For any setting not covered in the list below, refer to the manufacturer's documentation.

- **Resolution:** Data format and image resolution. The available choices depend on the type of video unit you have.

  NOTE: On certain models of video units that support a large number of video feeds (4 to 12), some high resolution formats might be disabled if you enable all the video streams, because the unit cannot handle all the streams at high resolutions.
- **Quality:** Video quality depends on a combination of settings. Config Tool proposes a list of predefined configurations for you to choose from. To adjust each of them individually, select *Custom* from the *Quality* drop-down list.
- **Bit rate:** Sets the maximum bandwidth (kbps) allowed for this encoder.
- **Bit rate mode:** Certain types of video units (such as Axis) allow you to set the maximum bit rate at the unit level. In this case, the *Bit rate mode* drop-down list is available for your bit rate settings.
  - **Variable:** Variable bit rate (VBR) adjusts the bit rate according to the complexity of the images in the video. This uses a lot of bandwidth when there is a lot of activity in the image and less bandwidth when the monitored area is quiet.
  - **Constant:** Constant bit rate (CBR) allows you to set a fixed target bit rate that will consume a predictable amount of bandwidth, which will not change, whatever happens in the image. This requires you to set another parameter, the *Bit rate priority*.
- **Bit rate priority:** If you choose to maintain a constant bit rate, the encoder might not be able to keep both the frame rate and the image quality at their set values when the activity in the image increases. The *Bit rate priority* lets you configure which aspect of video quality you wish to favor when you are forced to make a compromise.
  - **Frame rate:** Maintains the frame rate at the expense of the image quality.
  - **Image quality:** Maintains the image quality at the expense of the frame rate.
  - **None:** Lowers both the frame rate and the image quality to maintain the bit rate.
- **Frame rate:** Sets the number of *frames* per second (fps). A high frame rate (10 fps or more) produces fluid video and is essential for accurate *motion detection*. However, increasing the frame rate also sends more information over the network, and therefore, requires more bandwidth.
- **Image quality:** Sets the image quality (the higher the value, the better the quality). Higher image quality requires more bandwidth, which might compromise the frame rate.

When bandwidth is limited, you should consider the following:

- To retain very good image quality, restrict the number of images per second (lower frame rate).
- To transmit more images per second at a high frame rate, lower the image quality.

The encoder tries to maintain each quality setting. However, if bandwidth is limited, the encoder might reduce the frame rate in favor of the image quality.

- **Automatic settings:** Certain models of encoders (such as Bosch) let you select this option instead of setting your own value for image quality. To set the image quality manually, you have to select *Custom* in the *Quality* drop-down list.
- **Key frame interval:** A *key frame* is a frame that contains a complete image by itself as opposed to a usual frame that only holds information that changed compared to the previous frame. If your network is less reliable, you require a higher key frame rate to recover more quickly from cumulative errors in the video. Frequent key frames require a higher bandwidth. You can specify the key frame interval in seconds (1 to 20) or by frames (based on the frame rate).
- **Recording frame rate:** Record the video at a lower frame rate than the rate used for viewing video. This setting save storage space, but it does not reduce bandwidth usage. Setting the *Recording frame rate* to anything other than *All frames* locks the *Key frame interval*.
- **Profile and level:** Used only for *MPEG-4* streams, the profile determines the tools available when generating the stream (for example, interlace, or B frames), and the level limits the resource usage (for example, max bit rate).
- **Video object type:** The Video Object Type (VOT) to use for MPEG-4 streams. The available choices are governed by the choice of *Profile and Level*.
- **GOP structure:** Stands for *Group Of Picture* structure. It is possible to configure up to four types of GOP structures:
  - **I:** Stands for *Intra* frame structure. Meaning only Intra (key frame) frames are sent. This is primarily for using an external multiplexer.
  - **IP:** Stands for *Intra and Predicted* frame structure. This setting results in the lowest possible video delay.
  - **IPB:** Stands for *Intra and Predicted and Bidirectional* frame structure. This setting enables the user to have a higher quality and a higher delay.
  - **IPBB:** Stands for *Intra and Predicted and Bidirectional and Bidirectional* frame structure. This setting enables the highest quality and a highest delay.
- **GOP length:** Stands for *Group Of Picture* length. With this value, it is possible to change the *distance* (number of frames) between the *intra-frames* in the MPEG-2 video stream.
- **Streaming type:** Select between VES (video elementary stream), which sends only video information, or PRG (program stream), which sends both video and audio information.
- **Input filter mode:** Lets you select a noise filter to apply to the video signal before it is encoded. It has four settings: *None*, *Low*, *Medium*, and *High*.

  NOTE: Removing noise from the video signal also reduces the sharpness of the image. If the video signal is relatively clean, do not apply any filter (*None*). The higher the filter level, the more blurry the video image becomes. Keeping a sharp image creates more pixels to encode, which uses more bandwidth. This is why on some video units the default is set to *Medium*.
- **Bit rate control:** Lets the encoder automatically lower the *bit rate* when one of the decoders is reporting transmission errors (dropped packets). This usually happens when there is a lot of motion on the camera. The encoder drops the bit rate as low as necessary to let all decoders receive an error free transmission. When the motion subsides, the encoder gradually increases the bit rate until it reaches the configured maximum limit. The trade-off between low bit rate and transmission errors is that with a low bit rate, the image stays crisp but the video might appear choppy, while with transmission errors, the image contains noises, but the video stays fluid.
- **Compression mode:** Select between SM4, Verint's proprietary version of MPEG-4 compression, or ISO, the standard MPEG-4 compression.

Stream usage

The *Stream usage* options are only available for encoders capable of generating multiple video streams. It allows you to specify the usage (or function) of each stream.

- **Live:** Default stream used for viewing live video in Security Desk.
- **Recording:** Stream recorded by the Archiver for future investigation.
- **Remote:** Stream used for viewing video when the bandwidth is limited.
- **Low resolution:** Stream used instead of the *Live* stream when the tile used to view the stream in Security Desk is small.
- **High resolution:** Stream used instead of the *Live* stream when the tile used to view the stream in Security Desk is large.

Network settings

The *Network settings* options allow you to configure the desired connection type used by the video encoder.

- **UDP port:** Port number used when the connection type is unicast *UDP*. If the encoder supports multiple video streams, this parameter is different for each stream.
- **Connection type:** Defines how communication is established between the Archiver and the camera for sending or receiving video streams.
  - **Best available:** Lets the Archiver select the best available connection type for the stream. The best available types rank in this order, according to availability: *Multicast*, *UDP*, *TCP*, *RTSP over HTTP*, and *RTSP over TCP*.
  - **Unicast UDP:** Forces the stream to be sent in UDP to the Archiver. The stream must be formatted using the RTP protocol.
  - **Unicast TCP:** Forces the stream to be sent in *TCP* to the Archiver. Here, TCP is taken in the broad sense. For some types of cameras, the Archiver establishes a TCP connection to the unit and receives the stream in a proprietary protocol. For others, the stream is sent over HTTP. Typically, the stream is not formatted according to the RTP protocol by the unit. The Archiver has to convert the stream to the RTP protocol to be archived or retransmitted to the system.
  - **RTSP stream over HTTP:** This is a special case of TCP connection. The Archiver uses the RTSP protocol to request the stream through an HTTP tunnel. The stream is sent back through this tunnel using the RTP protocol. This connection type is used to minimize the number of ports needed to communicate with a unit. It is usually the best way to request the stream when the unit is behind a NAT or firewall, because requests sent to HTTP ports are easily redirected through them.
  - **RTSP stream over TCP:** This is another special case of TCP connection. The Archiver uses the RTSP protocol to request the stream in TCP. The request is sent to the RTSP port of the unit.
  - **Same as unit:** Special case for Panasonic units. The connection type is the same for all streams of the unit. When present, it is the only connection type supported. The real connection type must be set in the specific configuration page of the unit.
- **Multicast address:** The *multicast* address and *port number* are assigned automatically by the system when the video unit is discovered. Each video encoder is assigned a different multicast address with a fixed port number. If the encoder is capable of generating multiple video streams, then a multicast address should be assigned to each stream. This is the most efficient configuration.

Boost quality on manual recording

Temporarily boost video quality when the recording is started manually by a Security Desk user when they click the *Record* (●) button or the *Add bookmark* (🔖) button. This option is only available for the recording stream.

Boost quality on event recording

Temporarily boost video quality when the recording is triggered by a *system event* (the *Start recording* action was executed, an *alarm* was triggered, or because of a motion event). *Boost quality on event recording* settings have priority over the *Boost quality on manual recording* settings. The length of the video quality boost depends on the event type, and the camera’s recording settings.

Camera - Recording tab

This section lists the settings found in the Camera **Recording** tab, in the *Video* task.

In the *Recording* tab, you can customize the recording settings on each individual camera instead of using the archiving role settings.

If the camera is associated to additional Auxiliary Archiver roles, there is one group of settings for each archiving role the camera is associated to.

- **Recording settings:** Select whether the camera uses the settings inherited from the archiving role or uses its own custom settings.
    - **Inherit from Archiver:** Use the recording settings of the archiving role.
    - **Custom settings:** Configure the recording settings for the individual camera.

You can get a description of each recording setting from the Archiver recording tab.

Camera - Video analytics > Motion detection tab

This section lists the settings found in the Camera **Video analytics** > **Motion detection** tab, in the *Video* task.

On the *Motion detection* page, you can define multiple motion detection configurations for your camera. Each configuration is based on a different schedule.

- **Motion detection:** Turns motion detection ON or OFF for the time periods covered by the schedule.
- **Detection is done on:** Specifies whether motion detection is performed on the Archiver (always available), or on the video unit (not all units support this feature).
- **Sensitivity:** Controls how much difference must be detected in a block between two consecutive frames before it is highlighted as a motion block. With the sensitivity set to the maximum (100%), the slightest variation in an image block is detected as motion. Lowering the sensitivity reduces the number of motion blocks detected in the video. You can decrease the sensitivity when your equipment is prone to noise.
- **Auto calibrate:** Automatically set the sensitivity to determine what constitutes positive motion.
- **Consecutive frame hits:** A frame where the number of motion blocks reaches the *Motion on* **Threshold** is called a hit. Setting this parameter higher than 1 helps avoid false motion detection hits, such as from video noise in a single frame. This setting ensures that positive motion detection only raised an event when a hit is observed over a certain number of consecutive frames. When enough consecutive hits have been observed, the first hit in the series is marked as the beginning of motion.
- **Advanced settings:** When an *H.264* stream is selected as the recording stream, the **Advanced settings** button is available. Click this button to open the *H.264 advanced motion detection settings* dialog box where you can refine your motion detection settings for an H.264 stream.
  - **Preset:**
    - **Vector emphasis:** Sets motion detection based on the difference in motion vector values (movement) between consecutive frames.
    - **Luma emphasis:** Sets motion detection based on the difference in luma values (brightness) between consecutive frames.
    - **Custom:** Customize your settings using the available sliders, if the *Vector emphasis* and *Luma emphasis* presets provide too many or too few motion events. Adjust the following slider values between 0 and 100, until you achieve good results. The higher the value, the more motion is detected.
      - **Luma weight:** Sets motion detection based on the difference in luma values (brightness) between consecutive frames.
      - **Chroma weight:** Sets motion detection based on the difference in chroma (color) values between consecutive frames.
      - **Vectors weight:** Sets motion detection based on the difference in vector values (movement) between consecutive frames.
      - **Macroblocks weight:** Sets motion detection based on the presence of intra-macroblocks in your frame. This setting is useful when you notice motion detection indicators on still frames. For example, some units generate frames completely comprised of intra-macroblocks as a new reference point. When this happens, you will see motion detection blocks covering your whole image. Setting the **Macroblocks weight** to 0 helps prevent this from happening.
- **Motion zones:** A motion zone defines a location on the video image where motion is detected. Up to six different motion zones can be defined per configuration. The video image is divided into a large number of blocks (1,320 for NTSC encoding standard and 1,584 for PAL). Each of these blocks can be turned on and off for motion detection. A block where motion detection is turned on is represented by a semi-transparent blue square overlay on the video image.
- **Motion on:** If the number of detected motion blocks reaches the **Threshold** over the required number of **Consecutive frame hits**, the selected event is raised.

- **Motion off:** If the number of detected motion blocks falls below the **Threshold** for at least five seconds, the selected event is raised.
- **Test zone:** The motion zone is displayed as blue overlays. Motion blocks are displayed as green overlays. The number of motion blocks is updated in real time. When the number of motion blocks reaches the *Motion on* **Threshold**, it is displayed in red.
- **Test all zones:** In this mode, all motion zones are displayed at once, with the number of motion blocks in each zone displayed separately.
- **View all motion:** Test the entire video image for motion. Motion anywhere on the image is displayed as motion blocks (green overlays). The total number of motion blocks is updated in real time. Use this mode to test the **Sensitivity** setting for this camera.
- **Events:** Select the motion detection events generated by the system (default or custom events).

Camera - Video analytics > Visual tracking tab

This section lists the settings found in the Camera **Video analytics** > **Visual tracking** tab, in the *Video* task.

From the *Visual tracking* tab, you can configure the visual tracking feature.

- **Select:** Resize, reposition, and rotate the selected video overlay using your mouse.
- **Rectangle:** Draw a rectangle on the video image.
- **Ellipse:** Draw an ellipse on the video image.
- **Entities:** Display the area view from which the cameras linked to the selected overlay can be dragged from.
- **Size and position:** Resize and reposition the selected video overlay.
- **Fill:** Select the fill color of the selected overlay.
- **Border:** Select the border color of the selected overlay.
- **Opacity:** Select the opacity percentage of the selected overlay.
- **Thickness:** Select the border thickness of the selected overlay.
- **Links:** List of cameras that were dragged from the area view into the selected overlay, and that a user can jump to from that camera in Security Desk.

Camera - Color tab

This section lists the settings found in the Camera **Color** tab, in the *Video* task.

In the *Color* tab, you can adjust the video attributes such as brightness, contrast, hue, and saturation, based on different schedules.

- **Brightness:** Adjust the brightness of the video image for the selected schedule.
- **Contrast:** Adjust the contrast of the video image for the selected schedule.
- **Hue:** Adjust the hue of the video image for the selected schedule.
- **Saturation:** Adjust the saturation of the video image for the selected schedule.
- **Load default:** Reset all parameters to their default values for the selected schedule.
- **Analog format:** Select NTSC (National Television System Committee) or PAL (Phase Alternating Line) analog format for the video signal. PAL format generally streams video at a lower frame rate, but at a higher resolution.

Camera - Hardware tab

This section lists the settings found in the Camera **Hardware** tab, in the *Video* task.

In the *Hardware* tab, you can associate other hardware devices (PTZ motors, speakers, microphones, and so on) to this camera and configure specific hardware settings. When the unit is initially added to the system, all hardware devices belonging to the same unit are configured by default. You can manually associate your camera to other devices, according to how they are physically connected.

PTZ configuration

If the PTZ motor is not integrated to your camera, you need to configure the PTZ motor separately before you can control it in Security Desk. When you turn the PTZ switch on, additional settings appear.

- **Protocol:** Protocol used by the PTZ motor.
- **Serial port:** Serial port used to control the PTZ motor. Click ✏ to set the Idle delay, Idle command, and Lock delay parameters.
- **Enhanced PTZ:** Turn this option on to enable the zoom-box, center-on-click, and enhanced zoom PTZ commands.
- **Calibrate:** Click to calibrate the PTZ.

  NOTE: Not all cameras require PTZ calibration.
- **PTZ address:** Number identifying the selected PTZ motor on the serial port. This number is important because it is possible to connect more than one PTZ motor on the same serial port. This number must correspond to the dip switch settings on the PTZ hardware.
- **Max zoom factor:** The maximum zoom factor allowed for this camera.

If you observe positioning or rotation issues when controlling a PTZ camera, you can click **Specify rotation and direction offsets** for the following additional options:

- **Pan offset:** Enter the pan offset (in degrees) needed to align the camera with the position shown in Security Center.
- **Tilt offset:** Enter the tilt offset (in degrees) needed to align the camera with the position shown in Security Center.
- **Invert rotation direction:** If the camera does not rotate in the same direction as shown in Security Center, select this option to invert the direction of rotation.

Idle delay

The Idle delay is the amount of time that a PTZ motor becomes locked for when a user does one of the following:

- Moves an idle PTZ (which generates the *PTZ activated* event). After the idle delay period, the *PTZ stopped* event is generated. If users continue to move the PTZ, then the idle delay countdown timer continuously restarts.
- Zooms a PTZ motor (which generates the *PTZ zoom by user* event). After the last zoom operation and the idle delay period ends, the *PTZ zoom by user stopped* event is generated.

Example

The idle delay is 120 seconds. If a user zooms several times, and each zoom action is less than 120 seconds apart, only one *PTZ zoom by user* event is generated. If another user performs a zoom on the same PTZ before the idle delay expires, the *PTZ zoom by user* event is generated again, logged to the second user, and the countdown timer is restarted. The *PTZ zoom by user stopped* event is only generated after the Idle delay expires, and is logged to the second user.

Idle command

When the PTZ becomes idle (after the idle delay expires and the *PTZ stopped* or *PTZ zoom by user stopped* event is generated), this option determines the next action of the PTZ.

- **None:** The PTZ remains idle until a user starts controlling it.
- **Preset:** The PTZ moves to a preset position when it becomes idle.
- **Pattern:** The PTZ motor starts a PTZ pattern when it becomes idle.

Lock delay

The *Lock delay* is the amount of time that a PTZ motor becomes locked when a user clicks the Lock PTZ button (🔒) in the PTZ widget. The overall maximum delay is 60 days. After the lock delay period, the PTZ automatically unlocks.

NOTE: The PTZ lock is removed immediately in the following scenarios:

- The Archiver goes down or fails over.
- The main server goes down or fails over.
- The user who performed the lock is deleted.

Speaker and microphone

Even if the unit your camera belongs to does not support audio, you can still link your camera with audio devices (speaker and microphone) found on other units.

Camera tampering

Select this option to let Security Center process *Camera tampering* events issued by the unit. This setting is only available if the video unit is capable of detecting camera tampering.

- **Minimum duration:** Typically, any dysfunction that prevents the scene from being viewed properly (partial or complete obstruction of the camera view, sudden change of the field of view, or loss of focus) can be seen as an attempt to tamper with the camera. You can control how sensitive the unit is to these changes, by specifying how long the dysfunction must last before the unit generates a *Camera tampering* event.
- **Alarm for dark images:** Select this option for total obstructions to be considered as dysfunctions.

Audio alarm

Select this option to let Security Center process audio alarms issued by the unit as *Audio alarm* events. This setting is only available if the video unit is capable of raising audio alarms.

NOTE: The *Alarm level* sets the value used to trigger audio alarms on the unit. A unit can be configured to issue audio alarms when the sound level rises above or falls below the set value. The alarm level can be set in the range 0-100%, where 0% is the most sensitive and 100% the least sensitive.

Image rotation

Use this setting to correct the orientation of the image when the camera is mounted upside down or at a 90 degree angle. This method uses the camera's capability to perform image rotation.

- This feature is only available if it is supported by the camera hardware.
- The rotation options vary depending on the model of the camera.
- Rotating the image using the *Image rotation* feature is preferable to using the *Video rotation* feature, however if using image rotation adversely affects video frame rate, try using video rotation instead.

Video rotation

Use this setting to correct the orientation of the image when the camera is mounted upside down or at a 90 degree angle. This method uses Security Center to rotate the video.

- Using *Video rotation* adds extra load on the client workstations. For this reason, it is preferable to use *Image rotation*, if it is available for the camera.
- This feature is not available for PTZ cameras or cameras that use panomorph (fisheye) lenses.

Lens type

Use this setting to select the lens type for cameras with interchangeable lenses. Depending on the selected lens type, you might have additional settings to configure, such as *dewarping* a fisheye lens.

Camera sequence - Cameras tab

The **Cameras** tab is where you can add cameras that make up the camera sequence.

The order of the cameras in the list is the order they are displayed in Security Desk. Each camera is defined by the following display properties:

- **Dwell time:** The amount of time the camera is displayed when cycling through the sequence.
- **PTZ command:** (PTZ cameras only) The action the PTZ camera will perform when it is displayed in the sequence.
- **PTZ command:** (PTZ cameras only) The switch number and the state to set the switch to when the camera is displayed in the sequence.

Related Topics

Creating camera sequences on page 644

Cardholder configuration tabs

This section lists the settings found in Cardholder configuration tabs, in the *Access control* task.

Cardholder - Properties tab

In the *Properties* tab, you can view the cardholder's personal information and status. Additional information might be found in the *Custom fields* tab, if custom fields are created for cardholder entities.

- **First name:** Cardholder's first name. If the software language (chosen at installation) is latin-based, the *Name* field is configured as the first name followed by the last name. This order is reversed if you are using an Asian language such as Japanese or Chinese.
- **Last name:** Cardholder's last name.
- **Email address:** Cardholder's email address, used for automated actions associated to the cardholder (send an email).
- **Use extended grant time:** Grants the cardholder more time to pass through doors where the *Extended grant time* parameter is configured for a door. Use this option for cardholders with reduced mobility.
- **Bypass antipassback rules:** Exempts the cardholder from all *antipassback* restrictions.
- **Security clearance :** Cardholder's security clearance level. A cardholder's security clearance level determines their access to areas when a threat level is set in Security Center. Level 0 is the highest clearance level, with the most privileges.
  - **Inherited from parent cardholder groups:** The cardholder's security clearance level is inherited from the parent cardholder groups. If the cardholder is part of multiple cardholder groups, then they inherit the highest security clearance level from the parent cardholder groups.
  - **Specific:** Set a security clearance level for the cardholder.
- **Status:** Set their status to *Active* by clicking **Activate**, or *Inactive* by clicking **Deactivate**. For their credentials to work, and for them to have access to any area, their status must be *Active*.
- **Activation:** Displays the date when the cardholder was activated.
- **Expiration:** Set an expiration for their profile:
  - **Never:** Never expires.
  - **Specific date:** Expires on a specific date and time.
  - **Set expiration on first use:** Expires a specified number of days after the first use.
  - **When not used:** Expires when it has not been used for a specified number of days.

Cardholder - Picture tab

In the *Picture* tab, you can assign a picture to the cardholder.

Cardholder group - Properties tab

This section lists the settings found in the Cardholder group **Properties** tab, in the *Access control* task.

In the **Properties** tab, you can view and configure the members of this cardholder group, and configure their common properties. Additional information might be found in the **Custom fields** tab, if custom fields are created for cardholder groups.

- **Group available for visitors:** Set this to **ON** if this group will be used for visitors
- **Email address:** Email address for automated actions associated to the group (send an email).
- **Security clearance:** Security clearance level for the cardholder group. A cardholder group's security clearance level determines their access to areas when a minimum security clearance level is required on areas by setting a threat level in Security Center. Level 0 is the highest clearance level, with the most privileges.
  - **Inherited from parent cardholder groups:** The cardholder group's security clearance level is inherited from their parent cardholder group. When multiple parent cardholder groups exist, the highest clearance level is inherited.
  - **Specific:** Set a specific security clearance level for the cardholder group.
- **Cardholders:** Define the cardholder group members using the ➕ and ❌ buttons. Both individual cardholders and other cardholder groups can be members.

Credential configuration tabs

This section lists the settings found in Credential configuration tabs, in the *Access control* task.

Credential - Properties tab

In the *Properties* tab, you can configure the credential information and status. Additional information might be found in the *Custom fields* tab.

- **Credential information:** This section identifies the details of the credential itself. If the credential is an access control card, the format, facility code and card number will be shown.
  - **Cardholder:** Displays the cardholder this credential is associated with. The cardholder can be changed if required.
- **Status:** Shows whether the credential status is *active* or *Inactive/Lost/Stolen/Expired*.
- **Activation:** Displays the date and time when the credential was attributed to this state.
- **Expiration:** Set an expiration for the credential:
  - **Never:** The credential never expires.
  - **Specific date:** The credential expires on a specific date and time.
  - **Set expiration on first use:** The credential expires after a specified number of days after the first use.
  - **When not used:** The credential expires when it has not been used for a specified number of days.

Credential - Badge template tab

In the *Badge template* tab, you can define the default badge template associated to this credential. You can preview what the credential will look like when printed using any specific badge template. You can also print the card credential.

Door configuration tabs

This section lists the settings found in Door configuration tabs, in the *Area view* task.

Door - Properties tab

In the *Properties* tab, you can configure the general behavior of the door. Some of the behaviors are not supported by all types of access control units. If the configured behavior is not supported by the selected access control unit, a yellow warning appears on the page, explaining why your configuration is not valid.

- **Unlocked for maintenance:** Turn on this option if the door is unlocked, and possibly open for maintenance purposes. While the door is in maintenance mode it remains unlocked, and no events are generated except for the *Door offline: Device is offline* event. The *maintenance mode* icon (◆) is also displayed on the door icon in maps.
- **Standard grant time:** Amount of time the door is unlocked after an *Access granted* event is generated.
- **Extended grant time:** For cardholders with the property "extended grant time" turned on, the amount of time the door is unlocked after access is granted.
- **Standard entry time:** Amount of time the cardholder has to cross the entry sensor, in addition to the *Standard grant time*. If no entry is detected during this time, a *No entry detected* event is generated. This option is only supported when your door is configured with an entry sensor. If no entry sensor is configured, entry is assumed when the door opens. If no door sensor is configured, entry is assumed when an access is granted.

  For example, if the *Standard grant time* is 5 seconds, and the Entry time is 3 seconds, the cardholder has a total of 8 seconds to trigger the entry sensor of the door.
- **Extended entry time:** For cardholders with the property 'extended grant time' turned on, the amount of time the cardholder has to cross the entry sensor, in addition to the Extended grant time. If no entry is detected during this time, a *No entry detected* event is generated. This option is only supported when your door is configured with an entry sensor. If no entry sensor is configured, entry is assumed when the door opens. If no door sensor is configured, entry is assumed when an access is granted.

  For example, if the *Extended grant time* is 10 seconds, and the *Extended crossing time* is 10 seconds, the cardholder has a total of 20 seconds to cross the entry sensor of the door.
- **Door relock:** Specifies when to re-lock the door after an access has been granted.
  - **On close:** Relocks when the door closes.
    NOTE: This option is not supported by HID units.
  - **Delay after opening:** Relocks after the specified delay after the door has been opened.

    NOTE: For HID units, the maximum delay is 27 minutes.
- **When door is unlocked by schedule:** Select the events you want to suppress when the door is unlocked by schedule.
  - *Door open too long* events
  - *Access granted* and *Access denied* events
- **Door held:** What to do when the door is held open.
  - **Trigger event:** Turn on this option if the *Door open too long* event must be generated after the specified duration.
  - **Reader buzzer behavior:** Set to either **Suppressed** to never sound the buzzer, or to **Suppressed when door closes** to silence the buzzer as soon as the door closes.
  - **Trigger pre-alarm events:** (Only for doors controlled by Synergis™ IX) Turn on this option if you want to generate a pre-alarm condition after the specified delay. The pre-alarm delay must be shorter than the delay for triggering the *Door open too long* event, otherwise, no alarm will be triggered. The

pre-alarm condition is typically used to activate an output to warn users that the door will generate an alarm if it is left open any longer. For more information on pre-alarm, see the documentation on Synergis IX.

- **Door forced:** What to do when the door is forced.
  - **Trigger event:** Turn on this option if the *Door forced open* event must be generated.
  - **Reader buzzer behavior:** Set to either **Suppressed** to never sound the buzzer, to **Suppressed when door closes** to stop the buzzer as soon as the door closes, or to **Suppressed on access granted** stop the buzzer when an access is granted, or when the door is manually locked.
- **Request to exit (REX):** The options in this section are generally used to decrease the number of false *Request to exit* events at a door.
  - **Time to ignore REX after granted access:** Ignore any requests to exits for this long after access has been granted.
  - **Unlock on REX:** Turn on this option if a REX is being used, and you want to automatically grant access to all requests to exit.
    NOTE: Security Center does not receive REX events if the access control unit is connected to the Access Manager. However, the REX events are received when the unit is offline and then connects back to the Access Manager.
  - **Ignore REX events while door is open:** Do not generate REX events when door is open.
  - **Time to ignore REX after door closes:** Once the door has closed, wait this long before generating any more REX events.

    NOTE: HID controllers do not support this feature.
- **Visitor escort rule and two-person rule:** Settings common to the visitor escort and the two-person rule restrictions.
  - **Enforce two-person rule:** Turn on this option if two cardholders must present their credentials within a certain delay of each other in order to gain access. This rule can be enforced only on one door side or both.
  - **Maximum delay between card presentations:** Maximum delay allowed between the two card presentations to satisfy the visitor escort rule and the two-person rule restrictions.

Door - Hardware tab

In the *Hardware* tab, you can configure the physical wiring relationships between the access control unit and the door, and associate cameras to door sides.

- **Preferred unit:** Access control unit that is connected to the door.
- **Preferred interface:** Interface module that is connected to the door.
- **Door side:** Readers, REX's, entry sensors, and cameras associated with the door side, that match the physical wiring done on the controller and the door.

  The available reader settings are:
  - **PIN entry timeout:** This sets the entry timeout for the PIN after the card has been read. For example, by default, you have 5 seconds to enter all the PIN digits.
  - **Use card and PIN:** Turn on the option to change the reader mode to *Card and PIN* and use the **Schedule** list to select when this mode applies. When not in a scheduled time period, the reader behaves in either *Card only* or *Card or PIN* mode, depending on the unit-wide parameters configured in the portal of the Synergis unit.
- **Additional connections:** Other physical connections associated with the controller and the door.

Door - Access rules tab

In the *Access rules* tab, you can view the access rules applied to this door.

- **Door access applies to:** Which door sides the access rules apply to.
  - **Both sides:** Apply the same access rules to both door sides.
  - **Individual sides:** Apply individual access rules to each door side.
- **Access rights for door (side):** Define who has access to this door (or door side).
  - **Access rules:** Add access rules to grant (or deny) access to the door to cardholders and cardholder groups based on a schedule. This is the recommended approach.
  - **Cardholders, cardholder groups:** Add cardholders and cardholder groups to grant them access to the area at all times. Only use this approach for temporary situations.

    NOTE: If all perimeter doors of an area share the same access rules, define those rules at the area level.

Door - Unlock schedules tab

In the *Unlock schedules* tab, you can configure scheduled periods when the door is not used for secured access, and no access rules are in effect.

- **Unlock schedules (free access):** Periods when the door is unlocked, and no access rules are in effect.
- **Exceptions to unlock schedules (controlled access):** Periods when the door is locked, and access rules apply.

Related Topics

HID I/O linking considerations on page 1487

Elevator configuration tabs

This section lists the settings found in Elevator configuration tabs, in the *Area view* task.

Elevator - Floors tab

In the **Floors** tab, you can configure the physical wiring relationships between the access control unit and the elevator floors, and select cameras used to monitor this elevator in Security Desk.

- **Preferred unit:** Access control unit that manages this elevator cab's panel.
- **Elevator cab reader:** *Reader* interface that is used inside the elevator cab.

  The available reader settings are:

  - **PIN entry timeout:** This sets the entry timeout for the PIN after the card has been read. For example, by default, you have 5 seconds to enter all the PIN digits.
  - **Use card and PIN:** Turn on the option to change the reader mode to *Card and PIN* and use the **Schedule** list to select when this mode applies. When not in a scheduled time period, the reader behaves in either *Card only* or *Card or PIN* mode, depending on the unit-wide parameters configured in the portal of the Synergis unit.
- **Camera:** Camera that monitors this elevator in Security Desk.
- **Floors:** Push button relays and inputs connected to the elevator floor buttons.
  - **Push button relay:** Output relays assigned to the different elevator floor buttons. Access granted events cause an output relay to close, which enables the button-push to request a certain floor.
  - **Floor tracking:** Inputs assigned to elevator floor buttons. When you assign inputs, Security Center can take note of which floor button was pushed.
  - **Cameras:** Cameras used to monitor the elevator door on each floor.

Elevator - Access tab

In the **Access** tab, you can configure the access rules applied to each of the elevator floor, and determine when access to the elevator floors is controlled and when *free access* is available.

- **Access rules:** Select access rules to determine which floor buttons are enabled, when, and for which cardholders. Different access rules can be applied to different floors, or applied to all floors.
- **Exceptions:** Determine if there are any exceptions to the access rule you set.
  - **Schedule:** Select a schedule when the exception applies.
  - **Floor:** Select which floors the exception applies to.
  - **Mode:** Select whether access to the elevator floor is *free* or *controlled* during the exception schedule.

Elevator - Advanced tab

In the **Advanced** tab, you can configure the advanced behavior of this elevator.

- **Grant time:** How long the elevator floor button is enabled after an access granted event is generated.
- **Free access when the output relay is:**
  - **Normal:** Floor access is granted when the access control unit output relay is de-energized. This means that a power loss results in free access to the floor.
  - **Active:** Floor access is granted when the access control unit output relay is energized. This mean that a power loss results in floor access being denied.

Hardware zone configuration tabs

Hardware zones are controlled by a single access control unit. They can work offline, and can be armed or disarmed using a key switch or on schedule.

Hardware zone - Properties tab

Click the **Properties** tab to configure the inputs that define this zone, and define how they are evaluated.

- **Access control unit:** Access control unit that controls the hardware zone.
- **Interface module:** Interface module where the inputs are selected from.
- **Inputs:** Inputs combined to evaluate the zone state.
- **Operator:** Logical operator used to combine the input states to evaluate the zone state.
- **Associated events:** Events representing the zone states. Select *None* if a zone state should be ignored.
  - **Normal state:** When the combination of inputs yields a zero (0).
  - **Active state:** When the combination of inputs yields a one (1).
  - **Trouble state:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.
  - **Reactivation threshold:** The time period during which the same event should not be re-triggered.

Hardware zone - Arming tab

Click the **Arming** tab to configure the arming source of your zone and its arming behavior.

- **Arming source:** Select whether the hardware zone is armed by a key switch or on a schedule.
  - **Schedule:** Select the schedule corresponding to the period when the zone is armed.
  - **Input point:** Select the input that is wired to the key switch.
- **Delays:** Optional delays that give you time to leave the premises after arming the zone, and time to disarm the zone after tripping a sensor.
  - **Arming delay:** Duration (mm:ss) you want between the time the zone is armed and the time the event triggers become active.
  - **Entry delay:** Duration (mm:ss) you want between the time the entry sensor is tripped and the time the events are triggered. This option allows you to disarm the zone before triggering the output relays.
- **Countdown buzzer:** You can assign an output relay to activate a countdown buzzer to match the arming delay.
  - **Countdown sounder:** Select the output relay.
  - **Output behavior:** Select the output behavior that defines the signal pattern for the buzzer.

Hotlist configuration tabs

This section lists the settings found in Hotlist configuration tabs, in the *ALPR* task.

Hotlist - Properties tab

In the *Properties* tab, you can configure the basic properties of the hotlist (hotlist priority, hotlist path, attributes, and so on). These settings tell Security Center how to parse the hotlist file into the format required by the *Patroller entity* and the *ALPR Manager* to identify plates read by *Sharp units*.

- **Priority. :** Hotlist priority. Zero (0) is the highest priority setting and 100 is the lowest priority setting. If a plate read matches more than one hotlist, the hotlist with the highest priority is displayed first in the list of hotlist matches.
- **Hotlist path:** Path to the hotlist source text file that contains the hotlist data, such as license plate numbers and other related vehicle information. The source text file can be located on the ALPR Manager computer’s local drive (for example, the C drive), or on a network drive that is accessible from the ALPR Manager computer.
- **Use delimiters:** Tells Security Center that the fields in the hotlist file vary in length, and indicates the character used to separate each field in the file. By default, *Use delimiters* is set to *On*, and the delimiter specified is a *semi-colon* (;). If your hotlist file is made up of fixed length fields, set *Use delimiters* to *Off*.
- **Visible in editor:** Allow a user to edit the hotlist or permit list using the Hotlist and permit editor task.
- **Attributes:** Tells Security Center the name and order of the fields (attributes) in the source text file.

Hotlist - Advanced tab

In the *Advanced* tab, you can configure the advanced properties of the hotlist (the color, sound, download frequency, and so on). These properties are not required for all hotlists, but allow you to customize certain hotlists for specific scenarios.

- **Color. :** Assigns a color to a hotlist. When you choose a color, the map symbol that marks the location of the hotlist hit in Security Desk and Genetec Patroller™, as well of the Hotlist Hit and Review Hits screen in Patroller, appears in that color.
- **Use wildcards. :** Indicates that the hotlist contains wildcards (partial license plate numbers). You can have a maximum of two wildcard characters (asterisk *) in a PlateNumber. Wildcard hotlists are used in situations where witnesses did not see, or cannot remember a complete license plate number. This allows the officer to potentially intercept vehicles associated with a crime, which otherwise would not have been detected using standard hotlists.
- **Covert:** Set the hotlist to a *covert hotlist*. When you choose this setting, Patroller users are not alerted when a hit occurs. Only users with sufficient privileges can view *covert hits* in Security Desk.
- **Email address:** Email address that receives a notification when the hotlist you’re configuring generates a hit.
- **Sound file:** The sound that Patroller plays when a hotlist hit occurs. If you leave this field blank, Patroller plays its default sounds. The path (you must include the filename) indicates the file’s location on the Patroller in-vehicle computer.
- **Override privacy for emails:** Bypasses any privacy settings you applied at the Directory level, and sends an email with real ALPR data to the email address you specified for this particular hotlist.
- **Disable periodic transfer:** Turns off periodic transfer of hotlist modifications to the Patroller computer. When this setting is off, hotlist changes are only downloaded to Patroller when the user logs on to the application. This option requires a wireless connection between Patroller and Security Center.
- **Enable transfer on modification:** Transfer hotlist modifications to Patroller as soon as they occur. For example, you can use this option on a hotlist to force Patroller to query for changes more frequently than the periodic transfer period (which applies to all hotlists). This can be useful for Amber alerts because

they can be added to a specific hotlist and sent to a Patroller almost immediately. This option requires a continuous wireless connection between Patroller and Security Center.

I/O zone - Properties tab

On the I/O zone **Properties** tab, you can configure the inputs that define this zone, and the output relays that should be triggered, along with the desired output behavior, when the zone state be armed and active.

- **Maintenance:** Switch to **ON** to set the zone in maintenance mode. While in maintenance mode, the zone is disarmed and reverts to *Normal* state. No events are generated, and no output behaviors are triggered during this time, not even the *Trouble* event.
- **Arming schedule:** Select the schedules corresponding to the periods when the zone is armed.
- **Exceptions:** Select the schedules corresponding to the periods when the zone is not armed. The exception schedules take precedence over the arming schedules.
- **Master unit:** Shows the Synergis™ unit that is selected at the creation of the zone to do I/O linking. The I/O zone stops working if the master unit is down.
- **Inputs:** Select the inputs that must be combined to evaluate the zone state. The inputs can belong to different Synergis units, but all units must be under the same Access Manager.

  IMPORTANT: If the inputs do not belong to the same Synergis unit, you must select the **Activate peer-to-peer** option in the Access Manager. Up to 15 Synergis units can be connected as peers.
- **Outputs:** Select the output relays you want to send the configured output behavior to, when the zone is armed and in the *Active* state. The zone can also be configured to trigger the outputs when the zone is in the *Trouble* state, regardless whether the zone is armed or not. The output relays can belong to different Synergis units, as long as the units are all under the same Access Manager.

  IMPORTANT: If the output relays do not belong to the same Synergis unit, you must select the **Activate peer-to-peer** option in the Access Manager. Up to 15 Synergis units can be connected as peers.

  BEST PRACTICE: As much as possible, use the output relays on the master unit. This allows the I/O zone to continue to function when one or more slave units are down.
- **Output behavior:** Select the output behavior to send to the output relays.
- **Activate output on trouble when the zone is disarmed:** Select this option to always trigger the events and the output relays when the zone is in the *Trouble* state, regardless whether the zone is armed or not.
- **Revert to:** Select the output behavior to send to the output relays when the zone returns to the *Normal* state.
- **Associated events:** Events representing the zone states. Select *None* if a zone state should be ignored.
  - **Normal state:** When the combination of inputs yields a zero (0).
  - **Active state:** When the combination of inputs yields a one (1).
  - **Trouble state:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.
  - **Reactivation threshold:** The time period during which the same event should not be re-triggered.

Intrusion detection area - Properties tab

This section lists the settings found in the Intrusion detection area **Properties** tab, in the *Area view* task.

On the *Properties* page, you can do the following:

- View the properties of the intrusion detection area as configured on the *intrusion detection unit*
- Configure the virtual input that lets you trigger intrusion alarms from Security Center
- **Physical name:** Name of the intrusion detection area (sometimes called zone, area, or partition) as it is configured on the physical intrusion panel. Changing the entity name of the intrusion detection area does not change its physical name.
- **Intrusion detection unit:** Entity name of the intrusion detection unit (intrusion panel) where this area is configured.
- **Virtual alarm configuration:** By configuring a virtual alarm, you can trigger intrusion alarms on the intrusion detection area from Security Center, even when the hardware does not support this feature.

  For this to work, you must physically connect an output relay to an input pin on the intrusion panel, and configure them as properties of the intrusion detection area.

  The input so wired is called a *virtual input* ().
- **Devices:** Name, description, and associated cameras of the inputs that define the intrusion detection area. Cameras can be added or removed from the inputs by clicking **Edit the item** ().

Related Topics

Configuring Security Center to trigger intrusion alarms on any intrusion panel on page 1223

Intrusion detection unit configuration tabs

The settings found on the configuration pages of intrusion detection units vary by manufacturer.

For the specific settings, refer to the documentation related to the integration of your intrusion panel into Security Center.

Intrusion detection unit - Properties tab

On the *Properties* page, you can configure the hardware-specific options for the unit.

Intrusion detection unit - Peripherals tab

On the *Peripherals* page, you can view and configure the peripherals (inputs pins and output relays) connected to the intrusion detection unit; including assign cameras to inputs.

You can change the **Name**, **Logical ID**, and **Description** of a peripheral by selecting it and clicking **Edit the item** (✏).

For input pins, you can also change the **Input type**, which changes the icon representing the input pin on maps.

ALPR unit - Properties tab

This section lists the settings found in the ALPR unit **Properties** tab, in the *ALPR* task.

In the *Properties* tab, you can view hardware and software information about the SharpV unit, such as the IP address and port being used. You can also associate a specific hotlist to the SharpV, or link the ALPR camera in the SharpV to an *Omnicast*™ camera, or the SharpV unit's own context camera.

- **Properties:** Displays hardware and software information about the Sharp unit:
  - **IP address:** IP address of the SharpV unit.
  - **Port:** Port used by the *ALPR Manager* to communicate with the SharpV unit.
  - **Version:** AutoVu *PlateReaderServer* software version running on the unit.
  - **Type:** Unit hardware version.
  - **Serial number:** Unit factory installed serial number.
  - **Updater Service version:** Displays the Updater service version running on the Sharp.
  - **Firmware version:** Displays the firmware version running on the Sharp.
- **Network configuration (SharpV units only):**
  - **IP address:** The IP address of the SharpV unit. The ALPR Manager searches for the SharpV unit at this IP address.
  - **Assignment:** How the SharpV unit was enrolled in Security Center:
    - **Passive:** The ALPR Manager discovered the Sharp unit on the network using the discovery port.
    - **Active:** The SharpV unit was added manually in Security Center Config Tool.
  - **Port:** Port used by the *ALPR Manager* to communicate with the fixed Sharp unit.
- **Devices:** Link the ALPR camera to an Omnicast™ camera.
- **File association:** Select how the SharpV unit behaves with hotlists:
  - **Inherit from ALPR Manager role:** The SharpV unit uses the hotlists associated with its parent ALPR Manager. This is the default setting.
  - **Specific:** Associate specific hotlists with the SharpV unit. This allows you to create Event-to-actions in Security Desk that trigger on that specific hotlist. For example, if you're using the SharpV to allow access to a parking lot, you would put the vehicle plates on a hotlist, and then associate that hotlist to the SharpV.

NOTE: To reboot a SharpV camera, click the **Reboot** button found in the toolbar at the bottom of the Config Tool workspace. If the **Reboot** button is not visible, log on to the Sharp Portal *Configuration* page, and then select *Accept remote reboot requests*. For more information, see the administrator guide for your SharpV camera.

Macro configuration tabs

This section lists the settings found in Macro configuration tabs, in the *System* task.

Macro - Properties tab

In the *Properties* tab, you can write your C# code using a basic text editor.

- **Import from file:** Click this button to import the source code from a file.
- **Checking syntax:** Click this button to validate the C# code. If errors are found in the code, they are listed in a dialog box with the line and column numbers where they are found.

Marco - Default execution context tab

In the *Default execution context* tab, you can view the context variables (input parameters) defined in your macro.

Monitor group - Monitors tab

This section lists the settings found in the Monitor group **Monitors** tab, in the *Alarm* task.

In the *Monitors* tab, you can add multiple analog monitors to the monitor group. Later, when you create alarms, you can add a monitor group and its members as a recipient of the alarm.

Network - Properties tab

This section lists the settings found in the Network **Properties** tab, in the *Network view* task.

In the **Properties** tab, you can define the network characteristics and routing information.

- **Capabilities:** Data transmission capabilities for streaming live video on the network.
  - **Unicast TCP:** Unicast (one-to-one) communication using TCP protocol is the most common mode of communication. It is supported by all IP networks, but it is also the least efficient method for transmitting video.
  - **Unicast UDP:** Unicast (one-to-one) communication using UDP protocol. Because UDP is a connectionless protocol, it works better for live video transmission. When the network traffic is busy, UDP is much less likely to cause choppy video than TCP. A network that supports unicast UDP necessarily supports unicast TCP.
  - **Multicast:** Multicast is the most efficient transmission method for live video. It allows a video stream to be transmitted once over the network to be received by as many destinations as needed. The gain could be very significant if there are many destinations. A network supporting multicast necessarily supports unicast UDP and unicast TCP.
    NOTE: Multicast requires specialized routers and switches. Make sure you confirm this with your IT department before setting the capabilities to multicast.
- **IPv4 address prefix:** *IPv4* has two display modes. Click 👁 to select the preferred display mode.
  - **Subnet display:** This mode displays the IPv4 subnet mask as four bytes.
  - **CIDR block display:** The Classless Inter-Domain Routing (CDIR) mode displays the IPv4 subnet mask as a number of bits.
- **IPv6 address prefix:** Version 6 IP address prefix for your network. Your network must support *IPv6* and you must enable the option *Use IPv6* on all your servers using Server Admin.
- **Public servers:** You only need to specify the proxy server when *Network Address Translation* (NAT) is used between your configured networks. The proxy server must be a server known to your system and must have a public port and address configured on your firewall.
- **Routes:** Lists the routes between every two networks on your system, and the route capabilities.

Related Topics

Server - Properties tab on page 1291

Output behavior - Properties tab

This section lists the settings found in the Output behavior **Properties** tab, in the *System* task.

In the *Properties* tab, you can configure the output signal pattern.

- **Output type:** Choose the output type.
  - **State:** Sets the circuit’s state to open or closed.
  - **Pulse:** Sets a pulse to be generated.
  - **Periodic:** Sets a cyclic output to be generated.
- **Delay:** The delay before the pulse or periodic output is generated.
- **Duration:** The duration (in milliseconds) of the pulse.
- **Infinite:** Select this option if the periodic behavior should continue until it is told to stop by another output behavior.
- **Duty cycle:** The ratio of the output signal pattern pulse width divided by the period.
- **Period:** The time for one complete cycle of the output signal pattern.

Overtime rule configuration tabs

This section lists the settings found in Overtime rule configuration tabs, in the *ALPR* task.

Overtime rule - Properties tab

In the *Properties* tab, you can configure the parking regulations enforced by this overtime rule.

- **Color:** Assign a color to the overtime rule. When you select the overtime rule in Genetec Patroller™, the plate reads on the map, and the hit screen, are displayed in this color.
- **Vehicle parking position:** This setting tells the Patroller which set of calibrated parameters to use for the optimal reading of wheel images, based on the parking position of the vehicles: Parallel or Angled (45-degree).
- **Long term overtime:** Use this option for long term parking, where vehicles can park in the same spot for over 24 hours. When Long term overtime is selected, the parking time limit is specified in days (2 to 5 days).
- **Parking enforcement:** Type of restricted parking area that applies to the time limit:
  - **Same position.:** A vehicle is parked overtime if it parks in the same spot beyond the time limit specified.
  - **District:** A vehicle is parked overtime if it is parked anywhere within a city district (a geographical area) beyond the specified time limit.
  - **Block face (2 sides):** A vehicle is parked overtime if it is parked on both sides of a road between two intersections beyond the specified time limit.
- **Regulation:** Defines parameters of the parking time limit:
  - **Time limit:** Enter how long in hours and minutes a vehicle is allowed to park.
  - **Grace period:** Add extra time beyond the *Time limit* before raising an overtime hit. For example, if you set a 10 minute time limit, and a 5 minute grace period, Patroller will raise a hit after 15 minutes.
  - **Applicable days:** Select which days to enforce the *Time limit*.
  - **Applicable hours:** Select what time of day to enforce the *Time limit*.

Overtime rule - Zones tab

In the *Zones* tab, you can configure the parking area where this overtime rule must be enforced. The Parking lot tab displays a map, on which you can add a parking lot, define the number of spaces in the lot, and then draw a polygon on top of the map to represent the physical parking lot. The number of spaces in the lot is used to calculate the percentage of parking occupancy in that area. For more information on how this information is being used in the *Zone occupancy* report, see the *Security Center User Guide*.

NOTE: You can add multiple lots to a map.

Parking facility - Properties tab

This section lists the settings found in the Parking facility **Properties** tab, in the *ALPR* task.

In the *Properties* tab, you can assign an ALPR Manager to the parking facility and configure its sectors and rows for the license plate collection route.

- **AutoVu™ ALPR Manager:** Select the ALPR Manager responsible for creating and managing the *license plate inventory* for this parking facility. Only offloads from MLPI patrol vehicles managed by the same ALPR Manager are used to build the inventory for this parking facility.
- **Configuration:** List of sectors, rows, and space count of the parking facility.
- **Route:** License plate collection route followed by the MLPI units responsible for collecting the license plates for the inventory. The route is downloaded by the patrol vehicles and handheld devices assigned to this parking facility.

Partition - Properties tab

This section lists the settings found in the Partition **Properties** tab, in the *User management* task.

In the *Properties* tab, you can view and manage the partition content.

- **Members:** List of members that are part of the partition.
- **Show:** Filter the members list by entity type.
- **Global partition:** Turn this option on to share the partition with other independent Security Center systems using Global cardholder management.

  NOTE: You cannot share the *root* partition.

Patroller - Properties tab

This section lists the settings found in the Genetec Patroller™ **Properties** tab, in the *ALPR* task.

In the *Properties* tab, you can view information about the computer hosting the Patroller entity (you cannot edit the Patroller properties). You can also configure sound management, acknowledgment buffer settings, and a hit delay for the Patroller unit.

- **Properties:** Lists the properties of the Patroller in-vehicle computer.
  - **IP address:** IP address of the Patroller computer.
  - **Version:** Version number of the Patroller application.
  - **Type:** Patroller installation type(s).
  - **Serial number.:** Serial number of the Patroller.
  - **Machine name:** Name of the Patroller computer.
  - **Updater Service version:** Displays the updater service version running on the Patroller computer.
- **File association:** Select how the Patroller behaves with hotlists and/or permit lists:
  - **Inherit from ALPR Manager role:** Patroller uses the hotlists and permit lists associated with its parent ALPR Manager. This is the default setting.
  - **Specific:** Associate specific hotlists or permit lists with the Patroller unit rather than the ALPR Manager. If you later want to move the Patroller entity to another ALPR Manager on your system, the hotlist or permit list will follow.
- **Sound management:** Configure Patroller to play a sound when reading a plate and/or generating a hit, and choose whether sounds should be played even when Patroller is minimized.
  - **Play sound on hit:** Plays a sound when Patroller generates a hit.
  - **Play sound on read:** Plays a sound when Patroller reads a plate.
  - **Play sounds even when minimized:** Play sounds even if the Patroller window is minimized.
- **Acknowledgment buffer:** Specify a buffer restriction that limits how many hits can remain unacknowledged (not accepted or rejected) before Patroller starts automatically rejecting *all* subsequent hits. You can also choose (by priority) which hotlists should comply with this restriction.
  - **Reject count:** How many unacknowledged hits are allowed.
  - **Reject priority:** When you create a hotlist entity, you can specify a priority for that hotlist. This setting tells Patroller which hotlist(s) should comply with the buffer restriction.
- **Hotlist and permit:** Specify the *Duplicate hit delay* that tells Patroller to disregard multiple hits on the same plate for the duration of the delay. For example, if you set a delay of 10 minutes, no matter how many times Patroller reads the same plate during those 10 minutes, it will generate only one hit.

Permit - Properties tab

This section lists the settings found in the Permit **Properties** tab, in the *ALPR* task.

In the *Properties* tab, you can configure the parsing of the source permit data file.

- **Path:** Path to the permit source text file that contains the permit data, such as license plate numbers and other related vehicle information. The source text file can be located on the ALPR Manager computer's local drive (for example, the C drive), or on a network drive that is accessible from the ALPR Manager computer.
- **Use delimiters:** Tells Security Center that the fields in the permit list file vary in length, and indicates the character used to separate each field in the file. By default, *Use delimiters* is set to *On*, and the delimiter specified is a *semi-colon* (;). If your permit list file is made up of fixed length fields, set *Use delimiters* to *Off*.
- **Visible in editor:** Allow a user to edit the hotlist or permit list using the Hotlist and permit editor task.
- **Attributes:** Tells Security Center the name and order of the fields (attributes) in the source text file.

Permit restriction configuration tabs

This section lists the settings found in Permit restriction configuration tabs, in the *ALPR* task.

Permit restriction - Properties tab

In the *Properties* tab, you can configure the restrictions for the individual permits that apply to the parking area represented by the rule.

- **Color:** Color used to represent the permit restriction in Security Desk. In Genetec Patroller™, permit restrictions are always green for regular permit hits, or blue for shared permit hits. A read is displayed as a triangular-shaped icon in the selected color on the map, when an permit restriction is in effect. When a read violates one of the restrictions, the icon is encircled with a red ring. It indicates a permit hit.
- **Permits:** The permits the time restriction applies to.
  - *Everyone***:** Parking is available to everyone, regardless of whether they have a permit or not. No restriction is enforced during the specified time period. This restriction is used with other restrictions as a temporary override. For example, if a university is hosting a football game, parking would be made available to everyone during the game instead of specific permit holders.
  - *No permit***:** Only vehicles without permits can park. For example, you can use this type of restriction to reserve a zone for visitors parking. A plate read that matches any of the permits downloaded to the Patroller raises a hit.
  - *All permits***:** Only vehicles with a permit can park. A plate read that does not match any of the permits downloaded to the Patroller raises a hit.
  - *Specific permits***:** Only vehicles having one or more of the specified permits can park. A plate read that does not match any of the specified permits raises a hit.
- **Days:** Days of the week when parking is allowed.
- **Hours:** Time during the day when parking is allowed.
- **Validity:** Dates when parking is allowed.

Permit restriction - Zones tab

In the *Zones* tab, you can configure the parking area where this overtime rule must be enforced. The Parking lot tab displays a map, on which you can add a parking lot, define the number of spaces in the lot, and then draw a polygon on top of the map to represent the physical parking lot. The number of spaces in the lot is used to calculate the percentage of parking occupancy in that area. For more information on how this information is being used in the *Zone occupancy* report, see the *Security Center User Guide*.

NOTE: You can add multiple lots to a map.

Schedule - Properties tab

This section lists the settings found in the Schedule **Properties** tab, in the *System* task.

The *Properties* tab lets you configure the time constraints that define the schedule.

Date coverage

In the *Date coverage* section, you can define a date pattern or specific dates to be covered by the schedule.

- **Daily:** Defines a pattern that repeats every day.
- **Weekly:** Defines a pattern that repeats every week. Each day of the week can have a different time coverage. This option is not available for twilight schedules.
- **Ordinal:** Defines a series of patterns that repeat on a monthly or yearly basis. Each date pattern can have a different time coverage. For example, on July 1st every year, on the first Sunday of every month, or on the last Friday of October every year.
- **Specific:** Defines a list of specific dates in the future. Each date can have a different time coverage. This option is ideal for special events that occur only once.

Time coverage

In the *Time coverage* section, you can define which time periods apply during a 24-hour day.

- **All day:** Covers the entire day. This option is not available for twilight schedules.
- **Range:** Covers one or multiple discrete time periods within the day. For example, from 9 am to 12 pm and from 1 pm to 5 pm This option is not available for twilight schedules.
- **Daytime:** Covers from sunrise to sunset. This option is only available for twilight schedules.
- **Nighttime:** Covers from sunset to sunrise. This option is only available for twilight schedules.

Scheduled task - Properties tab

This section lists the settings found in the Scheduled task **Properties** tab, in the *System* task.

In the *Properties* tab, you can configure the behavior of the scheduled task.

- **Status:** Turns the scheduled task on or off.
- **Recurrence:** Specifies when and how often the scheduled task is run.
  - **Once:** Executed once at a specific date and time.
  - **Every minute:** Executed every minute.
  - **Hourly:** Executed at a specific minute of every hour.
  - **Daily:** Executed at a specific time every day.
  - **Weekly:** Executed at a specific time on one or more days of the week
  - **Monthly:** Executed at a specific time on the same day every month.
    CAUTION: Tasks scheduled on day 29, 30, or 31 are not run in shorter months that do not include the selected day.
  - **Yearly:** Executed at a specific time on the same day every year.
  - **On startup:** Executed on system startup.
  - **Interval:** Executed at regular intervals that can be days, hours, minutes, or seconds.
- **Action:** Specifies an action to execute at the scheduled time.
- **Additional parameters:** Additional information might be required, depending on the selected action type.

Related Topics

Action types on page 1434

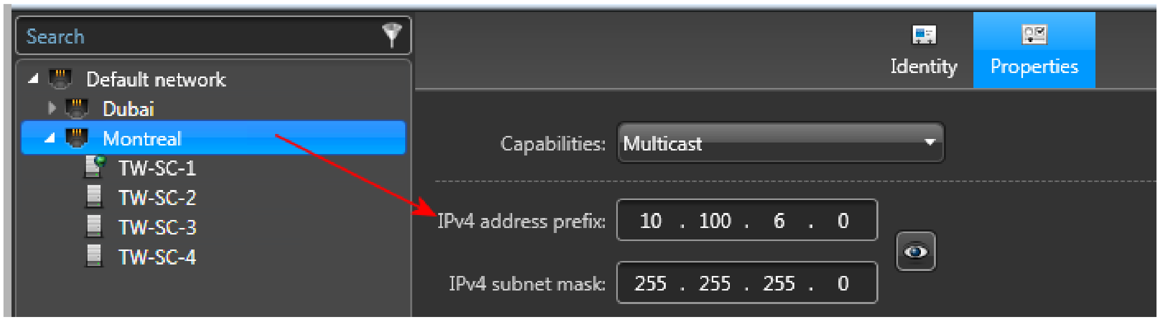
Server - Properties tab

On the server **Properties** tab, you can view the network settings configured for this server in Server Admin.

NOTE: All network settings are read-only in Config Tool. They must be configured in Server Admin.

- **Public address:** Public address of this server. This setting appears only if a public address is configured in Server Admin.
  - **Port:** Port used by the Genetec™ Server service to listen to commands received from other Security Center servers on the public address.
  - **Proxy:** This switch is turned on if this server is configured as a proxy server for a private network protected by a firewall.
- **Private addresses:** List of *private IP addresses* used for the communication between Security Center servers. Only the private addresses enabled in Server Admin appear in this list.
  - **Port:** Port used by the Genetec™ Server service to listen to commands received from other Security Center servers on the private addresses.

  IMPORTANT: If the server is running in backward compatibility mode (5.2 or earlier), the first address in the private address list must match the IPv4 properties of the network entity the server belongs to in the Network view task.



Capabilities: Multicast

IPv4 address prefix: 10 . 100 . 6 . 0

IPv4 subnet mask: 255 . 255 . 255 . 0

- **Secure communication:** Use this section to view the current *identity certificate* used by the server to communicate with other Security Center servers.
  - **Issued to:** Subject of the current certificate. A *self-signed certificate* created at software installation appears in the form *GenetecServer-{MachineName}*.
  - **Issued by:** Name of the *certificate authority (CA)* that issued the certificate. The issuer and the subject are the same for self-signed certificates.
  - **Valid from/Expiration:** Validity period of the current certificate.

  Click **View** to open the dialog box to view more information.

Related Topics

What is Transport Layer Security protocol? on page 461

Network - Properties tab on page 1281

Server Admin - Overview page on page 99

Server Admin - Main server page on page 102

Server Admin - Expansion server page on page 105

Tile plugin - Properties tab

This section lists the settings found in the Tile plugin **Properties** tab, in the *Area view* task.

In the *Properties* tab, you can link the tile plugin entity to a website or a .dll file.

- **Web page:** Type a web address to link the tile plugin to.
- **Modify:** Select a .dll to link the tile plugin to.

User configuration tabs

This section lists the settings found in User configuration tabs, in the *User management* task.

User - Properties tab

In the *Properties* tab, you can configure the user's personal information and password.

- **Status:** Activate or deactivate the user profile. A user cannot log on when their profile is deactivated. Deactivating a user's profile while the user is logged on will immediately log off the user.
- **Personal information:** The personal information of a user can be imported from your company's directory service.
  - **First and last name:** First and last name of the user.
  - **Email address:** The email address of the user. Can be used to send emails, reports, or messages to the user.
- **Password settings:** All users require a password to log on to Security Center. The user must have the *Change own password* privilege for the password options to be enabled.
  - **Expires:** Turn this option on to force the user to change their password after a given number of days.
  - **Change on next logon:** Turn this option on for Genetec Patroller™ or Security Desk to force the user to change their password the next time they log on.
  - **Change password:** To change the password of another user, you need the *Modify user properties* privilege.
- **User level:** Set the user level. A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera PTZ, viewing the video feed from a camera, or staying logged on when a threat level is set. Level 1 is the highest user level, with the most privileges.
  - **Inherit from parent:** The user level can be inherited from a parent group. If the user has multiple parents, the highest user level is inherited. If the user has no parent group, the lowest user level (254) is inherited. You must set *Inherit from parent* option to **Override** in order to change this setting.
  - **Configure user-level overrides:** Set a different user level for the selected areas or cameras. These override values take precedence over the general user level for the cameras you specify.

    NOTE: If you override the user level for an area, it applies to all cameras in that area.

User - Access rights tab

In the *Access rights* tab, you can view and configure the user's access rights over *partitions*. This tab only appears when user-created partitions exist in the system.

- **List of partitions:** Select a partition to grant access rights for that partition to the user. Access rights over parent and child partitions can be configured independently. Access rights inherited from parent user groups cannot be revoked.
- **Administrator:** Select this option to grant full administrative rights over all entities contained in that partition to the user, including the rights to create and delete users, user groups, and child partitions.
- **Display checked items (▼):** Click to toggle the display between showing only selected partitions and all partitions.

User - Privileges tab

In the *Privileges* tab, you can view and configure the user's privileges. The privileges of a user can be inherited from parent user groups.

- **Allow:** The privilege is granted to the user.
- **Deny:** The privilege is denied to the user.
- **Undefined:** This privilege must be inherited from a parent user group. If the user is not a member of any group, or if the privilege is also undefined to the parent user group, then the privilege is denied.
- **Exceptions:** Basic privileges can be superseded at the partition level if the user is authorized to access multiple partitions. Only *Administrative* and *Action* privileges, plus the privileges over public tasks, can be overwritten at the partition level.
- **Additional settings (⚙):** Click to view additional commands for privilege templates.
  - **Apply template:** Select one of the privilege templates to apply.
  - **Set configuration to read-only:** Set all entity configuration privileges found under the *Administrative privileges* group to *View properties*.
  - **Set configuration to read-write:** Allow the modification of all entity configurations, including *Add* and *Delete*.

User - Advanced tab

In the *Advanced* tab, you can configure the user’s advanced settings.

- **Logon settings:** Configure the user’s logon settings.
  - **User logon schedule:** Restrict the user logon according to schedules. A schedule can either be used to allow user logon or to block user logon.
  - **Logon supervisor of:** Lists the users whose logons are supervised by this current user. When a user in this list needs to log on to the system, the current user must also provide their username and password to complete the logon. A user can have more than one logon supervisor.
  - **Limit concurrent logons:** Set the maximum number of different workstations a user can log on to at the same time. This limit only applies to Security Desk. Config Tool is not restricted by this setting.
  - **Auto-lock:** Set this option to **ON** to lock the user out of their Security Desk session after a period of inactivity. To resume their current session, the user must re-enter their password. This requirement can be inherited from a parent user group. You must set **Inherit from parent** to **Override** in order to change this setting.
    NOTE: If the user is authenticated through ADFS with passive authentication, the user will be logged off and their current session closed instead of being locked.
- **Security Desk settings:** Configure the user’s Security Desk workspace.
  - **List of active tasks:** Displays the tasks found in the user’s active task list.
  - **Hot actions:** Displays the *hot actions* mapped to the PC keyboard function keys (Ctrl+F1 through Ctrl+F12) when this user is logged on to Security Center using Security Desk.
  - **Allow remote control over:** Lists the Security Desk workstations this user is allowed to control remotely using the *Remote* task in Security Desk, or a CCTV keyboard. You can specify which workstations can be controlled by user, user group, or by specific workstation.
  - **Start task cycling on logon:** Turn this option on so that next time the user logs on from Security Desk *task cycling* starts automatically.
- **Security settings:** Configure what the user can see in the system.
  - **Limit archive viewing:** Turn this option on to restrict the user's ability to view archived video to the last *n* days. This limitation can be inherited from a parent user group. If the user has multiple

  parents, the most restrictive limitation is inherited. If the user has no parent group, no restriction will be imposed. You must set **Inherit from parent** to **Override** to change this setting.
  - **Scramble entity names:** (Only non-administrative users) Turn this option on to display the entity GUID in Security Desk and Config Tool, everywhere the entity name is supposed to be displayed for this user. This option also prevents the user from updating the entity name fields in Config Tool.
  - **Include additional properties on export/snapshot:** Turn this option on to enable the user to include metadata to exported videos or snapshots, such as camera name, creation date, and camera coordinates, which can be useful for investigation.
  - **Enable video watermarking:** Turn this option on to overlay an identifying text on all video requested by this user through Config Tool, Security Desk, Web Client or Genetec™ Web App. Click **Configure** to set the overlaid text. The *video watermark* can be inherited from a parent user group. If the user has multiple parents, only the video watermark from the first parent group is inherited. You must set **Inherit from parent** to **Override** to change this setting.
  - **Manage partition memberships:** Turn this option on to grant the *Manage partition memberships* privilege to the user. With this option enabled, the user can copy and move any type of entity from one partition to another to which they have access. If the user has multiple parents, the most restrictive limitation is inherited. You must set **Inherit from parent** to **Override** to change this setting.
- **Default map:** The map loaded by default when the user opens the *Maps* task. The default map can be inherited from a parent user group. In a multiple-parent hierarchy, where the user has more than one parent, only the default map from the direct parent group is inherited. To select a personalized default map for the user, you must change the **Default map** setting from **Inherit from parent** to **Override**.

Related Topics

Configuring video watermarking on page 449

User group configuration tabs

This section lists the settings found in User group configuration tabs, in the *User management* task.

User group - Properties tab

In the *Properties* tab, you can view and configure the members of the user group.

- **External unique identifier:** Only used for *third-party authentication*. This field is used to match groups coming from an external identity provider to user groups in Security Center. This identifier defaults to the group name. If your identity provider uses a separate ID to identify groups, that ID must be added here.
- **Email address:** Email address that is used by all members of the group. This information can be imported from your company's directory service. The email address can be used to send emails, reports, or messages to the users.
- **User level:** Set the user level. A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera PTZ, viewing the video feed from a camera, or staying logged on when a threat level is set. Level 1 is the highest user level, with the most privileges.
    - **Inherit from parent:** The user level can be inherited from a parent group. If the user has multiple parents, the highest user level is inherited. If the user group has no parent group, the lowest user level (254) is inherited. You must set **Inherit from parent** option to *Override* in order to change this setting.
    - **Configure user-level overrides:** Set a different user level for the selected areas or cameras. These override values take precedence over the general user level for the cameras you specify.

      NOTE: If you override the user level for an area, it applies to all cameras in that area.
- **Members:** List of user group members. By default, the members inherit the privileges and partition rights of the user group.

User group - Access rights tab

In the *Access rights* tab, you can view and configure the access rights shared by the members of the user group. This tab only appears when user-created partitions exist in the system.

- **List of partitions:** Select a partition to grant access rights for that partition to the user group. Access rights over parent and child partitions can be configured independently. Access rights inherited from parent user groups cannot be revoked.
- **Administrator:** Select this option to grant full administrative rights over all entities contained in that partition to the user group, including the rights to create and delete users, user groups, and child partitions.
- **Display checked items (▾):** Click to toggle the display between showing only selected partitions and all partitions.

User group - Privileges tab

In the *Privileges* tab, you can view and configure the user group's privileges. The privileges of a user group can be inherited by the members of the group, or can be inherited from other user groups.

- **Allow:** The privilege is granted to the user group.
- **Deny:** The privilege is denied to the user group.
- **Undefined:** This privilege must be inherited from a parent user group. If the user group is not a member of any other group, or if the privilege is also undefined to the parent user group, then the privilege is denied.

- **Exceptions:** Basic privileges can be superseded at the partition level if the user group is authorized to access multiple partitions. Only *Administrative* and *Action* privileges, plus the privileges over public tasks, can be overwritten at the partition level.
- **Additional settings (⚙):** Click to view additional commands for privilege templates.
  - **Apply template:** Select one of the privilege templates to apply.
  - **Set configuration to read-only:** Set all entity configuration privileges found under the *Administrative privileges* group to *View properties*.
  - **Set configuration to read-write:** Allow the modification of all entity configurations, including *Add* and *Delete*.

User group - Advanced tab

In the *Advanced* tab, you can configure common advanced settings for the group members.

- **Logon settings:** Configure the common logon settings for the group members.
  - **Logon supervisor of:** Lists the users whose logons are supervised by the members of this user group. When users from this list need to log on to the system, any member of this user group can help them complete their logon.
  - **Auto-lock:** Set this option to **ON** to lock members of the user group out of their Security Desk session after a period of inactivity. To resume their current session, the user must re-enter their password. This requirement can be inherited from a parent user group. You must set **Inherit from parent** to *Override* in order to change this setting.
    NOTE: If the user is authenticated through ADFS with passive authentication, the user will be logged off and their current session closed instead of being locked.
- **Security Desk settings:** Configure the common Security Desk settings for the group members.
  - **Allow remote control over:** Lists the Security Desk workstations the members of this user group are allowed to control remotely using the *Remote* task in Security Desk, or a CCTV keyboard. You can specify which workstations can be controlled by user, user group, or by specific workstation.
- **Limit archive viewing:** Turn this option on to restrict the user group's ability to view archived video to the last *n* days. This limitation can be inherited from a parent user group. If the user group has multiple parents, the most restrictive limitation is inherited. If the user group has no parent group, no restriction will be imposed. You must set **Inherit from parent** to *Override* to change this setting.
- **Enable video watermarking:** Turn this option on to overlay an identifying text on all video requested by this user group through Config Tool, Security Desk, Web Client, or the Genetec™ Web App. Click **Configure** to set the overlaid text. The *video watermark* can be inherited from a parent user group. If the user group has multiple parents, only the video watermark from the first parent group is inherited. You must set **Inherit from parent** to **Override** to change this setting.
- **Manage partition memberships:** Turn this option on to grant the *Manage partition memberships* privilege to the user group. With this option enabled, the user group can copy and move any type of entity from one partition to another to which they have access. If the user group has multiple parents, the most restrictive limitation is inherited. You must set **Inherit from parent** to **Override** to change this setting.
- **Default map:** The map loaded by default when a user belonging to this user group opens the *Maps* task. The default map can be inherited from a parent user group. In a multiple-parent hierarchy, where the user group has more than one parent, only the default map from the direct parent group is inherited. To select a personalized default map for the group, you must change the **Default map** setting from **Inherit from parent** to **Override**

Related Topics

Configuring video watermarking on page 449

Video unit - Identity tab

This section lists the settings found in the Video unit **Identity** tab, in the *Video* task.

In the *Identity* tab, you can view hardware-specific information, in addition to the standard entity information (name, description, logical ID, and so on).

- **Manufacturer:** Manufacturer of the video unit.
- **Product type:** Model of the video unit.
- **Firmware version:** Current firmware version installed on the video unit.
- **Proposed:** Displays the recommended firmware version. If the firmware version is the same as the proposed version, it will display *Up to date*.
- **Upgrade (☢):** Upgrade the firmware on the video unit.
- **Audio:** Indicates whether the video unit supports audio.
- **SSL:** Indicates whether the video unit supports *SSL* (Secure Socket Layer protocol).

Video unit - Properties tab

This section lists the settings found in the video unit **Properties** tab, in the *Video* task.

In the *Properties* tab, you can configure the information required by the Archiver to connect to this unit and other data transmission properties. These settings vary from one manufacturer to another. Additional options might be available, depending on the unit type.

- **IP address:** Set the IP address of the video unit.
- **Obtain network settings dynamically (DHCP):** Select this option to have the IP address assigned dynamically by your DHCP (Dynamic Host Configuration Protocol) server.

  NOTE: Do not use this option unless your DHCP server is configured to always assign the same IP address to the same device.
- **Specific settings:** Select this option to enter a fixed address. This can be the IP address you entered when you initially created the video unit entity. However, if using a NAT or VPN, then the local IP and public IP are different. You need to enter the following fields:
  - *Local IP*. Fixed IP address.
  - *Subnet mask*. The subnet mask tells the unit which peripherals it can communicate with directly. Anything that does not belong to the same subnet must go through the Gateway.
  - *Gateway*. IP address of the gateway. It must be on the same subnet as the unit.
- **Public IP:** The public IP (WAN) address used to add the video unit to Security Center. This field cannot be edited.
- **Command port:** The port used by the Archiver to connect to the video unit. The command port is sometimes called the HTTP port by some manufacturers.
- **Discovery port:** The port used for automatic discovery. Not all manufacturers supports this feature.
- **VSIP port:** (Only for Verint units) On Verint units, both the command port and discovery port are replaced by the *VSIP port*.
- **Authentication:** Credentials used by the Archiver to connect to the video unit.
  - **Use default logon:** Select this option for the Archiver to use the credentials defined in the unit manufacturer’s extension.
  - **Specific:** Select this option for the Archiver to use specific credentials to connect to this unit. The fields you need to fill in depend on the unit manufacturer.
  - **Use HTTPS:** Select this option to use HTTPS communication instead of HTTP (default).
- **Bit rate:** Use this option to limit the maximum bit rate allowed for this unit. Setting a limit to the bit rate helps prevent one unit from using up all the bandwidth available on the network.
- **Enable UPnP:** Select this option to enable the UPnP (Universal Plug and Play) protocol. Disable UPnP if you do not want the unit to be discovered by other Windows applications.
- **Enable Bonjour:** Select this option to enable the Bonjour protocol. Disable Bonjour if you are not using zero-configuration networking.
- **Enable link-local address:** Select this option to enable the use of link-local address.
- **Event stream connection type:** Select the connection type (HTTP or TCP) used for sending events. The use of TCP is recommended. Select HTTP if there is a firewall between the Archiver and the unit.
- **Application events:** (Axis only) List of ACAP applications installed on the unit. Select the applications you want to enable.

  NOTE: To enable the AXIS Video Motion Detection (VMD) application, you must select the **Use camera application motion detection** option from the *Motion detection* tab of the camera.

Related Topics

Changing video unit passwords on page 574
Viewing video unit password history on page 576

Video unit - Peripherals tab

This section lists the settings found in the Video unit **Peripherals** tab, in the *Video* task.

In the *Peripherals* tab, you can view all the peripheral devices (inputs/outputs, audio encoders/decoders) found on the unit that are not explicitly shown as entities, such as the *video encoders* or *video decoders*.

- **Peripheral State (LED):**
  - Green (🟢): Active peripheral.
  - Red (🔴): Peripheral disabled by user.
  - Yellow (🟡): Peripheral activation in progress.

    NOTE: If the LED stays yellow, it indicates that the peripheral is either not supported or has problems, in which case it is recommended to disable it.
- **Name:** Logical name. It is the same as the physical name by default.
- **Logical ID:** Logical identifier.
- **Description:** Description of the device.

You can also modify the selected peripheral devices.

- **Edit the item (✏️):** Change the settings of the selected peripheral device.
- **Enable/Disable selected items (🟢/🔴):** Enable or disable the selected peripheral devices.

Output relay settings

The setting specific to output relays is as follows:

- **Default mode:** Default state of the output relay.
  - **Normally option:** The normal contact state of the output is open.
  - **Normally closed:** The normal contact state of the output is closed.

Speaker settings

The settings specific to speakers (*audio decoder* devices) are as follows:

- **Volume:** Desired volume level (0 to mute, 100 equals maximum volume).
- **UDP port:** Port number used when the connection type is unicast UDP.
- **Connection type:** Connection type that is used between the unit and the Archiver for this audio decoder.

Microphone settings

The settings specific to microphones (*audio encoder* devices) are as follows:

- **Data format:** Audio compression format.
- **Input type:** Type of input source.
  - **Line in:** Used for pre-amplified source.
  - **Mic in:** Use this if the microphone is directly connected to the unit. In this case, the signal is amplified by the hardware.
  - **Internal:** Use microphones integrated to the unit.
- **Sensitivity:** Desired amplification level (default=68). The lower the level, the less sensitive the microphone is to ambient noise, but the recording level will also be lower.

- **UDP port:** Port number used when the connection type is unicast UDP.
- **Connection type:** Connection type that is used between the unit and the Archiver for this audio encoder.
- **Multicast address:** The *multicast* address and *port number* are assigned automatically by the system when the video unit is discovered. Each audio encoder is assigned a different multicast address with a fixed port number. This is the most efficient configuration.

Virtual zone configuration tabs

Virtual zones are controlled by the Zone Manager role. Virtual zones are used to combine inputs and trigger outputs that belong to different units of different types. Virtual zones can be armed and disarmed from Security Desk or using *Arm zone* and *Disarm zone* actions.

Virtual zone - Properties tab

Click the **Properties** tab to configure the inputs that define this zone, and define how they are evaluated.

- **Zone Manager:** Zone Manager role that controls the virtual zone.
- **Inputs:** Inputs combined to evaluate the zone state.
- **Operator:** Logical operator used to combine the input states to evaluate the zone state.
- **Associated events:** Events representing the zone states. Select *None* if a zone state should be ignored.
  - **Normal state:** When the combination of inputs yields a zero (0).
  - **Active state:** When the combination of inputs yields a one (1).
  - **Trouble state:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.
  - **Reactivation threshold:** The time period during which the same event should not be re-triggered.

Virtual zone - Arming tab

Click the **Arming** tab to configure the arming source of your zone and its arming behavior.

- **Arming source:** Select the schedules corresponding to the periods when the zone is armed.
- **Delays:** Optional delays that give you time to leave the premises after arming the zone, and time to disarm the zone after tripping a sensor.
  - **Arming delay:** Duration (mm:ss) you want between the time the zone is armed and the time the event triggers become active.
  - **Entry delay:** Duration (mm:ss) you want between the time the entry sensor is tripped and the time the events are triggered. This option allows you to disarm the zone before triggering the output relays.

58

Role types

This section includes the following topics:

- "Zone Manager configuration tabs" on page 1392

Access Manager configuration tabs

You configure the settings of the Access Manager role from the **Roles and units** view of the *Access control* task in Security Center Config Tool.

Access Manager - Properties tab

Click the **Properties** tab to configure the general settings of the Access Manager.

- **Keep events:** Specify how long you want to keep the events in the Access Manager database before deleting them. The access control event are used for reporting and maintenance purposes (they include events related to doors, elevators, areas, and other access control entities).
  - **Indefinitely:** Keep the events until you manually delete them.
  - **For:** Select the number of days for the retention period.

  CAUTION: If you are using the *SQL Server 2014 Express* database engine (included with the Security Center installation files), the database size is limited to 10 GB. A door event uses (on average) 200 bytes in the database. If you configure the Access Manager to keep door events indefinitely, the database eventually reaches the 10 GB limit and the engine stops.
- **Activate peer-to-peer:** Select this option to enable the communication between Synergis units managed by this Access Manager. Up to 15 units can be connected as peers, supporting a maximum of 512 outputs and 128 inputs in I/O linking configurations.

  BEST PRACTICE: Only enable peer-to-peer communication if you plan to create I/O zones that involve multiple Synergis units, or apply antipassback to areas controlled by multiple Synergis units. Leave this option off for better system security and performance.
- **Activate global antipassback:** Select this option if you need to apply antipassback to areas controlled by multiple Synergis units. To enable this option, you must first enable peer-to-peer.

  BEST PRACTICE: If all your antipassback areas are controlled by a single unit, do not enable global antipassback. Enabling global antipassback increases the communication between Synergis units.
- **Include identifiable personal data in synchronization:** (Synergis units only) Select this option to sync cardholder names with the Synergis units. If this option is cleared (default), only credentials without personal data are synced. Enable this option when you have devices that can display cardholder names and you want them to appear.
- **Minimal cardholder synchronization:** Select this option to minimize the number of cardholders the Access Manager needs to synchronize with its units. This option is only recommended for large systems and requires following specific design guidelines. It is disabled by default.

Access Manager - Extensions tab

Click the **Extensions** tab to configure the manufacturer-specific connection parameters shared by access control units that are controlled by this Access Manager.

- **Genetec™ Synergis™:** Extension for all Synergis units. This extension requires at least one discovery port. For more information, see the *Synergis™ Appliance Configuration Guide*.
- **HID VertX:** Extension for all HID units, including the legacy VertX models (V1000 and V2000), the VertX EVO, and the Edge EVO controllers. For the complete list of supported controller units and firmware, see the *Security Center Release Notes*.

Access Manager - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role. All must have access to the role database.

- **Database status:** Current status of the database.
- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.
- **Database:** Name of the database instance.
- **Actions:** You can perform the following functions on the role database:
  - **Create a database (✚):** Create a new database with the option to overwrite the existing one.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (🔔):** Set up notifications for when the database space is running low.
  - **Resolve conflicts (⚠):** Resolve conflicts caused by imported entities.
  - **Backup/Restore (▭):** Back up or restore the database.
- **Authentication:** Specifies which SQL Server authentication is to be used:
  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.

Related Topics

Creating databases on page 140

Deleting databases on page 141

Viewing database information on page 145

Receiving notifications when databases are almost full on page 146

Backing up databases on page 147

Restoring databases on page 151

Resolving conflicts caused by imported entities on page 487

About minimal cardholder synchronization on page 761

Active Directory configuration tabs

You configure the settings of the Active Directory role from the **Roles** view of the *System* task in Security Center Config Tool.

Active Directory - Properties tab

Click the **Properties** tab to define the parameters for how the Active Directory role operates.

- **Connection status:** Connection status between the role and the corporate AD.
- **Status:** Shows what the role is doing. *Idle* is the normal status. If there is a problem, an error message is displayed.
- **Active Directory:** AD Fully Qualified Domain Name (FQDN), hostname or IP address of the corporate AD server.
  - **Use Windows credentials:** You can use the Windows credentials used for running the *Genetec Server* service, or specify a different set of Windows usernames and passwords. In both cases, the credentials you specify must have read and write access to the specified corporate AD.
  - **Use SSL connection:** Select this option to encrypt LDAP (Lightweight Directory Access Protocol) network traffic. LDAP is the protocol used for communication between the Active Directory role and the AD. The default port used for encrypted communication is 636. If you use a different port, you need to explicitly specify it by appending the port number after the AD server name, separated by a colon (':').
  - **Use a specific domain controller:** Select this option and specify the name of your domain controller if you have one that is dedicated to Security Center.
- **Partition:** Default *partition* where the entities synchronized with the corporate AD are created if the partition is not mapped to an AD attribute.

  NOTE: If the partition property is changed, only newly created or synchronized entities are added to the new partition. Existing entities remain in the partition originally selected the first time it was synchronized.
- **Synchronized groups:** List of all AD security groups imported as user groups, cardholder groups, or both.
- **No scheduled task exists to synchronize this role. :** This warning message appears if you have not configured a scheduled task to automatically handle synchronization with the corporate AD.
- **Synchronize now. :** Synchronize with the Active Directory now. You should always synchronize after making changes to the synchronized groups.

Active Directory - Links tab

Click the **Links** tab to map AD attributes to Security Center fields.

- **Cardholder:** Map AD attributes to Security Center cardholder fields.
- **Upload pictures to Active Directory:** Select this option if you want the pictures you assign to imported cardholders from Security Center to be uploaded to the AD.
- **Maximum uploaded picture file size:** This parameter only appears if *Upload pictures to Active Directory* is selected. It servers to limit the file size of the pictures you upload from Security Center to the AD.
- **Card format:** Select the default card format to use for the imported cardholder credentials when the card format property is either not mapped to an AD attribute, or when the mapped attribute is empty.
- **Badge template:** Select a default badge template to use for the imported cardholder credentials.
- **Custom fields:** Map additional AD to Security Center custom fields.

Active Directory - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Active Directory role does not require a database.

- **Servers:** Servers hosting this role. All must have access to the role database.

ALPR Manager - Properties tab

In the ALPR task on the *Properties* tab, you can configure the general ALPR Manager role settings and optional AutoVu™ features. The availability of certain features depends on your Security Center license.

General settings

Use the *General settings* to configure the *Root folder* for the ALPR Manager, the user group for the Genetec Patroller™ installations, and how long the data from the ALPR Manager is kept in the database.

- **Root folder:** Main folder on the computer hosting the ALPR Manager, where all the configuration files are created, saved, and exchanged between the ALPR Manager and the Patroller units it manages.
- **Optimize Root folder disk space:** Enable the use of symbolic links to reduce disk utilization when the same file is replicated in multiple folders, such as when you have large hotlists or permit lists associated to individual Patroller units. This reduces the Root folder's overall disk space, and optimizes file transfer performance to the Patroller in-vehicle computer.

  IMPORTANT: If your root folder is on a network drive, the Genetec™ Server service must be configured to run using a domain user and not a local user.
- **User group for Patrollers:** List of users (and their passwords) who are allowed to log on to the patrol vehicles managed by the ALPR Manager. This list is downloaded to the patrol vehicles.
- **Retention period:** Specify how many days of ALPR-related data Security Center can query. The default is 90 days, and the maximum is 4000 days. The ALPR date that is older than the values specified do not appear in Security Center queries and reports (Hit reports, Read reports, and so on).
  - **Genetec Patroller™ route retention period:** Number of days the Patroller *route* data (GPS coordinates) is kept in the database.
  - **Hit retention period:** Number of days the hit data is kept in the ALPR Manager database.
  - **Hit image retention period:** Number of days the hit image data is kept by the linked Archiver role. The *Hit image retention period* cannot exceed the *Hit retention period* since a hit image is always associated with a hit.
  - **Read retention period:** Number of days the *license plate reads* are kept in the ALPR Manager database. The *Read retention period* cannot exceed the *Hit retention period*. If the read retention is lower than the hit retention, only the reads that are associated with hits are kept.
  - **Read image retention period:** Number of days the read image data is kept by the linked Archiver role. The *Read image retention period* cannot exceed the *Read retention period* since a read image is always associated to a read.
  - **Event retention period:** Number of days Patroller events (user logged on, logged off, and patrol vehicle positions) are kept in the ALPR Manager database.
  - **Parking occupancy retention period:** Number of days the parking occupancy data is kept in the ALPR Manager database.
  - **Parking zone data retention period:** Number of days the parking zone data is kept in the ALPR Manager database. This data includes parking session information, for example, parking session start times and state transitions, as well as information on the events that occur within the parking zone. The *Parking zone data retention period* cannot exceed the *Read retention period*.

Live

The *Live* settings are used to configure how data is transferred between Security Center and SharpV cameras, and also between Security Center and Patroller.

NOTE: You only need to configure the Live settings if you are enrolling a Sharp camera running SharpOS 12.6 or earlier, or if you are configuring a Patroller connection.

- **Listening port:** Port used to listen for connection requests coming from SharpV cameras. After the connection is established, the ALPR Manager can receive live updates from the *ALPR units* it manages.

  NOTE: If you are using multiple ALPR Managers, each ALPR Manager must use a different listening port.
- **Sharp discovery port:** Port used by the ALPR Manager to find fixed SharpV units on the network. The same port number must be used in the *Discovery port* setting on the SharpV.

  NOTE: When setting the discovery port, do not use port 5050 as it is reserved for the logger service.
- **Send on read (SharpV units only):** The SharpV images that are sent to Security Center for each plate read. These images are displayed in Security Desk when monitoring ALPR events.

  NOTE: This Live setting also applies when using the LPM protocol.

  - **License plate image:** Include the high resolution close-up image of the license plate along with the plate read data.
  - **Context image:** Include the wide angle context image of the vehicle along with the plate read data.
- **Channel security:** Encrypt communication between Security Center and Patroller.

  IMPORTANT: If you select this option, encryption must also be enabled in Patroller Config Tool.

  - **Encrypt communication channel:** Encrypt communication between Patroller and Security Center.
  - **Accept non encrypted messages:** Security Center will accept incoming connections from patrol vehicles that do not have the encryption option enabled.

LPM protocol

When a Sharp camera (SharpOS 12.7 or later with the LPM protocol enabled) connects to the ALPR Manager role, the connection is managed by the LPM protocol which provides a secure and reliable connection to Security Center.

- **Listening port:** Port used to listen for connection requests coming from fixed Sharp cameras. When the connection is established, the ALPR Manager can receive live updates from the ALPR units it manages.

File association

The *File association* settings specify which hotlists and permits are active and managed by the ALPR Manager.

- **Hotlists:** A list of all the *hotlists* in Security Center. Select which hotlists you want the ALPR Manager to manage.
- **Permits:** A list of all the *permits* in Security Center. Select which permits the ALPR Manager manages.

Matching

The *Matching* settings are used to enable matching between hotlists and fixed Sharp units. When matching is enabled, you can configure event-to-actions in Security Desk that trigger on *Match* and *No match* events.

- **Matching:** When matching is enabled, you can configure event-to-actions in Security Desk that trigger when the Sharp reads a plate that is on a hotlist you've activated in File association.
- **Generate No match events:** Security Center generates *No match* events when a plate is not found on a specific hotlist. You can then configure event-to-actions in Security Desk based on *No match* events.
- **Past-read matching:** When past-read matching is enabled, the system compares new or updated hotlists against previously-captured license plate reads.

NOTE:

  - The database retention period is configurable. All hits past the configured retention period are deleted from the database.
  - If a hotlist hit has already been generated for a plate, performing past-read matching does not generate a duplicate hit for the plate.
  - Federated hotlists cannot be used for past-read matching.
  - If a hit is generated based on a past-read match, it is indicated in the **Post matched** column in the Security Desk *Hits* report.
  - **Hotlists:** Select one or more hotlists to be used for past-read matching.
    NOTE: For a hotlist to be used with past-read matching, the hotlist must first be associated with the role or SharpV camera for which past-read matching has been activated.
  - **Search back time:** Set the limit for how far in the past the system searches for plate reads when past-read matching is triggered.

Geocoding

The *Geocoding* feature allows the ALPR Manager to perform *geocoding* and *reverse geocoding*.

NOTE: If your patrol vehicles are equipped with GPS but no maps, you need reverse geocoding to convert the raw GPS data (longitude, latitude) from patrol vehicles into street addresses. The street addresses are then saved along with the reads in the ALPR Manager database.

- **Map type:** Displays the map type set in the Security Center license.
- **Maps and data folder:** Folder where the Benomad files are found. This folder must be on the same computer where the ALPR Manager is installed.

Plate filtering

The *Plate filtering* settings determine what to do when a hotlist or permit list is modified and the ALPR Manager detects that there are entries with invalid characters (non-alphanumeric characters).

- **Plate number valid characters:** The types of characters to filter on (Latin, Arabic, Japanese, Cyrillic, or Thai).
- **Invalid plate number:** How the ALPR Manager handles invalid records.
  - **Modify record:** (Default setting). Removes any non-alphanumeric characters from the plate number. For example, the plate number “ABC#%3” becomes “ABC3”.
  - **Remove record:** Deletes the entire entry from the list.
- **Log filtering:** Select to log the filtering process. The plate filtering logs will be saved in the AutoVu root folder: *C:\Genetec\AutoVu\RootFolder*.

Email notification

The *Email notification* setting turns on email notifications for hotlist hits, and lets you customize the look and contents of the email message.

- **Email attribute name:** Used for email notification at the individual license plate level. Type the name of the hotlist attribute related to email notification. For example, if you added an “Email” attribute on the hotlist entity’s Properties tab, then type the exact same name here. The names must match exactly.
- **Email attachments:** The ALPR data that is attached to the notification email, and whether to hide the license plate numbers in the message body.

  - **License plate image:** High resolution close-up images of the license plate.
  - **Context image:** A wider angle color image of the vehicle.
  - **Wheel image:** Replaces the read plate number, and the matched plate number in the email with asterisks (*).
- **Log emails:** Select this option to log hotlist hit notification emails. The email logs will be saved in the AutoVu root folder: *C:\Genetec\AutoVu\RootFolder*.
- **Template:** Customize the email. Do any of the following:
  - Edit the email’s subject line or message body.
  - Switch between plain text and HTML.
  - Add formatting (bold, italics, and so on).
  - Right-click in the message body for a menu of quick tags that you can use to add more information to the email.
  - Restore the default email template at any time.

XML import

The *XML import* settings are used to import data from third-party applications into the ALPR Manager database. When you turn this setting on, Security Center creates an *XML import* entity, and then associates the imported data with this entity. In Security Desk, you can then filter on the *XML import* entity when running hit or read reports

NOTE: This option requires a license. Please contact your representative of Genetec Inc. for more information.

- **XML read template file:** Specify where the XML read template file is located. You'll find a default template in the Security Center installation package in *Program Files (x86)\Genetec Security Center X.X\Add-On\LPR\XMLTemplatesSamples\XMLImport*.

  NOTE: In most cases the default template can be used.
- **XML data folder:** Specify the folder that contains the XML data files for Security Center to import.

  NOTE: Files are deleted from this folder once they've been processed.
- **Supported XML import hashtags:** The following XML import hashtags are supported. Each hashtag must have an opening and closing XML tag (for example, to use the tag *#CONTEXT_IMAGE#* you must write *<ContextImage>#CONTEXT_IMAGE#</ContextImage>* in the XML).
  - **#PLATE_READ#:** License plate as read by the Sharp.
  - **#PLATE_STATE#:** License plate's issuing state or province, if read.
  - **#DATE_LOCAL#:** Local date of the ALPR event.
  - **#DATE_UTC#:** UTC date of the ALPR event.
  - **#TIME_UTC#:** UTC time of the ALPR event.
  - **#TIME_ZONE#:** Local time zone for the ALPR event.
  - **#CONTEXT_IMAGE#:** Context image (Base64-encoded JPEG).
  - **#PLATE_IMAGE#:** License plate image (Base64-encoded JPEG).
  - **#LONGITUDE#:** Longitude of the ALPR event (in decimal degrees or DMS).
  - **#LATITUDE#:** Latitude of the ALPR event (in decimal degrees or DMS).
  - **#GUID#:** Unique identifier of the ALPR event.
  - **#CUSTOM_FIELDS#:** You can import other fields with this hashtag by using the key=value format. Format the key as #CUSTOM_FIELDS#{KEY}.
    NOTE: You must specify a format for DATE and TIME hashtags. For example, #DATE_LOCAL#{yyyy/MM/dd}). Click here for more information about which formats to use. If these hashtags are not

included, UTC dates and times are used as a baseline for calculating the local time. If an error occurs, the time the ALPR Manager role imported the data is used

XML export

The *XML export* settings are used to send ALPR Manager reads and hits to third-party applications. Reads and hits are sent live as they occur.

- **XML templates folder:** Specify where the XML templates folder is located. You'll find default templates in *Program Files (x86)\Genetec Security Center X.X\Add-On\LPR\XMLTemplatesSamples\XMLExport*. There are XML templates for each type of ALPR event (plate reads, hotlist hits, overtime hits, permit hits, and shared permit hits).

  NOTE: In most cases the default template can be used.
- **XML export folder:** Specify the folder that contains the XML files exported by the ALPR Manager.
- **Time format:** Enter the time format used in the exported files. As you set the time format the information field displays what the time format will look like in the XML file.

  To identify the units of time, use the following notation:

Notation	Description
h	Hour
m	Minute
s	Second
:	Must use a colon (:) between the hour, minute, and second units.
hh,mm,ss	Display time with leading zero. For example: 03:06:03 represents 3 hours 6 minutes 3 seconds.
h,m,s	Display without leading zero. For example: 3:6:3 represents 3 hours 6 minutes 3 seconds.
tt	Include am or pm If using a 12-hour clock, you might want to use am or pm notation. Unit can be preceded with or without a space. For example, HH:mm:ss tt displays 17:38:42 pm.
Lowercase h	12-hour clock.
Uppercase H	24-hour clock.

- **Date format:** Select a date format to use in the exported files. You can choose either **MM/dd/yyyy** or **yyyy-MM-dd**. For example, yyyy-MM-dd displays 2016-06-21.
- **Supported XML hashtags:** The following XML export hashtags are supported. Each hashtag must have an opening and closing XML tag (for example, to use the tag *#CONTEXT_IMAGE#* you must write *<ContextImage>#CONTEXT_IMAGE#</ContextImage>* in the XML).

- **#ACCEPT_REASON#:** Reason hit was accepted.
- **#ADDRESS#:** Address of the ALPR event.
- **#ATTRIBUTES#:** Generate all Read and Hit attributes.
- **#CAMERA_NAME#:** Name of the camera.
- **#CONTEXT_IMAGE#:** Context image (Base64-encoded JPEG).
- **#DATE_LOCAL#:** Local date of the ALPR event.
- **#DATE_UTC#:** UTC date of the ALPR event.
- **#ELAPSED_TIME#:** For an overtime hit, this tag indicates the time difference between the two plate reads (displaying the number of days is optional).
- **#FIRST_VEHICLE#:** For a shared permit hit, this tag generates the content specified in *ReadTemplate.xml* for the first vehicle seen.
- **#FIRST_VEHICLE_FROM_STREET#:** For an overtime hit, this tag retrieves the attribute *From street* from the first plate read.
- **#FIRST_VEHICLE_TO_STREET#:** For an overtime hit, this tag retrieves the attribute *To street* from the first plate read.
- **#HOTLIST_CATEGORY#:** Category field of the hotlist that generated the hit.
- **#GUID#:** Unique identifier of the ALPR event.
- **#INVENTORY_LOCATION#:** For MLPI installations, the location of the vehicle inventory.
- **#IS_POST_MATCHED#:** (Hotlist only) If the Hit was post matched (matched with the Post-matching event).
- **#ISHIT#:** This tag indicates if the ALPR event is a hit.
- **#LATITUDE#:** Latitude of the ALPR event (in decimal degrees).
- **#LATITUDE#{dms}:** Latitude of the ALPR event (in degrees, minutes, and seconds).
- **#LATITUDE#{dec}:** Latitude of the ALPR event (in decimal degrees).
- **#LATITUDE_DEGREE#:** Latitude of the ALPR event (degrees).
- **#LATITUDE_DMS#:** Latitude of the ALPR event (in degrees, minutes, and seconds).
- **#LATITUDE_MINUTE#:** Latitude of the ALPR event (minutes).
- **#LATITUDE_SECOND#:** Latitude of the ALPR event (seconds).
- **#LONGITUDE#:** Longitude of the ALPR event (in decimal degrees).
- **#LONGITUDE#{dec}:** Longitude of the ALPR event (in decimal degrees).
- **#LONGITUDE#{dms}:** Latitude of the ALPR event (in degrees, minutes, and seconds).
- **#LONGITUDE_DEGREE#:** Longitude of the ALPR event (degrees).
- **#LONGITUDE_DMS#:** Longitude of the ALPR event (in degrees, minutes, and seconds).
- **#LONGITUDE_MINUTE#:** Longitude of the ALPR event (minutes).
- **#LONGITUDE_SECOND#:** Longitude of the ALPR event (seconds).
- **#MATCHED_PLATE#:** License plate against which the hit was generated.
- **#ORIGINAL#:** For an overtime hit, this tag generates the content specified in *ReadTemplate.xml* for the first read of a given plate.
- **#OVERVIEW_IMAGE#:** Overview image (Base64-encoded JPEG).
- **#PARKING_LOT#:** (Read & any Hit Type) Get the extracted parking lot based on the Rule ID and the Lot ID.
- **#PATROLLER_ID#:** ID of patrol vehicle.
- **#PATROLLER_NAME#:** Name of patrol vehicle.
- **#PERMIT_ID#:** (Permit only) Get the associated LPR Rule ID.
- **#PERMIT_NAME#:** Name of the permit that generated the ALPR event.
- **#PLATE_IMAGE#:** License plate image (Base64-encoded JPEG).

- **#PLATE_READ#:** License plate as read by the Sharp.
- **#PLATE_READ_MATCHED#:** (Hotlist only) (Same as #MATCHED_PLATE#) Get the Hit matched plate, based on the value of *MatchPlate* analytic.
- **#PLATE_STATE#:** License plate's issuing state or province, if read.
- **#REJECT_REASON#:** Reason hit was rejected.
- **#READ#:** Embed the contents of the *ReadTemplate.xml* inside another XML template (useful for hits).
- **#RULE_COLOR#:** Color of the rule associated to the ALPR event.
- **#RULE_ID#:** ID of the rule associated to the ALPR event.
- **#RULE_NAME#:** Name of the rule associated to the ALPR event (hotlist, overtime, permit, or permit restriction).
- **#SECOND_VEHICLE#:** For a shared permit hit, this tag generates the content specified in *ReadTemplate.xml* for the second vehicle seen.
- **#SECOND_VEHICLE_FROM_STREET#:** For an overtime hit, this tag retrieves the attribute *From street* from the second plate read.
- **#SECOND_VEHICLE_TO_STREET#:** For an overtime hit, this tag retrieves the attribute *To street* from the second plate read.
- **#SHARP_NAME#:** Name of the Sharp that read the plate.
- **#STATE#:** License plate's issuing state or province, if read.
- **#TIME_LOCAL#:** Local time.
- **#TIME_UTC#:** UTC time of the ALPR event.
- **#USER_ACTION#:** User action related to the ALPR event.
- **#USER_ID#:** ID of the user.
- **#USER_NAME#:** Name of the user.
- **#VEHICLE#:** Same as #READ#.
- **#ZONE_COLOR#:** (Overtime only) Get the color of the associated Overtime Rule.
- **#ZONE_ID#:** (Permit & Shared Permits & Overtime) Get the associated LPR Rule ID.
- **#ZONE_NAME# :** Get the Associated Rule Name.

AutoVu™ Free-Flow

Turn on *Free-Flow* to configure the XML export of parking events for third-party parking permit providers using the Pay-by-Plate Sync plugin.

- **Matching:**
  - **Match tolerance threshold:** This value indicates the number of single-character differences between entry and exit plate reads that will still be considered a match. Setting the value to 0 is equivalent to an exact match.

    IMPORTANT: Setting this value too high may cause plate reads to be associated with the wrong vehicle. The default value is 1.
- **Pay-by-Plate:**
  - **Server:** Enter the IP address of the machine where Pay-by-Plate Sync is installed.
  - **Port:** Enter the port number for the Pay-by-Plate Sync connection (default: 8787).
- **XML export:**
  - **XML export folder:** Specify the export folder for Free-Flow XML data.
  - **Include vehicle images with export:** By default, vehicle images are not included with the exported XML file. To include vehicle images, select **Include vehicle images with report**.
    NOTE: Including vehicle images increases the size of the XML export file.
  - **Export occupancy:**

  Export parking zone occupancy data to a separate XML file.
  - **Export violations:** When a vehicle is in violation, vehicle information is exported as a separate XML file.
  - **Export completed sessions:** When a vehicle exits the parking lot, the parking session information is exported as a separate XML file.
- **Events:**
  - **Capacity threshold:** Specify the parking zone capacity threshold where a *capacity threshold reached* event is generated.

AutoVu third party data exporter

Turn on *AutoVu third party data exporter* to configure the secure export of read and hit events to the required third-party systems.

- **Parameters:**
  - **Endpoint name:** Enter a relevant name for the required third party server.
  - **Destination folder:** Enter the path of the destination folder on the third-party server.
  - **Export format:** Select the format in which the data needs to be exported.
    - XML: Select this option if you want to export reads and hits in XML format.
    - JSON: Select this option if you want to export reads and hits in JSON format.
    - UTMC: Select this option if you want to export reads.
    - JSON2: Select this option if you want to export hits.
  - **File name template:** Enter a relevant name for the export type.
  - **Server URL:** Enter the IP address of the third party server.
- **File format-specific:** Enter the value for the *Customer ID* provided by the customer.

  NOTE: This section is displayed only if *Export format* selected in step 4 is **JSON2**.
- *What to export*: Select the events you want to export.
- **Export settings:** Choose the export settings as required.
  - **Export images:** Select this option to export the images along with the read or hit.
  - **Enforced hits only:** Select this option to export enforced hits.
- **Critical:** Select the events you want to resend after an export operation fails.
  - **Reads:** Select this option to resend any reads.
  - **Hits:** Select this option to resend any hits.

  NOTE: The AutoVu Data Exporter plugin will retry until the event is successfully exported or more than 1000 events need to be resent.
- **Authorization:**
  - **Authorization mode:** Choose the authorization mode as required.
    - **None:** Select this option if the third-party system does not require any specific authorization method.
    - **SslCertificate:** Select this mode if the third-party system uses TLS certificate.
    - **PasswordGrant:** Select this mode if the third party system uses PasswordGrant token.
  - **Client certificate:** Enter or browse the path to the TLS certificate provided by third-party API.

    NOTE: This parameter is displayed only if *Certificate* authorization mode is selected.
  - **Token URL:** Enter the value provided by third party API.
  - **Client ID:** Enter the value provided by third party API.
  - **Client secret:** Enter the value provided by third party API.
  - **Username:** Enter the value provided by third party API.
  - **Password:** Enter the value provided by third party API.
  - **Scope:** Enter the value provided by third party API.

NOTE: If no value is provided, the field can be left empty.

- **Connection settings:**
  - **Hostname or IP:** Enter the hostname or IP address of the destination.
  - **Port:** Enter the port number of the destination address.
  - **Username:** Enter the value provided by third-party API.
  - **Password:** Enter the value provided by third-party API.
  - **SSH Key:** Enter the value provided by third-party API.
    NOTE: If no value is provided, the field can be left empty.
  - **SSH passphrase:** Enter the value provided by third-party API.

    NOTE: If no value is provided, the field can be left empty.

Examples of JSON files for the AutoVu third-party data exporter

When you send ALPR data to an external server, you can configure the AutoVu™ third-party data exporter feature to send the data in JSON format.

JSON format sample:

The following is an example of a license plate hotlist hit event.

NOTE: The binary image data has been removed from the example.

```
{
    "InventoryLocation": "",
    "IsPostMatched": "No",
    "MatchedPlate": "ABC123",
    "RuleId": "c43806f7f60e",
    "RuleName": "Sample-Hotlist",
    "Vehicle": {
        "Read": {
            "Address": "1234 1st Avenue, City Name, X1Y",
            "Attributes": {
                "State Name": "QC",
                "Vehicle Type": "-",
                "Relative Motion": "Approaching",
                "Context": "Quebec",
                "Characters Height": "26",
                "Confidence Score": "97",
                "Vehicle Make": "Skoda",
                "Speed": "70 km/h"
            },
            "CameraName": "LprCamera",
            "ContextImage": "",
            "DateLocal": "10/01/2022",
            "DateUtc": "10/01/2022",
            "InventoryLocation": "",
            "IsHit": "Yes",
            "Latitude": "0",
            "LatitudeDegree": "0",
            "LatitudeDMS": "N0",
            "LatitudeMinute": "0",
            "LatitudeSecond": "0",
            "Longitude": "0",
            "LongitudeDegree": "0",
            "LongitudeDMS": "W0",
            "LongitudeMinute": "45",
            "LongitudeSecond": "47",
            "OverviewImage": "",
            "ParkingLot": "",
            "PatrollerId": "631580e1307f",
            "PatrollerName": "Default",
            "PermitName": "AV50",
            "Plate": "ABC123",
            "PlateImage": "",
            "SharpName": "AV1",
            "State": "State Name",
            "TimeLocal": "07:49:22",
            "TimeUtc": "11:49:22",
            "UserId": "0d5f7d4fefaf",
            "UserName": "PatrollerDefault",
            "VehicleID": "53c39685b980"
        }
    },
    "Attributes": {
        "Category": "Scofflaw",
        "PlateState": "QC",
        "MatchPlate": "******",
        "hide_SP": 9922,
        "hide_OverridePrivacy": false
    }
    "DateLocal": "10/01/2022",
    "DateUtc": "10/01/2022",
    "HitID": "ccde9ad151bc",
    "HotlistCategory": "Scofflaw",
    "ParkingLot": "",
    "PatrollerId": "631580e1307f",
    "PatrollerName": "Default",
    "RejectReason": null,
    "TimeLocal": "07:49:37",
    "TimeUtc": "11:49:37",
    "UserAction": "Enforced",
    "UserId": "0d5f7d4fefaf",
    "UserName": "PatrollerDefault"
}
```

The following is an example of a license plate overtime hit event.

NOTE: The binary image data has been removed from the example.

```
{
    "ElapsedTime": "00:04:29",
    "FirstRead": {
        "FromStreetName": "1st Avenue",
        "Read": {
            "Address": "1234 1st Avenue, City Name, X1Y",
            "Attributes": {
                "State Name": "QC",
                "Vehicle Type": "-",
                "Relative Motion": "Approaching",
                "Context": "Quebec",
                "Characters Height": "26",
                "Confidence Score": "97",
                "Vehicle Make": "Skoda",
                "Speed": "70 km/h"
            }
            "CameraName": "LprCamera",
            "ContextImage": "",
            "DateLocal": "10/01/2022",
            "DateUtc": "10/01/2022",
            "InventoryLocation": "",
            "IsHit": "Yes",
            "Latitude": "0",
            "LatitudeDegree": "0",
            "LatitudeDMS": "N0",
            "LatitudeMinute": "0",
            "LatitudeSecond": "0",
            "Longitude": "0",
            "LongitudeDegree": "0",
            "LongitudeDMS": "W0",
            "LongitudeMinute": "45",
            "LongitudeSecond": "47",
            "OverviewImage": "",
            "ParkingLot": "",
            "PatrollerId": "6446e421b257",
            "PatrollerName": "DefaultCity",
            "PermitName": "AV50",
            "Plate": "ABC123",
            "PlateImage": "",
            "SharpName": "AV1",
            "State": "State Name",
            "TimeLocal": "19:34:52",
            "TimeUtc": "23:34:52",
            "UserId": "5845088e1036",
            "UserName": "PatrollerCityDefault",
            "VehicleID": "fd064be7f67b"
        },
        "ToStreetName": "Main street"
    },
    "LastRead": {
        "FromStreetName": "1st Avenue",
        "Read": {
            "Address": "1234 1st Avenue, City Name, X1Y",
            "Attributes": {
                "State Name": "QC",
                "Vehicle Type": "-",
                "Relative Motion": "Approaching",
                "Context": "Quebec",
                "Characters Height": "26",
                "Confidence Score": "97",
                "Vehicle Make": "Skoda",
                "Speed": "70 km/h"
            }
            "CameraName": "LprCamera",
            "ContextImage": "",
            "DateLocal": "10/01/2022",
            "DateUtc": "10/01/2022",
            "InventoryLocation": "",
            "IsHit": "Yes",
            "Latitude": "0",
            "LatitudeDegree": "0",
            "LatitudeDMS": "N0",
            "LatitudeMinute": "0",
            "LatitudeSecond": "0",
            "Longitude": "0",
            "LongitudeDegree": "0",
            "LongitudeDMS": "W0",
            "LongitudeMinute": "45",
            "LongitudeSecond": "47",
            "OverviewImage": "",
            "ParkingLot": "",
            "PatrollerId": "6446e421b257",
            "PatrollerName": "DefaultCity",
            "PermitName": "AV50",
            "Plate": "ABC123",
            "PlateImage": "",
            "SharpName": "AV1",
            "State": "State Name",
            "TimeLocal": "19:39:21",
            "TimeUtc": "23:39:21",
            "UserId": "5845088e1036",
            "UserName": "PatrollerCityDefault",
            "VehicleID": "5c63043f0806"
        },
        "ToStreetName": "Main street"
    },
    "RuleColor": "#FFBDD1A3",
    "RuleId": "0019e81ad77c",
    "RuleName": "AVDefault",
    "Attributes": {
        "VehicleOvertimeGUID": "fd064be7f67b",
        "MatchPlate": "******",
        "Read1FromStreetName": "RUE WELLINGTON",
        "Read1ToStreetName": "BOULEVARD LASALLE",
        "Read2FromStreetName": "1st Avenue",
        "Read2ToStreetName": "Main street"
    }
    "DateLocal": "10/01/2022",
    "DateUtc": "10/01/2022",
    "HitID": "7d8af905eec9",
    "HotlistCategory": "",
    "ParkingLot": "",
    "PatrollerId": "6446e421b257",
    "PatrollerName": "DefaultCity",
    "RejectReason": null,
    "TimeLocal": "19:39:21",
    "TimeUtc": "23:39:21",
    "UserAction": "Enforced",
    "UserId": "5845088e1036",
    "UserName": "PatrollerDefault"
}
```

The following is an example of a license plate permit hit event.

NOTE: The binary image data has been removed from the example.

```
{
    "Hit": {
        "Read": {
            "Address": "1234 1st Avenue, City Name, X1Y",
            "Attributes": {
                "State Name": "QC",
                "Vehicle Type": "-",
                "Relative Motion": "Approaching",
                "Context": "Quebec",
                "Characters Height": "26",
                "Confidence Score": "97",
                "Vehicle Make": "Skoda",
                "Speed": "70 km/h"
            }
            "CameraName": "LprCamera",
            "ContextImage": "",
            "DateLocal": "10/01/2022",
            "DateUtc": "10/01/2022",
            "InventoryLocation": "",
            "IsHit": "Yes",
            "Latitude": "0",
            "LatitudeDegree": "0",
            "LatitudeDMS": "N0",
            "LatitudeMinute": "0",
            "LatitudeSecond": "0",
            "Longitude": "0",
            "LongitudeDegree": "0",
            "LongitudeDMS": "W0",
            "LongitudeMinute": "45",
            "LongitudeSecond": "47",
            "OverviewImage": "",
            "ParkingLot": "",
            "PatrollerId": "6446e421b257",
            "PatrollerName": "DefaultCity",
            "PermitName": "AV50",
            "Plate": "ABC123",
            "PlateImage": "",
            "SharpName": "AV1",
            "State": "State Name",
            "TimeLocal": "05:52:21",
            "TimeUtc": "09:52:21",
            "UserId": "5845088e1036",
            "UserName": "PatrollerDefault",
            "VehicleID": "c4d439602832"
        }
    },
    "RuleId": "33986ca13124",
    "RuleName": "AVDefault",
    "Attributes": {
        "MultipleHit": ""
    }
    "DateLocal": "10/01/2022",
    "DateUtc": "10/01/2022",
    "HitID": "934956228419",
    "HotlistCategory": "",
    "ParkingLot": "",
    "PatrollerId": "6446e421b257",
    "PatrollerName": "DefaultCity",
    "RejectReason": null,
    "TimeLocal": "05:52:25",
    "TimeUtc": "09:52:25",
    "UserAction": "Enforced",
    "UserId": "5845088e1036",
    "UserName": "PatrollerDefault"
}
```

The following is an example of a license plate shared permit hit event.

NOTE: The binary image data has been removed from the example.

```
{
    "FirstVehicle": {
        "Read": {
            "Address": "1234 1st Avenue, City Name, X1Y",
            "Attributes": {
                "State Name": "QC",
                "Vehicle Type": "-",
                "Relative Motion": "Approaching",
                "Context": "Quebec",
                "Characters Height": "26",
                "Confidence Score": "97",
                "Vehicle Make": "Skoda",
                "Speed": "70 km/h"
            }
            "CameraName": "LprCamera",
            "ContextImage": "",
            "DateLocal": "10/01/2022",
            "DateUtc": "10/01/2022",
            "InventoryLocation": "",
            "IsHit": "Yes",
            "Latitude": "0",
            "LatitudeDegree": "0",
            "LatitudeDMS": "N0 0 0",
            "LatitudeMinute": "0",
            "LatitudeSecond": "0",
            "Longitude": "0",
            "LongitudeDegree": "0",
            "LongitudeDMS": "E0 0 0",
            "LongitudeMinute": "0",
            "LongitudeSecond": "0",
            "OverviewImage": "",
            "ParkingLot": "",
            "PatrollerId": "6942bb945e0b",
            "PatrollerName": "PatrollerDefault",
            "PermitName": "Hotlist1",
            "Plate": "******",
            "PlateImage": "",
            "SharpName": "AV1",
            "State": "",
            "TimeLocal": "18:50:40",
            "TimeUtc": "22:50:40",
            "UserId": "e1e3ab0bd753",
            "UserName": "",
            "VehicleID": "5e213c54fe73"
        }
    },
    "RuleId": "7a22869b87ba",
    "RuleName": "Shared permit",
    "SecondVehicle": {
        "Read": {
            "Address": "1234 1st Avenue, City Name, X1Y",
            "Attributes": {
                "State Name": "QC",
                "Vehicle Type": "-",
                "Relative Motion": "Approaching",
                "Context": "Quebec",
                "Characters Height": "26",
                "Confidence Score": "97",
                "Vehicle Make": "Skoda",
                "Speed": "70 km/h"
            }
            "CameraName": "LprCamera",
            "ContextImage": "",
            "DateLocal": "10/01/2022",
            "DateUtc": "10/01/2022",
            "InventoryLocation": "",
            "IsHit": "Yes",
            "Latitude": "0",
            "LatitudeDegree": "0",
            "LatitudeDMS": "N0",
            "LatitudeMinute": "0",
            "LatitudeSecond": "0",
            "Longitude": "0",
            "LongitudeDegree": "0",
            "LongitudeDMS": "W0",
            "LongitudeMinute": "45",
            "LongitudeSecond": "47",
            "OverviewImage": "",
            "ParkingLot": "",
            "PatrollerId": "6942bb945e0b",
            "PatrollerName": "DefaultPatroller",
            "PermitName": "Hotty",
            "Plate": "******",
            "PlateImage": "",
            "SharpName": "AV1",
            "State": "",
            "TimeLocal": "18:56:57",
            "TimeUtc": "22:56:57",
            "UserId": "e1e3ab0bd753",
            "UserName": "",
            "VehicleID": "511c5db6e636"
        }
    },
    "Attributes": {
        "Category": "Hotty",
        "PlateState": "",
        "MatchPlate": "******",
        "EffectiveDate": "Wednesday, January 1, 2022",
        "DurationViolated": 120,
        "hide_ClosestMatchPlateState": "QC",
        "VehicleRead": "ac0ad66d-84f6-451f-a8df-5e213c54fe73",
        "ExpiryDate": "Friday, January 1, 2024",
        "hide_ClosestMatchPlateNumber": "******",
        "VehicleColor": "Red",
        "VehicleMake": "Toyota",
        "PermitID": "A000",
        "VehicleOvertimeGUID": "ac0ad66d-84f6-451f-a8df-5e213c54fe73"
    }
    "DateLocal": "10/01/2022",
    "DateUtc": "10/01/2022",
    "HitID": "82323d82d8dd",
    "HotlistCategory": "Hotlist1",
    "ParkingLot": "",
    "PatrollerId": "6942bb945e0b",
    "PatrollerName": "DefaultPatroller",
    "RejectReason": null,
    "TimeLocal": "18:57:14",
    "TimeUtc": "22:57:14",
    "UserAction": "Enforced",
    "UserId": "e1e3ab0bd753",
    "UserName": "DefaultPatroller"
}
```

The following is an example of a license plate read event.

NOTE: The binary image data has been removed from the example.

```
{
    "Read": {
        "Address": "1234 1st Avenue, City Name, X1Y",
        "Attributes": {
            "State Name": "QC",
            "Vehicle Type": "-",
            "Relative Motion": "Approaching",
            "Context": "Quebec",
            "Characters Height": "26",
            "Confidence Score": "97",
            "Vehicle Make": "Skoda",
            "Speed": "70 km/h"
        },
        "CameraName": "LprCamera",
        "ContextImage": "",
        "DateLocal": "10/01/2022",
        "DateUtc": "10/01/2022",
        "InventoryLocation": "",
        "IsHit": "Yes",
        "Latitude": "0",
        "LatitudeDegree": "0",
        "LatitudeDMS": "N0",
        "LatitudeMinute": "0",
        "LatitudeSecond": "0",
        "Longitude": "0",
        "LongitudeDegree": "0",
        "LongitudeDMS": "W0",
        "LongitudeMinute": "45",
        "LongitudeSecond": "47",
        "OverviewImage": "",
        "ParkingLot": "",
        "PatrollerId": "6446e421b257",
        "PatrollerName": "DefaultPatroller",
        "PermitName": "AV50",
        "Plate": "******",
        "PlateImage": "",
        "SharpName": "AV1",
        "State": "State Name",
        "TimeLocal": "05:52:21",
        "TimeUtc": "09:52:21",
        "UserId": "5845088e1036",
        "UserName": "PatrollerDefault",
        "VehicleID": "c4d439602832"
    }
}
}
```

Examples of XML files for the AutoVu third-party data exporter

When you send ALPR data to an external server, you can configure the AutoVu™ third-party data exporter feature to send the data in XML format.

XML format sample:

The following is an example of a license plate hotlist hit event.

NOTE: The binary image data has been removed from the example.

```
<Hotlist>
 <attributes>
  <Attributes>
   <Attribute name="Category">Stolen</Attribute>
   <Attribute name="PlateState"/>
   <Attribute name="MatchPlate">******</Attribute>
   <Attribute name="hide_OverridePrivacy">False</Attribute>
   <Attribute name="hide_SP">5150</Attribute>
   <Attribute name="ExpiryDate"/>
   <Attribute name="MultipleHit"/>
   <Attribute name="EffectiveDate"/>
   <Attribute name="VehicleMake"/>
   <Attribute name="VehicleColor"/>
  </Attributes>
 </attributes>
 <Date>10/01/2022</Date>
 <DateLocal>10/01/2022</DateLocal>
 <DateUtc>10/01/2022</DateUtc>
 <HitID>8fc6b1873817</HitID>
 <HotlistCategory>Stolen</HotlistCategory>
 <ParkingLot />
 <PatrollerId>6942bb945e0b</PatrollerId>
 <PatrollerName>Patroller</PatrollerName>
 <Time>18:13:11</Time>
 <TimeLocal>18:13:11</TimeLocal>
 <TimeUtc>22:13:11</TimeUtc>
 <UserAction>Enforced</UserAction>
 <UserId>e1e3ab0bd753</UserId>
 <UserName />
 <InventoryLocation />
 <IsPostMatched>No</IsPostMatched>
 <MatchedPlate>******</MatchedPlate>
 <PlateReadMatched>******</PlateReadMatched>
 <RuleId>80678c50873d</RuleId>
 <RuleName>Hotlist1</RuleName>
 <Vehicle>
  <Read>
   <Address>415 (1st Avenue - Main Street), City Name, X1Y</Address>
   <attributes>
    <Attributes>
     <Attribute name="Relative Motion" customFieldGuid="000000000000">-</Attribute>
     <Attribute name="Vehicle Type" customFieldGuid="000000000000">-</Attribute>
     <Attribute name="Confidence Score" customFieldGuid="000000000000">100</
Attribute>
     <Attribute name="Vehicle Make" customFieldGuid="000000000000">BMW</Attribute>
     <Attribute name="Speed" customFieldGuid="000000000000">10 mph</Attribute>
     <Attribute name="Context" customFieldGuid="000000000000">State Name</
Attribute>
     <Attribute name="Characters Height" customFieldGuid="000000000000">36</
Attribute>
     <Attribute name="PatrollerSpeed" customFieldGuid="000000000000">29 mph</
Attribute>
    </Attributes>
   </attributes>
   <CameraName>LprCamera</CameraName>
   <ContextImage />
   <Date>10/01/2022</Date>
   <DateLocal>10/01/2022</DateLocal>
   <DateUtc>10/01/2022</DateUtc>
   <InventoryLocation />
   <IsHit>Yes</IsHit>
   <Latitude>0</Latitude>
   <LatitudeDegree>0</LatitudeDegree>
   <LatitudeDMS>N0</LatitudeDMS>
   <LatitudeMinute>0</LatitudeMinute>
   <LatitudeSecond>0</LatitudeSecond>
   <Longitude>0</Longitude>
   <LongitudeDegree>0</LongitudeDegree>
   <LongitudeDMS>W0</LongitudeDMS>
   <LongitudeMinute>0</LongitudeMinute>
   <LongitudeSecond></LongitudeSecond>
   <OverviewImage />
   <ParkingLot />
   <PatrollerId>6942bb945e0b</PatrollerId>
   <PatrollerName>PatrollerDefault</PatrollerName>
   <PermitName />
   <Plate>******</Plate>
   <PlateImage />
   <SharpName>PatrollerDefault</SharpName>
   <State />
   <Time>18:13:06</Time>
   <TimeLocal>18:13:06</TimeLocal>
   <TimeUtc>22:13:06</TimeUtc>
   <UserId>e1e3ab0bd753</UserId>
   <UserName />
   <VehicleID>ab0cbea3143e</VehicleID>
  </Read>
 </Vehicle>
</Hotlist>
```

The following is an example of a license plate overtime hit event.

NOTE: The binary image data has been removed from the example.

```
<OvertimeHit>
 <attributes>
  <Attributes>
   <Attribute name="MatchPlate">******</Attribute>
   <Attribute name="MultipleHit"/>
   <Attribute name="TireImage2">21B97CAE52BA</Attribute>
   <Attribute name="TireImage1">6C5CB52984F0</Attribute>
   <Attribute name="VehicleMake"/>
   <Attribute name="VehicleColor"/>
   <Attribute name="VehicleOvertimeGUID">6726acb574ae</Attribute>
   <Attribute name="Read1FromStreetName">1st Avenue</Attribute>
   <Attribute name="Read1ToStreetName">1st Avenue</Attribute>
   <Attribute name="Read2FromStreetName">1st Avenue</Attribute>
   <Attribute name="Read2ToStreetName">1st Avenue</Attribute>
  </Attributes>
 </attributes>
 <Date>10/01/2022</Date>
 <DateLocal>10/01/2022</DateLocal>
 <DateUtc>10/01/2022</DateUtc>
 <HitID>55be4703261a</HitID>
 <HotlistCategory />
 <ParkingLot />
 <PatrollerId>6942bb945e0b</PatrollerId>
 <PatrollerName>PatrollerDefault</PatrollerName>
 <Time>18:20:00</Time>
 <TimeLocal>18:20:00</TimeLocal>
 <TimeUtc>22:20:00</TimeUtc>
 <UserAction>Enforced</UserAction>
 <UserId>e1e3ab0bd753</UserId>
 <UserName />
 <ElapsedTime>00:01:05</ElapsedTime>
 <FirstRead>
  <FromStreetName>1st Avenue</FromStreetName>
  <Read>
   <Address>485 (1st Avenue - 1st Avenue), City Name, X1Y</Address>
   <attributes>
    <Attributes>
     <Attribute name="Relative Motion" customFieldGuid="000000000000">Closer</
Attribute>
     <Attribute name="Vehicle Type" customFieldGuid="000000000000">Private</
Attribute>
     <Attribute name="Confidence Score" customFieldGuid="000000000000">70</
Attribute>
     <Attribute name="Vehicle Make" customFieldGuid="000000000000">Cadillac</
Attribute>
     <Attribute name="Speed" customFieldGuid="000000000000">70 km/h</Attribute>
     <Attribute name="Context" customFieldGuid="000000000000">State Name</
Attribute>
     <Attribute name="Characters Height" customFieldGuid="000000000000">28</
Attribute>
     <Attribute name="PatrollerSpeed" customFieldGuid="000000000000">29 mph</
Attribute>
    </Attributes>
   </attributes>
   <CameraName>LprCamera</CameraName>
   <ContextImage />
   <Date>10/01/2022</Date>
   <DateLocal>10/01/2022</DateLocal>
   <DateUtc>10/01/2022</DateUtc>
   <InventoryLocation />
   <IsHit>Yes</IsHit>
   <Latitude>0</Latitude>
   <LatitudeDegree>0</LatitudeDegree>
   <LatitudeDMS>N0</LatitudeDMS>
   <LatitudeMinute>0</LatitudeMinute>
   <LatitudeSecond>0</LatitudeSecond>
   <Longitude>0</Longitude>
   <LongitudeDegree>0</LongitudeDegree>
   <LongitudeDMS>W0</LongitudeDMS>
   <LongitudeMinute>0</LongitudeMinute>
   <LongitudeSecond>0</LongitudeSecond>
   <OverviewImage />
   <ParkingLot />
   <PatrollerId>6942bb945e0b</PatrollerId>
   <PatrollerName>PatrollerDefault</PatrollerName>
   <PermitName />
   <Plate>******</Plate>
   <PlateImage />
   <SharpName>PatrollerRight</SharpName>
   <State />
   <Time>18:18:44</Time>
   <TimeLocal>18:18:44</TimeLocal>
   <TimeUtc>22:18:44</TimeUtc>
   <UserId>e1e3ab0bd753</UserId>
   <UserName />
   <VehicleID>6726acb574ae</VehicleID>
  </Read>
  <ToStreetName>1st Avenue</ToStreetName>
 </FirstRead>
 <LastRead>
  <FromStreetName>1st Avenue</FromStreetName>
  <Read>
   <Address>485 (1st Avenue - 1st Avenue), City Name, X1Y</Address>
   <attributes>
    <Attributes>
     <Attribute name="Relative Motion" customFieldGuid="000000000000">Closer</
Attribute>
     <Attribute name="Vehicle Type" customFieldGuid="000000000000">-</Attribute>
     <Attribute name="Confidence Score" customFieldGuid="000000000000">27</
Attribute>
     <Attribute name="Vehicle Make" customFieldGuid="000000000000">Subaru</
Attribute>
     <Attribute name="Speed" customFieldGuid="000000000000">35 km/h</Attribute>
     <Attribute name="Context" customFieldGuid="000000000000">US</Attribute>
     <Attribute name="Characters Height" customFieldGuid="000000000000">18</
Attribute>
     <Attribute name="PatrollerSpeed" customFieldGuid="000000000000">29 mph</
Attribute>
    </Attributes>
   </attributes>
   <CameraName>LprCamera</CameraName>
   <ContextImage />
   <Date>10/01/2022</Date>
   <DateLocal>10/01/2022</DateLocal>
   <DateUtc>10/01/2022</DateUtc>
   <InventoryLocation />
   <IsHit>Yes</IsHit>
   <Latitude>0</Latitude>
   <LatitudeDegree>0</LatitudeDegree>
   <LatitudeDMS>N0</LatitudeDMS>
   <LatitudeMinute>0</LatitudeMinute>
   <LatitudeSecond>0</LatitudeSecond>
   <Longitude>0</Longitude>
   <LongitudeDegree>0</LongitudeDegree>
   <LongitudeDMS>W0</LongitudeDMS>
   <LongitudeMinute>0</LongitudeMinute>
   <LongitudeSecond>0</LongitudeSecond>
   <OverviewImage />
   <ParkingLot />
   <PatrollerId>6942bb945e0b</PatrollerId>
   <PatrollerName>PatrollerDefault</PatrollerName>
   <PermitName />
   <Plate>******</Plate>
   <PlateImage />
   <SharpName>PatrollerRight</SharpName>
   <State />
   <Time>18:19:49</Time>
   <TimeLocal>18:19:49</TimeLocal>
   <TimeUtc>22:19:49</TimeUtc>
   <UserId>e1e3ab0bd753</UserId>
   <UserName />
```

```
    <VehicleID>ffd62bcb09b7</VehicleID>
   </Read>
   <ToStreetName>1st Avenue</ToStreetName>
  </LastRead>
  <RuleColor>#FF191970</RuleColor>
  <RuleId>1d1d6e34d07b</RuleId>
  <RuleName>Data Xporter OT</RuleName>
  <ZoneColor>#FF191970</ZoneColor>
  <ZoneId>1d1d6e34d07b</ZoneId>
  <ZoneName>Data Xporter OT</ZoneName>
 </OvertimeHit>
```

The following is an example of a license plate permit hit event.

NOTE: The binary image data has been removed from the example.

```
<PermitHit>
 <attributes>
  <Attributes>
   <Attribute name="MultipleHit"/>
   <Attribute name="VehicleMake"/>
   <Attribute name="VehicleColor"/>
   <Attribute name="MatchPlate"/>
  </Attributes>
 </attributes>
 <Date>10/01/2022</Date>
 <DateLocal>10/01/2022</DateLocal>
 <DateUtc>10/01/2022</DateUtc>
 <HitID>fa92097260eb</HitID>
 <HotlistCategory />
 <ParkingLot />
 <PatrollerId>6942bb945e0b</PatrollerId>
 <PatrollerName>Adi Patroller</PatrollerName>
 <Time>18:04:21</Time>
 <TimeLocal>18:04:21</TimeLocal>
 <TimeUtc>22:04:21</TimeUtc>
 <UserAction>Enforced</UserAction>
 <UserId>e1e3ab0bd753</UserId>
 <UserName />
 <Hit>
  <Read>
   <Address>360 (1st AVENUE - Main Street), City Name, X1Y</Address>
   <attributes>
    <Attributes>
     <Attribute name="Relative Motion" customFieldGuid="000000000000">Farther</
Attribute>
     <Attribute name="Vehicle Type" customFieldGuid="000000000000">Private</
Attribute>
     <Attribute name="Confidence Score" customFieldGuid="000000000000">99</
Attribute>
     <Attribute name="Vehicle Make" customFieldGuid="000000000000">Suzuki</
Attribute>
     <Attribute name="Speed" customFieldGuid="000000000000">10 mph</Attribute>
     <Attribute name="Context" customFieldGuid="000000000000">State Name</
Attribute>
     <Attribute name="Characters Height" customFieldGuid="000000000000">18</
Attribute>
     <Attribute name="PatrollerSpeed" customFieldGuid="000000000000">29 mph</
Attribute>
    </Attributes>
   </attributes>
   <CameraName>LprCamera</CameraName>
   <ContextImage />
   <Date>10/01/2022</Date>
   <DateLocal>10/01/2022</DateLocal>
   <DateUtc>10/01/2022</DateUtc>
   <InventoryLocation />
   <IsHit>Yes</IsHit>
   <Latitude>0</Latitude>
   <LatitudeDegree>0</LatitudeDegree>
   <LatitudeDMS>N0</LatitudeDMS>
   <LatitudeMinute>0</LatitudeMinute>
   <LatitudeSecond>0</LatitudeSecond>
   <Longitude>0</Longitude>
   <LongitudeDegree>0</LongitudeDegree>
   <LongitudeDMS>W0</LongitudeDMS>
   <LongitudeMinute>0</LongitudeMinute>
   <LongitudeSecond>0</LongitudeSecond>
   <OverviewImage />
   <ParkingLot />
   <PatrollerId>6942bb945e0b</PatrollerId>
   <PatrollerName>PatrollerDefault</PatrollerName>
   <PermitName>Hotlist1</PermitName>
   <Plate>******</Plate>
   <PlateImage />
   <SharpName>PatrollerDefault</SharpName>
   <State />
   <Time>18:04:07</Time>
   <TimeLocal>18:04:07</TimeLocal>
   <TimeUtc>22:04:07</TimeUtc>
   <UserId>e1e3ab0bd753</UserId>
   <UserName />
   <VehicleID>fade04a772ba</VehicleID>
  </Read>
 </Hit>
 <Name>Hotlist1</Name>
 <PermitId>4ce759c9f14d</PermitId>
 <RuleId>4ce759c9f14d</RuleId>
 <RuleName>Hotlist1</RuleName>
 <ZoneId>4ce759c9f14d</ZoneId>
 <ZoneName>Hotlist1</ZoneName>
</PermitHit>
```

The following is an example of a license plate shared permit hit event.

NOTE: The binary image data has been removed from the example.

```
<SharedPermitHit>
 <attributes>
  <Attributes>
   <Attribute name="Category">Hotlist1</Attribute>
   <Attribute name="PlateState"/>
   <Attribute name="MatchPlate">******</Attribute>
   <Attribute name="hide_ClosestMatchPlateNumber">ROBOTO</Attribute>
   <Attribute name="EffectiveDate">Wednesday, January 1, 2022</Attribute>
   <Attribute name="DurationViolated">120</Attribute>
   <Attribute name="hide_ClosestMatchPlateState">QC</Attribute>
   <Attribute name="ExpiryDate">Friday, January 1, 2022</Attribute>
   <Attribute name="hide_SP">87</Attribute>
   <Attribute name="MultipleHit"/>
   <Attribute name="VehicleRead">30d8d6995f4e</Attribute>
   <Attribute name="VehicleMake"/>
   <Attribute name="PermitID">PASTA000</Attribute>
   <Attribute name="VehicleColor"/>
   <Attribute name="VehicleOvertimeGUID">30d8d6995f4e</Attribute>
  </Attributes>
 </attributes>
 <Date>10/01/2022</Date>
 <DateLocal>10/01/2022</DateLocal>
 <DateUtc>10/01/2022</DateUtc>
 <HitID>874c480ab041</HitID>
 <HotlistCategory>Hotlist1</HotlistCategory>
 <ParkingLot />
 <PatrollerId>6942bb945e0b</PatrollerId>
 <PatrollerName>PatrollerDefault</PatrollerName>
 <Time>18:05:22</Time>
 <TimeLocal>18:05:22</TimeLocal>
 <TimeUtc>22:05:22</TimeUtc>
 <UserAction>Enforced</UserAction>
 <UserId>e1e3ab0bd753</UserId>
 <UserName />
 <FirstVehicle>
  <Read>
   <Address>3294 (1st Avenue - Main Street), City Name, X1Y</Address>
   <attributes>
    <Attributes>
     <Attribute name="Relative Motion" customFieldGuid="000000000000">-</Attribute>
     <Attribute name="Vehicle Type" customFieldGuid="000000000000">Temporary</
Attribute>
     <Attribute name="Confidence Score" customFieldGuid="000000000000">95</
Attribute>
     <Attribute name="Vehicle Make" customFieldGuid="000000000000">Volkswagen</
Attribute>
     <Attribute name="Speed" customFieldGuid="000000000000">35 km/h</Attribute>
     <Attribute name="Context" customFieldGuid="000000000000">US</Attribute>
     <Attribute name="Characters Height" customFieldGuid="000000000000">18</
Attribute>
     <Attribute name="PatrollerSpeed" customFieldGuid="000000000000">29 mph</
Attribute>
    </Attributes>
   </attributes>
   <CameraName>LprCamera</CameraName>
   <ContextImage />
   <Date>10/01/2022</Date>
   <DateLocal>10/01/2022</DateLocal>
   <DateUtc>10/01/2022</DateUtc>
   <InventoryLocation />
   <IsHit>Yes</IsHit>
   <Latitude>0</Latitude>
   <LatitudeDegree>0</LatitudeDegree>
   <LatitudeDMS>N0</LatitudeDMS>
   <LatitudeMinute>0</LatitudeMinute>
   <LatitudeSecond>0</LatitudeSecond>
   <Longitude>0</Longitude>
   <LongitudeDegree>0</LongitudeDegree>
   <LongitudeDMS>W0</LongitudeDMS>
   <LongitudeMinute>0</LongitudeMinute>
   <LongitudeSecond>0</LongitudeSecond>
   <OverviewImage />
   <ParkingLot />
   <PatrollerId>6942bb945e0b</PatrollerId>
   <PatrollerName>PatrollerDefault</PatrollerName>
   <PermitName>Hotlist1</PermitName>
   <Plate>******</Plate>
   <PlateImage />
   <SharpName>PatrollerDefault</SharpName>
   <State />
   <Time>18:05:00</Time>
   <TimeLocal>18:05:00</TimeLocal>
   <TimeUtc>22:05:00</TimeUtc>
   <UserId>e1e3ab0bd753</UserId>
   <UserName />
   <VehicleID>30d8d6995f4e</VehicleID>
  </Read>
 </FirstVehicle>
 <Name>Shared permit</Name>
 <RuleId>7a22869b87ba</RuleId>
 <RuleName>Shared permit</RuleName>
 <SecondVehicle>
  <Read>
   <Address>3270 (1st Avenue - Main Street), City Name, X1Y</Address>
   <attributes>
    <Attributes>
     <Attribute name="Relative Motion" customFieldGuid="000000000000">Closer</
Attribute>
     <Attribute name="Vehicle Type" customFieldGuid="000000000000">Taxi</Attribute>
     <Attribute name="Confidence Score" customFieldGuid="000000000000">97</
Attribute>
     <Attribute name="Vehicle Make" customFieldGuid="000000000000">Lexus</
Attribute>
     <Attribute name="Speed" customFieldGuid="000000000000">70 km/h</Attribute>
     <Attribute name="Context" customFieldGuid="000000000000">US</Attribute>
     <Attribute name="Characters Height" customFieldGuid="000000000000">35</
Attribute>
     <Attribute name="PatrollerSpeed" customFieldGuid="000000000000">29 mph</
Attribute>
    </Attributes>
   </attributes>
   <CameraName>LprCamera</CameraName>
   <ContextImage />
   <Date>10/01/2022</Date>
   <DateLocal>10/01/2022</DateLocal>
   <DateUtc>10/01/2022</DateUtc>
   <InventoryLocation />
   <IsHit>Yes</IsHit>
   <Latitude>0</Latitude>
   <LatitudeDegree>0</LatitudeDegree>
   <LatitudeDMS>N0</LatitudeDMS>
   <LatitudeMinute>0</LatitudeMinute>
   <LatitudeSecond>0</LatitudeSecond>
   <Longitude>0</Longitude>
   <LongitudeDegree>0</LongitudeDegree>
   <LongitudeDMS>W0</LongitudeDMS>
   <LongitudeMinute>0</LongitudeMinute>
   <LongitudeSecond>0</LongitudeSecond>
   <OverviewImage />
   <ParkingLot />
   <PatrollerId>6942bb945e0b</PatrollerId>
   <PatrollerName>PatrollerDefault</PatrollerName>
   <PermitName>Hotlist1</PermitName>
   <Plate>******</Plate>
   <PlateImage />
   <SharpName>PatrollerDefault</SharpName>
   <State />
   <Time>18:05:15</Time>
   <TimeLocal>18:05:15</TimeLocal>
   <TimeUtc>22:05:15</TimeUtc>
   <UserId>e1e3ab0bd753</UserId>
   <UserName />
   <VehicleID>ace3c9983847</VehicleID>
  </Read>
 </SecondVehicle>
 <ZoneId>7a22869b87ba</ZoneId>
 <ZoneName>Shared permit</ZoneName>
</SharedPermitHit>
```

The following is an example of a license plate read event.

NOTE: The binary image data has been removed from the example.

```
<?xml version="1.0" encoding="UTF-8"?>
<Read xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
 <Address>360 RUE CHERRIER (AVENUE DU MANOIR - RUE DU PONT), MONTRÃ‰AL, H9C</
Address>
 <attributes>
  <Attributes>
   <Attribute name="Relative Motion"
 customFieldGuid="00000000-0000-0000-0000-000000000000">Farther</Attribute>
   <Attribute name="Vehicle Type"
 customFieldGuid="00000000-0000-0000-0000-000000000000">Private</Attribute>
   <Attribute name="Confidence Score"
 customFieldGuid="00000000-0000-0000-0000-000000000000">99</Attribute>
   <Attribute name="Vehicle Make"
 customFieldGuid="00000000-0000-0000-0000-000000000000">Suzuki</Attribute>
   <Attribute name="Speed"
 customFieldGuid="00000000-0000-0000-0000-000000000000">10 mph</Attribute>
   <Attribute name="Context"
 customFieldGuid="00000000-0000-0000-0000-000000000000">Quebec</Attribute>
   <Attribute name="Characters Height"
 customFieldGuid="00000000-0000-0000-0000-000000000000">18</Attribute>
   <Attribute name="PatrollerSpeed"
 customFieldGuid="00000000-0000-0000-0000-000000000000">29 mph</Attribute>
  </Attributes>
 </attributes>
 <CameraName>Adi Patroller Right - LprCamera</CameraName>
 <ContextImage/>
 <Date>10/01/2022</Date>
 <DateLocal>10/01/2022</DateLocal>
 <DateUtc>10/01/2022</DateUtc>
 <InventoryLocation/>
 <IsHit>Yes</IsHit>
 <Latitude>45.489108355432</Latitude>
 <LatitudeDegree>45</LatitudeDegree>
 <LatitudeDMS>N45 29 20</LatitudeDMS>
 <LatitudeMinute>29</LatitudeMinute>
 <LatitudeSecond>20</LatitudeSecond>
 <Longitude>-73.874856786922</Longitude>
 <LongitudeDegree>-73</LongitudeDegree>
 <LongitudeDMS>W-73 52 29</LongitudeDMS>
 <LongitudeMinute>52</LongitudeMinute>
 <LongitudeSecond>29</LongitudeSecond>
 <OverviewImage/>
 <ParkingLot/>
 <PatrollerId>abdbcaea-5f6a-4293-acc9-6942bb945e0b</PatrollerId>
 <PatrollerName>Adi Patroller</PatrollerName>
 <PermitName>Hotty</PermitName>
 <Plate>******</Plate>
 <PlateImage/>
 <SharpName>Adi Patroller Right</SharpName>
 <State/>
 <Time>18:04:07</Time>
 <TimeLocal>18:04:07</TimeLocal>
 <TimeUtc>22:04:07</TimeUtc>
 <UserId>64ebdce0-f4ed-4630-a33f-e1e3ab0bd753</UserId>
 <UserName/>
 <VehicleID>229d2f22-f88b-49d0-b4d1-fade04a772ba</VehicleID>
</Read>
```

ALPR Manager - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role. All must have access to the role database.
- **Database status:** Current status of the database.
- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.
- **Database:** Name of the database instance.
- **Actions:** You can perform the following functions on the role database:
  - **Create a database (➕):** Create a new database with the option to overwrite the existing one.
  - **Delete the database (❌):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (🔔):** Set up notifications for when the database space is running low.
  - **Backup/Restore (▭):** Back up or restore the database.
- **Authentication:** Specifies which SQL Server authentication is to be used:
  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.
- **Images saved to:** Archiver role responsible to manage the images (license plate, contextual, and wheel images) that are associated to the reads and hits.

  BEST PRACTICE: Select an Archiver that is not also managing video units. If all your current Archiver roles are managing video units, create a new one.

NOTE: When using the cloud base Azure database, the *Notifications* and *Backup/restore* options are disabled.

Related Topics

Creating databases on page 140

Deleting databases on page 141

Viewing database information on page 145

Receiving notifications when databases are almost full on page 146

Backing up databases on page 147

Restoring databases on page 151

Archiver: Camera default settings tab

You can use the *Camera default settings* page to configure the default recording settings applied to all cameras that are controlled by the Archiver role.

Click the **Camera default settings** tab to view or configure the following settings:

- **Video quality:** Select a **Resolution**.
  - **High:** 1270x720 and greater.
  - **Standard:** Between 320x240 - 1280x720.
  - **Low:** 320x240 and less.
  - **Default:** Manufacturer default settings.
  - **Frame rate:** You can select a value from 1 - 30 fps. Does not apply to default settings.
- **Recording mode:** Specifies when recording should take place. Select one of the following modes:
  - **Continuous:** Records continuously. Recording cannot be stopped by the user (🔴🔒).
  - **On motion/Manual:** Recording begins when triggered by the following:
    - A specific action, such as *Start recording*, *Add bookmark*, or *Trigger alarm*
    - Motion detection
    - User requests

    In this mode, the **Record** button in Security Desk indicates the recording status:
    - Grey (⚫) when the system is not recording. Clicking the button starts the recording.
    - Red (🔴) when the system is recording. Clicking the button stops the recording.
    - Red with a lock (🔴🔒) when the system is recording and cannot be stopped by the user, such as on motion or on alarm.
  - **Manual:** Records only when a user or a system action, such as *Start recording*, *Add bookmark*, or *Trigger alarm*, requests it.
  - **Custom:** Recording is specified by custom schedules.
    CAUTION: Two recording schedules of the same priority level, for example two daily schedules, cannot overlap, regardless of the recording mode configured for each. When a scheduling conflict occurs, the Archiver role and the video units are displayed in yellow in the entity browser and they issue entity warning messages. For more information, see Schedule conflicts on page 585.
  - **Off:** Recording is not permitted (⚫🔒), even when alarms are triggered.
- **Automatic cleanup:** Specifies a retention period for recorded video (in days).

  NOTE: Video archives older than this period are deleted.
- **(Optional) Show advanced settings:** Click to configure the advanced recording settings.
- **Record audio:** Switch **ON** to record audio with your video. A microphone entity must be attached to your cameras.

  NOTE: It is not necessary for the attached devices to belong to the same unit as the video encoder. However, for audio recording to work, ensure that the microphone belongs to a unit managed by the same Archiver, with the same Archiver extension, as the video encoder.
- **Record metadata:** Switch **ON** to record metadata with your video. Recording metadata is useful for analytics and for filtering recorded video.
- **Redundant archiving:** Switch **ON** to allow primary, secondary, and tertiary servers to archive video, and audio, at the same time. This setting is effective only if failover is configured.
- **Time to record before an event:** Use the slider to set the duration (in seconds) recorded before an event. This buffer is saved whenever the recording starts, ensuring that whatever prompted the recording is also captured on video.
- **Time to record after a motion:** Use the slider to set the duration (in seconds) recorded after a motion event. During this time, the user cannot stop the recording.

- **Default manual recording length:** Use the slider to select the duration (in minutes) the recording lasts when it is started manually by a user, or when the *Start recording* action is triggered.
- **Encryption:** Specifies whether or not to encrypt your video data. In this context, video refers to all media types: video, audio, and metadata.
  - **None:** The video is not encrypted.
  - **In transit from Archiver:** (Default) The video is encrypted only when it is streamed from the Archiver. The video archive is not encrypted. All users who have the right to access the camera can view the encrypted video. There is no need to install any *encryption certificates*. Use this option if your archive storage is secured behind firewalls.

    You must enable **Secure communication** on the Media Router for this option to work.

    This option has the following limitations:
    - Multicast from the unit is not supported
    - Audio streamed from Security Desk only supports TCP connection type
    - Video streamed to analog monitors is not encrypted in transit
    - Privacy protected streams are not encrypted in transit
    - Backward compatibility (Security Center 5.7 and earlier) is not supported:
      - Clients in compatibility mode cannot view video encrypted in transit
      - Auxiliary Archiver roles in backward compatibility mode cannot archive video encrypted in transit
      - Redirectors in backward compatibility mode cannot redirect video encrypted in transit
  - **In transit and at rest:** The video is encrypted after it reaches the Archiver, using *fusion stream encryption*. The video archive on disk is also encrypted. If the video unit supports encryption and is connected through HTTPS, then the video is encrypted end-to-end.

    To enable this option, you must install at least one encryption certificate on the server hosting the Archiver role.

    The video can only be viewed in one of the following ways:
    - Using a workstation with a certificate that matches one of the listed certificates on the Archiver. Access is restricted to the workstation.
    - Using a smart card with a certificate that matches one of the listed certificates on the Archiver. Access is restricted to the holder of the smart card.

    We recommend this option when your data center is managed by a third party.

    This option has the following limitations:
    - Video thumbnail and motion detection by the Archiver are not supported.
    - Multicast from the unit is supported only if the unit supports encryption.
    - Video encrypted in version 5.8 and later cannot be decrypted in version 5.7 and earlier.
- **Custom settings per server:** Switch **ON** to configure different archiving and retention settings for each server assigned to this Archiver role. Per-server settings is useful when managing limited data storage.
- **Archiving enabled:** Switch **ON** to enable video archiving on this server. When disabled and the Archiver role is running on this server, cameras are used only for live viewing and any recording schedule configuration is ignored.

NOTE:

- Recording settings that are configured in the Security Center installer assistant are carried over to the **Camera default settings** tab.
- Recording settings defined on the **Recording** tab of an individual camera supersede the settings defined on the **Camera default settings** tab.

Related Topics

Creating schedules on page 204
Configuring camera settings on page 614
Setting up Archiver failover on page 193
Configuring the Media Router role on page 597
What is fusion stream encryption? on page 543

Archiver: Extensions tab

You can use the *Extensions* page to configure the common connection parameters shared by the video units that are controlled by the Archiver. The extensions are automatically created when you add a unit to the Archiver.

Click the **Extensions** tab to view or configure the following settings:

- **Transaction timeout:** Time that is spent waiting for a response before re-sending a command to the unit.
- **Command port:** (Bosch only) Port used by the Archiver to send commands to the Bosch units. This field has default values that get reset every time the **Protocol** field is modified.
- **Protocol:** (Bosch only) Transport protocol used by the Archiver to send commands to the Bosch units.

  The accepted values are:

  - **RCP:** Use RCP+ over TCP (default). The command port must be set to 1756.
  - **HTTP:** Use HTTP or HTTPS (RCP+ over CGI).

    IMPORTANT: To enroll a Bosch unit using either HTTP or HTTPS, you must manually create the Bosch extension, or modify an existing one.

    - To use HTTP, set **Command port** to match the value of **HTTP browser port** configured on the Bosch unit.
    - To use HTTPS, set **Use HTTPS** to **On** under the *Default logon* group, and set **Port** to match the value of **HTTPS browser port** configured on the Bosch unit.

    NOTE: The command ports configured in the Bosch extension are default values. The values configured on the Bosch units might be different. The **Discovery port** must match the values configured on the Bosch units.
- **RSTP port:** RTSP (Real Time Streaming Protocol) port used by the Archiver to request video from the units that support this protocol.

  The RTSP port is used to listen for RTSP (Real Time Streaming Protocol) requests. When multiple archiving roles are hosted on the same server, this value must be unique for each one. The configured value cannot be the same as any value used for the Media Router role, its redirector agent, or any Auxiliary Archiver hosted on the same server.
- **VSIP port:** (Verint only) Port used for *automatic discovery*. All units that are controlled through the same Verint extension must be configured with the same *VSIP port*. All Verint extensions configured for the same Archiver must have different discovery ports.
- **Refuse basic authentication:** Use this switch to enable and disable basic authentication for an extension. This is useful if you turned off basic authentication in the Security Center InstallShield, but need to turn it on again to use a camera that only supports basic authentication. To turn basic authentication on again, you must switch **Refuse basic authentication** to **Off**.
- **Discovery port:** Automatic discovery port. If multiple instances of the same type of extension are configured for the same Archiver, they must all use a different discovery port.

  - (ACTi) Corresponds to the *Search server port 1* in the ACTi video server settings.
  - (Bosch) All units that are controlled through the same Bosch extension must be configured with the same discovery port.

  NOTE: If you decide to change the *Discovery port* after the units are discovered, you must create a new extension with the new discovery port and delete the old one. If the units are not automatically discovered, you must add them manually.
- **Discovery reply port:** (ACTi and Interlogix) Corresponds to the *Search server port 2* in the ACTi video server settings.
- **Unicast period:** Time period in which the extension repeats its connection tests using unicast to determine whether each unit is still active in the system.

- **Multicast period:** Time period in which the extension attempts to discover new units using multicast. This option can be disabled. The IP address that follows is the standard multicast IP address used by *Omnicast*™. Change the standard multicast IP address only if it is already used for something else.
- **Broadcast period:** Time period in which the extension attempts to discover new units using broadcast. This option can be disabled.
- **Default logon:** Certain types of units can be protected by a username and a password against illegal access. The logon credentials can be defined individually for each unit or for all units using the same extension.
  - **Username:** Certain types of units (such as Axis) require a username.
  - **Password:** Certain types of units (such as Bosch) require only a password.
  - **Use HTTPS:** Select this option to use *Secure Hypertext Transfer Protocol* for added security.

    NOTE: For Bosch units, this setting only appears when **Protocol** is set to **HTTP**. When **Use HTTPS** is set to **On**, the **Port** set here supercedes the **Command port**.
- **TCP notification port:** (Panasonic and Interlogix) Port used by the Archiver role to receive notifications from the units. When an event occurs, such as *Signal lost* or *Signal recovered*, the unit initiates a *TCP* connection with the Archiver and sends the notification through this port.

  NOTE: (Panasonic) When multiple Archiver roles are running on the same server or are configured to listen to the same units, each Archiver role must be associated to a unique TCP notification port.
- **Notification channel:** (Interlogix only) When you configure multiple Archiver roles to listen to the same units, such as in a failover list, each Archiver must be identified with a different notification channel (1 to 8). You can ignore this parameter if you are using only one Archiver. For multiple Archiver roles, you must follow these rules:
  - All Archiver roles that control the same units must be configured with the same TCP notification port.
  - All Archiver roles must use a different notification channel.
- **Bosch VRM settings:** The VRM settings are exclusive to Bosch VRM (Video Recording Manager). You can use these settings to query and play back video from Bosch cameras that are managed by a Bosch VRM. Multiple Bosch extensions can use the same VRM. VRMs serve as failovers if one VRM goes offline or is unreachable. If all listed VRMs on an extension are not configured correctly, archived video might not be found by the Archiver. You can add more than one VRM to a Bosch extension and use the move up (▲) and move down (▼) buttons to move a VRM up or down on the list. The Archiver uses the first VRM on the list for queries and archived video. If the first VRM is not available, the Archiver uses the next VRM on the list.

  NOTE: For the Bosch VRM to work properly in Security Center, you must configure the CHAP password on the device. See the Bosch documentation for information on configuring the CHAP password.
- **Verint specific settings:** The following settings are found only on Verint units.
  - **Show all available video streams as separate cameras:** (Verint only) Omnicast™ supports encoders that generate multiple video streams from the same video source. When these encoders are discovered, the Archiver creates a *video encoder* with multiple streaming alternatives. Select this option to represent every video stream as a separate camera.
    NOTE: This option requires a camera connection license for each stream.
  - **SSL settings:** SSL (Secure Sockets Layer) is a protocol used to protect applications that need to communicate over a network. Security Center supports SSL on all message transmissions between the Archiver and the units, except for video streams because the volume of data is too high. The purpose for using SSL in Security Center is to prevent attacks, not to stop eavesdropping. Select *Enforce SSL* only if SSL must be enforced on all units controlled by this Archiver. If this option is cleared, the Archiver will use SSL only to communicate with the units on which SSL is enabled.
- **Advanced security settings:** Depending on the certificate used on the camera, you might need to configure some advanced security settings.

  - **Allow unknown certificate authority:** Set this option to ON for the Archiver to accept self-signed certificates.
  - **Allow non-server certificates:** Set this option to ON for the Archiver to accept non-server certificates.
  - **Allow certificates with invalid subject name:** Set this option to ON for the Archiver to accept certificates that do not have the IP address or hostname of the unit entered as the Subject name and Alternative name.
  - **Allow certificates with invalid date:** Set the option to ON for the Archiver to accept expired certificates.
- **Advanced settings:** The advanced settings are reserved for use by Genetec™ Technical Assistance Center.
- **NTP settings:** Synchronizes the time between the units that support NTP (Network Time Protocol), and the NTP server. Keeping the units' time synchronized is particularly important for units that handle video archiving.

  NOTE: This feature may not apply to all extensions. Currently, only the following extensions are supported: Acti, Axis, Bosch, Generic Plus, Genetec Protocol, and Sony.
  You must set the following parameters:

  - **NTP server:** Specify the NTP server name.
  - **NTP port:** Specify the NTP server port number.
  - **Poll timeout:** Specify how often you want the time on the units to be checked to ensure that they are properly synchronized with the NTP server. For example, if 60 seconds is entered, the time is verified every 60 seconds.

Archiver: Resources tab

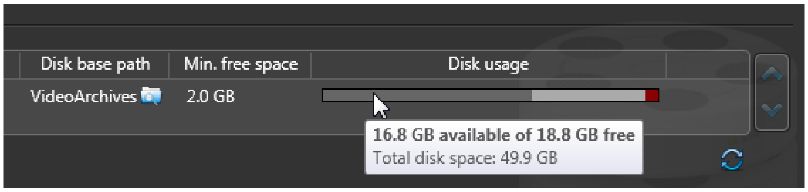
You can use the *Resources* page to configure the archive storage and view the operation statistics of the Archiver role.

Click the **Resources** tab to assign servers, databases, and disk storage to this Archiver role.

- **Server (⊕):** One of the servers hosting this Archiver role. You can assign a maximum of three servers to an Archiver role for failover purposes using the tabs at the bottom of the page.
  - **Network card:** Network card used to communicate with all video units.
  - **RTSP port:** Ports used to listen for RTSP (Real Time Streaming Protocol) requests. When multiple archiving roles are hosted on the same server, these values must be unique for each one. The default values are 555 and 605 for the Archiver and 558 for the Auxiliary Archiver. The values configured must not duplicate any values used for the Media Router role or its redirector agent hosted on the same server.
  - **Telnet port:** Port used to listen to the *Telnet console* connection requests for debugging purposes. When you change this value, you need to deactivate and reactivate the Archiver role for the change to take effect.
  - **Live streaming reception UDP ports:** For each Archiver agent, you can manually assign live streaming UDP ports, which are used to receive the streams from the cameras. Each camera can require multiple ports (1 port per peripheral). Therefore, the port range must be large enough to accommodate all peripherals for all devices. If your configuration exceeds the maximum port limit (65535), you can change the default start port (15000) and the allocated ports per Archiver agent (5000).
- **Database status:** Current status of the database.
- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.
- **Database:** Name of the database instance.
- **Actions:** You can perform the following functions on the role database:
  - **Create a database (➕):** Create a new database with the option to overwrite the existing one.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (🔔):** Set up notifications for when the database space is running low.
  - **Backup/Restore (▭):** Back up or restore the database.
- **Authentication:** Specifies which SQL Server authentication is to be used:
  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.
- **Recording:** Displays information about local drives and network drives, which can be used to store video footage. All local drives found on the host server are listed by default and grouped under *Default Disk Group*.

- **Disk base path:** Root folder on the disk where all video files are found. The default value is *VideoArchives*.
- **Min. free space:** Minimum free space that the Archiver must never use on the disk. The default value is .2% of total disk space capacity.
- **Disk usage:** Chart showing the total capacity of the disk (full chart), the minimum free space (red), the occupied disk space (dark gray), and the remaining free space for video archives (light gray). Hover over the chart with the mouse to display these values in a tooltip.



Disk base path	Min. free space	Disk usage
VideoArchives	2.0 GB	

16.8 GB available of 18.8 GB free
Total disk space: 49.9 GB

- **Add network location (🖧):** You can only add network drives to your archive storage. All local drives on the host server are listed by default. You can exclude them from being used by the Archiver by clearing the checkbox in front of each disk.
- **Add group:** A disk group is a logical storage unit used by the Archiver to improve the overall disk throughput. Click the **Up** and **Down** arrows to move the selected disk from one group to another.
- **Delete (✖):** Deletes the selected disk or disk group. Each disck group must have at least one disk associated to it.
- **Camera distribution (⚖):** Divide the cameras between the disk groups. This button appears only if you have more than one disk group defined.
- **Refresh drive information (🔄):** Refreshes the drive information.

- **Backup configuration:** Settings for archive transfer.
  - **Backup folder:** Location in which the backed up archives are saved as a G64x file.
  - **Delete oldest files when disks are full:** Turn on this option to delete the oldest video archives when the disk is full.
  - **Automatic cleanup:** Turn this option on to specify a retention period for the backed up video archives (in days). If you do not enable this option, the backed up video archives are not deleted by the system, and you must manually delete them.

Archiver statistics

The *Statistics* dialog box appears when you click the **Statistics** (◕) button. It provides information regarding the archive storage, and the rate at which it is being consumed.

- **Refresh (🔄):** Refreshes the statistics.
- **List of assigned disks:** Snapshot of the disk statistics taken from the last time a refresh occurred.
  - **Used space:** Amount of space used by video archives.
  - **Available space:** Available free space for video archives (equals *Free space on disk* minus *Min. free space*).
  - **Free space:** Free space on disk.
  - **Load percentage:** Percentage of space used over the allotted space.
  - **R/W:** Indicates whether the role has read and write access to the folder.
- **Protected video file statistics (◕):** View the percentage of protected video files on the selected disk.
- **Average disk usage:** Average space used per day (first line) and average space used per camera per day (second line).
- **Estimated remaining recording time:** Number of days, hours, and minutes of recording time remaining based on the average disk usage and the current load.
- **Active cameras:** Number of cameras detected by the Archiver.

- **Archiving cameras:** Number of cameras that have archiving enabled (Continuous, On event, or Manual) and that are not suffering from any issue that prevents archiving.

  See details: View the *recording state* and statistics of each individual camera in the *Archiving cameras* dialog box. The statistics are taken from the last refresh of the *Statistics* dialog box. This report allows you to verify whether each encoder is currently streaming video (and audio), whether the Archiver is currently recording the data, and the rate at which the events were received from the cameras over the last minute.
- **Total number of cameras:** Total number of cameras assigned to this role.
- **Archiving span:** Time bracket in which video archives can be found.
- **Archiver receiving rate:** Rate at which the Archiver is receiving data.
- **Archiver writing rate:** Rate at which the Archiver is writing to disk.
- **Network traffic in:** Incoming network traffic bit rate on this computer.
- **Network traffic out:** Outgoing network traffic bit rate on this computer.

Advanced settings

The advanced settings are independent of the server hosting the role.

- **Digital signature:** Turn on this option to protect your video archive against tampering.
- **Delete oldest files when disks are full:** Turn on this option to recycle the archive storage (the default mode). The oldest files are deleted to make space for new files when all the disks within a disk group are full.
- **Enable edge playback requests:** Turn on this option only if the Archiver controls units that are configured for *edge recording*. By default, this option is turned off to prevent sending playback requests to units that are not recording.
- **Enable thumbnail requests:** Turn on this option to show video thumbnails for the Archiver (for example, in reports). This option must also be turned on to send snapshots using the *Email a snapshot* action.
- **Enable archive consolidation:** Turn this option on to duplicate video archives from the secondary or tertiary Archiver server on the primary Archiver server after an Archiver failover occurs. The primary Archiver server checks every hour for video archives that can be consolidated from the secondary or tertiary servers for the period it was offline.
- **Enable Telnet console:** Turn on this option to enable the Telnet debug console for this Archiver.
- **Protected video threshold:** This is a safety threshold that limits the amount of space that protected video files can occupy on disks. The percentage you set is the proportion of protected video that you can have of the total size of recorded videos on the disk. Protected video files are files that will not be deleted by normal archive cleanup procedures. If this threshold is exceeded, the Archiver generates the *Protected video threshold exceeded* event once every 15 minutes for as long as the condition is true, but will not delete any video file that is protected.
- **Disk load warning threshold:** The percentage of disk space that must be occupied before the *Disk load threshold exceeded* event is generated. The default value is 90%. The Archiver generates this event once every hour for as long as the condition is true. The disk load is calculated as follows:

  Disk load = Occupied disk space / (Total disk capacity - Min. free space)
- **Max archive transfer throughput:** The maximum bandwidth available for outbound data transfers from the archiving role. Applies to individual data transfers between Archivers and to Cloud Storage.

  NOTE: The same limit is applied to archive transfers and Cloud uploads.
- **Maximum simultaneous edge transfer cameras:** The maximum number of edge transfer cameras the role can handle at any given time.
- **Video files:** These two settings are used to control the size of the video files created by the Archiver:

  - **Maximum length:** Limits the length of video sequence contained in each file. The video length is the time span between the first video frame and the last video frame stored in a file. The default value is 20 minutes.
  - **Maximum size:** Limits the size of the video file. The default value is 500 MB. The Archiver starts saving the video to a new video file when either one of these conditions is met.
- **Monitor incoming events:** Use these settings to monitor and detect a high rate of incoming events from cameras connected to the Archiver. When the event rate is reached, a warning message identifies the problematic cameras and allows you to investigate and take action.
  - **Send notification for high event rate:** Turn on this option to enable the event monitor and define the event rate (enabled by default).
  - **Event threshold:** The number of events that must be received from all the cameras within the defined time period, to trigger the warning. The default value is 10,000.
  - **Time period:** The amount of time in which the event threshold must be reached to trigger the warning. The default value is 5 minutes.

  NOTE: Changing the time period in the event monitor resets the event counters for all the cameras to zero.
- **Additional settings:** These additional settings are reserved for use by our Technical Assistance personnel.

Related Topics

Ports used by Omnicast applications in Security Center on page 1460
Creating databases on page 140
Deleting databases on page 141
Viewing database information on page 145
Receiving notifications when databases are almost full on page 146
Backing up databases on page 147
Restoring databases on page 151

Authentication Service - Properties tab (OpenID)

You can configure an Authentication Service using the OpenID protocol from the **Roles** view of *System* task in Security Center Config Tool.

In the **Properties** tab, you can configure an OpenID identity provider for third-party authentication.

- **Protocol:** Sets the authentication protocol to use with this identity provider. Changing the protocol migrates the Authentication Service configuration between OpenID and SAML2.

  CAUTION: Depending on the original configuration, migrating an Authentication Service role to another protocol might leave errors in the new configuration. After migrating, ensure that the new configuration is complete and accurate before using it.
- **Display name:** Identifies this provider on the client logon screen. Each provider is presented as a button with the text "Sign in with <*display name*>".
- **Issuer:** Secure URL (https) pointing to the provider's OpenID discovery document. This metadata file contains all necessary information to interact with the third-party identity provider, including endpoint locations and capabilities.
- **Domain names:** A list of domain names associated with users who will connect to Security Center using this identity provider. Usernames that include one of these domains will automatically be redirected to the provider's logon screen.
- **Client ID:** The client ID (also known as *audience*) is a unique identifier for Security Center that is issued by the identity provider when the application is registered.
- **Confidential client:** This option is turned off by default. Turn it on to setup Security Center as a confidential client of this identity provider. Being a confidential client is more secure and is highly recommended. Confidential clients use a private client secret to identify themselves to the identity provider.
- **Client secret:** Only displayed when **Confidential client** is switched on. The client secret is a confidential password issued by the identity provider when Security Center is registered as a confidential client.
- **Username claim:** OpenID claim used by the identity provider to return the username of the authenticated party. Security Center requires a username to authorize access to the client.
- **Group claim:** OpenID claim used by the identity provider to return the group memberships of the authenticated party. Security Center requires group membership to authorize access to the client.
- **Resource ID:** ADFS only. URI containing the Relying Party Identifier for Security Center.
- **Audience:** Keycloak only. Access tokens returned by Keycloak specify an audience that is different from the **Client ID**. That audience must be specified here.
- **Obtain claims from:** Specifies where Security Center should obtain claims made by this identity provider. Claims can be obtained from an access token, UserInfo endpoint, or both.
- **Scopes:** Azure AD only. The custom scopes defined for the Security Center application.
- **Custom parameters:** If required, specify one or more custom parameters to send to this identity provider with every authentication request. Custom parameters are not defined by the OpenID protocol and are intended to meet the needs of non-standard configurations.
- **User groups:** Add or remove Security Center user groups that are associated with this identity provider. If your identity provider can export a list of groups in CSV format, that list can be imported here. Groups missing from this list are not associated with the identity provider and will not be used to authorize incoming users.

Related Topics

OpenID Connect Integration overview on page 493

Authentication Service - Properties tab (SAML2)

You can configure an Authentication Service using the SAML2 protocol from the **Roles** view of *System* task in Security Center Config Tool.

In the **Properties** tab, you can configure a SAML2 identity provider for third-party authentication.

- **Protocol:** Sets the authentication protocol to use with this identity provider. Changing the protocol migrates the Authentication Service configuration between OpenID and SAML2.

  CAUTION: Depending on the original configuration, migrating an Authentication Service role to another protocol might leave errors in the new configuration. After migrating, ensure that the new configuration is complete and accurate before using it.
- **Display name:** Identifies this provider on the client logon screen. Each provider is presented as a button with the text "Sign in with <*display name*>".
- **Issuer:** EntityId URI for the identity provider.
- **Metadata URL:** Secure URL (https) pointing to the provider's SAML2 metadata document. This file contains all necessary information to interact with the third-party identity provider, including endpoint locations and capabilities.
- **Client ID:** The client ID (also known as *audience*) is a unique identifier for Security Center that is issued by the identity provider when the application is registered.
- **Domain names:** A list of domain names associated with users who will connect to Security Center using this identity provider. Usernames that include one of these domains will automatically be redirected to the provider's logon screen.
- **Use artifact resolution:** This option is turned off by default. Turn it on to use the Artifact Resolution Protocol if it is supported by your identity provider. Artifact resolution provides a more secure form of authentication.
- **Username assertion:** SAML2 assertion used by the identity provider to return the username of the authenticated party. Security Center requires a username to authorize access to the client.
- **Group assertion:** SAML2 assertion used by the identity provider to return the group memberships of the authenticated party. Security Center requires group membership to authorize access to the client.
- **User groups:** Add or remove Security Center user groups that are associated with this identity provider. If your identity provider can export a list of groups in CSV format, that list can be imported here. Groups missing from this list are not associated with the identity provider and will not be used to authorize incoming users.

Related Topics

SAML 2.0 Integration overview on page 515

Authentication Service - Properties tab (WS-Federation or WS-Trust)

In the **Properties** tab, you can configure your trust chain, and all the ADFS groups that you accept as Security Center user groups.

- **Trust chain (domains):** The trust chain defines the domain of your *root ADFS*, the ADFS server that the role is directly talking to, and the domains of remote ADFS servers that Security Center is receiving claims (*Group* and *UPN*) from, through the root ADFS.
- **Accepted user groups:** User groups corresponding to the ADFS groups that Security Center accepts. These user group names must match the name defined by the remote ADFS servers, followed by the ADFS domain name. For example: *operators@companyXYZ.com*.

Auxiliary Archiver - Camera recording tab

You can use the *Camera recording* page to configure the default recording settings applied to all cameras associated to the Auxiliary Archiver role. Recording settings defined on the *Recording* page of individual cameras supersede the settings defined on the *Camera recording* page of the Auxiliary Archiver.

Click the **Camera recording** tab to view or configure the following settings:

- **Video stream:** Select the default video stream that the Auxiliary Archiver should record for each camera. The video streams are configured for each individual camera.
- **Recording modes:** Apply different recording modes on different schedules.
  - **Continuous:** Records continuously. Recording cannot be stopped by the user (🔴🔒).
  - **Manual:** Records only when a user or a system action, such as *Start recording*, *Add bookmark*, or *Trigger alarm*, requests it. In this mode, the **Record** button in Security Desk indicates the recording status:
    - Grey (●) when the system is not recording. Clicking the button starts the recording.
    - Red (🔴) when the system is recording. Clicking the button stops the recording.
    - Red with a lock (🔴🔒) when the system is recording and cannot be stopped by the user, such as on alarm.
  - **Custom:** Recording is specified by custom schedules.
    CAUTION: Two recording schedules of the same priority level, for example two daily schedules, cannot overlap, regardless of the recording mode configured for each. When a scheduling conflict occurs, the Archiver role and the video units are displayed in yellow in the entity browser and they issue entity warning messages. For more information, see Schedule conflicts on page 585.
  - **Off:** Recording is not permitted (●🔒), even when alarms are triggered.
- **Automatic cleanup:** Specifies a retention period for recorded video (in days).
  NOTE: Video archives older than this period are deleted.
- **(Optional) Show advanced settings:** Click to configure the advanced recording settings.
- **Record audio:** Switch **ON** to record audio with your video. A microphone entity must be attached to your cameras.

  NOTE: It is not necessary for the attached devices to belong to the same unit as the video encoder. However, for audio recording to work, ensure that the microphone belongs to a unit managed by the same Archiver, with the same Archiver extension, as the video encoder.
- **Record metadata:** Switch **ON** to record metadata with your video. Recording metadata is useful for analytics and for filtering recorded video.
- **Time to record before an event:** Use the slider to set the duration (in seconds) recorded before an event. This buffer is saved whenever the recording starts, ensuring that whatever prompted the recording is also captured on video.
- **Time to record after a motion:** Use the slider to set the duration (in seconds) recorded after a motion event. During this time, the user cannot stop the recording.
- **Default manual recording length:** Use the slider to select the duration (in minutes) the recording lasts when it is started manually by a user, or when the *Start recording* action is triggered.

Related Topics

Creating schedules on page 204

Configuring camera settings on page 614

Auxiliary Archiver - Cameras tab

You can use the *Cameras* page to configure the cameras recorded by the Auxiliary Archiver role.

Click the **Cameras** tab to view or configure the cameras assigned to this role. The Auxiliary Archiver can record any camera on your system, except cameras federated from an Omnicast™ 4.x system.

Auxiliary Archiver - Resources tab

You can use the *Resources* page to configure the archive storage and view the operation statistics of the Auxiliary Archiver role.

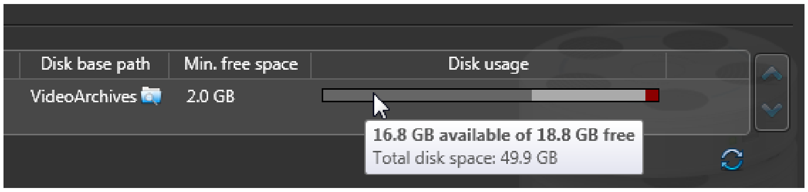
Click the **Resources** tab to assign servers, databases, and disk storage to this Auxiliary Archiver role.

- **Server (⊕):** Server hosting this role. Failover is not supported for the Auxiliary Archiver role. You can only select one server.
  - **Network card:** Network card used to communicate with all video units.

  NOTE: If a customer has multiple network cards and wants to specify which network card the units communicate with, then the connection type must be set to Multicast.

  - **RTSP port:** Ports used to listen for RTSP (Real Time Streaming Protocol) requests. When multiple archiving roles are hosted on the same server, these values must be unique for each one. The default values are 555 and 605 for the Archiver and 558 for the Auxiliary Archiver. The values configured must not duplicate any values used for the Media Router role or its redirector agent hosted on the same server.
- **Database status:** Current status of the database.
- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.
- **Database:** Name of the database instance.
- **Actions:** You can perform the following functions on the role database:
  - **Create a database (✚):** Create a new database with the option to overwrite the existing one.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications ():** Set up notifications for when the database space is running low.
  - **Backup/Restore ():** Back up or restore the database.
- **Authentication:** Specifies which SQL Server authentication is to be used:
  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.
- **Disk information:** Displays information about both local drives and network drives, which can be used to store video footage. All local drives found on the host server are listed by default and grouped under *Default Disk Group*.
  - **Disk base path:** Root folder on the disk where all video files are found. The default value is *AuxiliaryArchives*.
  - **Min. free space:** Minimum free space that the Auxiliary Archiver must never use on the disk. The default value is 1% of total disk space capacity.
  - **Disk usage:** Chart showing the total capacity of the disk (full chart), the minimum free space (red), the occupied disk space (dark gray), and the remaining free space for video archives (light gray). Hover over the chart with the mouse to display these values in a tooltip.



- **Add network location ( ):** You can only add network drives to your archive storage. All local drives on the host server are listed by default. You can exclude them from being used by the Archiver by clearing the checkbox in front of each disk.
- **Add group:** A disk group is a logical storage unit used by the Archiver to improve the overall disk throughput. Click the **Up** and **Down** arrows to move the selected disk from one group to another.
- **Delete ( ):** Deletes the selected disk or disk group. Each disck group must have at least one disk associated to it.
- **Camera distribution ( ):** Divide the cameras between the disk groups. This button appears only if you have more than one disk group defined.
- **Refresh drive information ( ):** Refreshes the drive information.

Auxiliary Archiver statistics

The *Statistics* dialog box appears when you click the **Statistics** ( ) button. It provides information regarding the archive storage, and the rate at which it is being consumed.

- **Refresh ( ):** Refreshes the statistics.
- **List of assigned disks:** Snapshot of the disk statistics taken from the last time a refresh occurred.
  - **Used space:** Amount of space used by video archives.
  - **Available space:** Available free space for video archives (equals *Free space on disk* minus *Min. free space*).
  - **Free space:** Free space on disk.
  - **Load percentage:** Percentage of space used over the allotted space.
  - **R/W:** Indicates whether the role has read and write access to the folder.
- **Protected video file statistics ( ):** View the percentage of protected video files on the selected disk.
- **Average disk usage:** Average space used per day (first line) and average space used per camera per day (second line).
- **Estimated remaining recording time:** Number of days, hours, and minutes of recording time remaining based on the average disk usage and the current load.
- **Active cameras:** Number of cameras detected by the Archiver.
- **Archiving cameras:** Number of cameras that have archiving enabled (Continuous, On event, or Manual) and that are not suffering from any issue that prevents archiving.

  See details: View the *recording state* and statistics of each individual camera in the *Archiving cameras* dialog box. The statistics are taken from the last refresh of the *Statistics* dialog box. This report allows you to verify whether each encoder is currently streaming video (and audio), whether the Archiver is currently recording the data, and the rate at which the events were received from the cameras over the last minute.
- **Total number of cameras:** Total number of cameras assigned to this role.
- **Archiving span:** Time bracket in which video archives can be found.
- **Archiver receiving rate:** Rate at which the Archiver is receiving data.
- **Archiver writing rate:** Rate at which the Archiver is writing to disk.
- **Network traffic in:** Incoming network traffic bit rate on this computer.
- **Network traffic out:** Outgoing network traffic bit rate on this computer.

Advanced settings

The advanced settings are independent of the server hosting the role.

- **Digital signature:** Turn on this option to protect your video archive against tampering.
- **Delete oldest files when disks are full:** Turn on this option to recycle the archive storage (the default mode). The oldest files are deleted to make space for new files when all the disks within a disk group are full.
- **Enable edge playback requests:** Turn on this option only if the Archiver controls units that are configured for *edge recording*. By default, this option is turned off to prevent sending playback requests to units that are not recording.
- **Enable thumbnail requests:** Turn on this option to show video thumbnails for the Archiver (for example, in reports). This option must also be turned on to send snapshots using the *Email a snapshot* action.
- **Enable archive consolidation:** Turn this option on to duplicate video archives from the secondary or tertiary Archiver server on the primary Archiver server after an Archiver failover occurs. The primary Archiver server checks every hour for video archives that can be consolidated from the secondary or tertiary servers for the period it was offline.
- **Enable Telnet console:** Turn on this option to enable the Telnet debug console for this Archiver.
- **Protected video threshold:** This is a safety threshold that limits the amount of space that protected video files can occupy on disks. The percentage you set is the proportion of protected video that you can have of the total size of recorded videos on the disk. Protected video files are files that will not be deleted by normal archive cleanup procedures. If this threshold is exceeded, the Archiver generates the *Protected video threshold exceeded* event once every 15 minutes for as long as the condition is true, but will not delete any video file that is protected.
- **Disk load warning threshold:** The percentage of disk space that must be occupied before the *Disk load threshold exceeded* event is generated. The default value is 90%. The Archiver generates this event once every hour for as long as the condition is true. The disk load is calculated as follows:

  Disk load = Occupied disk space / (Total disk capacity - Min. free space)
- **Max archive transfer throughput:** The maximum bandwidth available for outbound data transfers from the archiving role. Applies to individual data transfers between Archivers and to Cloud Storage.

  NOTE: The same limit is applied to archive transfers and Cloud uploads.
- **Maximum simultaneous edge transfer cameras:** The maximum number of edge transfer cameras the role can handle at any given time.
- **Video files:** These two settings are used to control the size of the video files created by the Archiver:
  - **Maximum length:** Limits the length of video sequence contained in each file. The video length is the time span between the first video frame and the last video frame stored in a file. The default value is 20 minutes.
  - **Maximum size:** Limits the size of the video file. The default value is 500 MB. The Archiver starts saving the video to a new video file when either one of these conditions is met.
- **Monitor incoming events:** Use these settings to monitor and detect a high rate of incoming events from cameras connected to the Archiver. When the event rate is reached, a warning message identifies the problematic cameras and allows you to investigate and take action.
  - **Send notification for high event rate:** Turn on this option to enable the event monitor and define the event rate (enabled by default).
  - **Event threshold:** The number of events that must be received from all the cameras within the defined time period, to trigger the warning. The default value is 10,000.
  - **Time period:** The amount of time in which the event threshold must be reached to trigger the warning. The default value is 5 minutes.

  NOTE: Changing the time period in the event monitor resets the event counters for all the cameras to zero.
- **Additional settings:** These additional settings are reserved for use by our Technical Assistance personnel.

Related Topics

Creating databases on page 140
Deleting databases on page 141
Viewing database information on page 145
Receiving notifications when databases are almost full on page 146
Backing up databases on page 147
Restoring databases on page 151

Cloud Playback configuration tabs

You configure the settings of the Cloud Playback role from the **Roles** view of the *System* task in Security Center Config Tool.

Cloud Playback - Configuration tab

Click the **Configuration** tab to change the default settings for this role.

- **RTSP port:** Port used by the Cloud Playback role to listen for incoming Real Time Streaming Protocol (RTSP) requests.

  IMPORTANT: All RTSP ports on the same server must be unique. If Cloud Playback is hosted on the same server as another role listening for RTSP requests, including Archiver, Auxiliary Archiver, Media Gateway, Media Router, and redirector agents, ensure that each role listens on a different port.
- **Local UDP port range:** Ports used to stream live video from cloud-connected appliances and cameras to the Cloud Playback role. The number of ports in this range should align with the expected number of simultaneous streams. UDP ports 12001-12500 are used by default.

  IMPORTANT: Firewall configuration is not required for these ports because the video is streamed using Web Real-Time Communication (WebRTC). This port range must not be used elsewhere in Security Center, or by other applications.

Cloud Playback - Resources tab

Click the **Resources** tab to configure the server and failover servers assigned to this role. The Cloud Playback role does not require a database.

- **Servers:** Servers hosting this role.

Related Topics

Activating Cloud Storage on page 691

Directory Manager configuration tabs

You configure the settings of the Directory Manager role from the **Roles** view of the *System* task in Security Center Config Tool.

Directory Manager - Directory servers tab

In the **Directory servers** tab, you can configure the servers assigned to Directory *failover* and *load balancing*.

- **List of Directory servers (for failover and load balancing):** List of servers assigned to Directory failover and load balancing, called the *Directory failover list.* The server identified with a different icon (🖥) than the rest (🖥) is the *main server*. The main server is the only Directory server that can write to the Directory database. The rest can only read from that database.
- **Advanced (⚙):** Configure the server as a gateway or disaster recovery server.
- **Modify license for all servers:** Modify your Security Center license every time you make a change to the list of servers assigned to host the Directory role.

Directory Manager - Database failover tab

In the **Database failover** tab, you can configure the Directory database failover.

- **Use database failover:** Enable Directory database failover.
- **Failover mode:** Select which database failover mode to use.
- **Backup and restore:** The Directory Manager protects the Directory database by regularly backing up the master database instance (source copy). During a failover, the latest backups are restored to the backup database that’s next in line.
  - **LED (●):** Indicates the database server that is active.
  - **Server:** Security Center *server* hosting the database instance. The server that manages the master database instance is flagged as *(Master).*
  - **Database server:** Database server name. The name must be accessible from all computers. Relative names, such as (local)\SQLSEXPRESS cannot be used. Always explicitly write the server’s DNS name (for example TW-WIN7-SC-5) instead of (local).
  - **Database name:** Database instance name.
  - **State:** Database state. If there is a problem, an error message is displayed.
  - **Last Backup/Restore time:** Time of the last backup on the master database, or the last restore on the backup database.
  - **Folder:** Local folder on the specified server where the backup files are copied.
  - **Automatically reconnect to master database:** Select this option to force all Directory servers to reconnect to the master database after it is back online after a failover. This will cause a short service disruption, and all changes made to the system configuration while the master database was offline will be lost. Note that this option only works if the primary Directory server is online.
  - **Generate full backup every:** Specify how often (in days) a full backup is generated, and at and what time.
  - **Generate differential backup every:** Specify how often (in minutes) a differential backup should is generated. A differential backup contains the database transactions made after the previous backup (full or differential). The differential backups are deleted after the next full backup is made.

    NOTE: All backup activities are stopped when the active database is not the master database.
- **Mirroring:** Database failover is taken care of by Microsoft SQL Server and is transparent to Security Center. The *Principal* and *Mirror* instances of the Directory database are kept in sync at all times. There is no loss of data during failover.

  - **Database server:** Database server name. The name must be accessible from all computers. Relative names, such as (local)\SQLSEXPRESS cannot be used. Always explicitly write the server's DNS name (for example TW-WIN7-SC-5) instead of (local).
  - **Database name:** Database instance name.
- **SQL AlwaysOn:** Select this option if you are using the Windows feature *SQL AlwaysOn* as your Directory database failover solution.

Global Cardholder Synchronizer configuration tabs

You configure the settings of the Global Cardholder Synchronizer role from the **Roles and units** tab of the *Access control* task in Security Center Config Tool.

Global Cardholder Synchronizer - Properties tab

Click the **Properties** tab to configure the connection parameters to the *sharing host*, the *global partitions* you want to share, and how you want to synchronize.

- **Connection status:** Indicates the current connection status between the Global Cardholder Synchronizer (GSC) role and the sharing host. The second line shows the connection activities or when the last synchronization was performed.
- **Directory:** Name of the *Directory server* on the sharing host. If anything else than the default connection port (5500) is used, you must explicitly indicate the port number after the Directory name, separated by a colon. For example: HostServer:5888.
- **Username and password:** Credentials used by the GCS role to connect to the sharing host. The rights and privileges of this user determine what your local system is able to see and share with the host system.
- **Global partitions:** List of global partitions found on the sharing host. Select the ones you want to share.
- **Refresh:** Click this button to view the list of global partitions found on the sharing host.
- **Synchronize:** Click this button to receive the latest updates from the sharing host. You can also synchronize the local system on schedule by setting up a scheduled task.

Global Cardholder Synchronizer - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The GCS role does not require a database.

- **Servers:** Servers hosting this role. All must have access to the role database.

Health Monitor configuration tabs

You configure the settings of the Health Monitor role from the **Roles** view of the *System* task in Security Center Config Tool.

Health Monitor - Properties tab

Click the **Properties** tab to configure the health events to be monitored.

- **Client app. maintenance mode:** Turn this option on to set the client applications in maintenance mode.
- **Events to monitor:** Select which events you want the Health Monitor role to watch.

Health Monitor - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role. All must have access to the role database.
- **Database status:** Current status of the database.
- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.
- **Database:** Name of the database instance.
- **Actions:** You can perform the following functions on the role database:
  - **Create a database (➕):** Create a new database with the option to overwrite the existing one.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (🔔):** Set up notifications for when the database space is running low.
  - **Resolve conflicts (⚠):** Resolve conflicts caused by imported entities.
  - **Backup/Restore (▭):** Back up or restore the database.
- **Authentication:** Specifies which SQL Server authentication is to be used:
  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.

Related Topics

Creating databases on page 140
Deleting databases on page 141
Viewing database information on page 145

Receiving notifications when databases are almost full on page 146
Backing up databases on page 147
Restoring databases on page 151

Intrusion Manager configuration tabs

You configure the settings of the Intrusion Manager role from the *Intrusion detection* task in Security Center Config Tool.

Intrusion Manager - Properties tab

Click the **Properties** tab to configure the retention period of the intrusion events in the Intrusion Manager database.

- **Keep events:** Specify how long to keep the intrusion detection events that are logged by the Intrusion Manager in the database, before they are deleted.
- **Reconnection delay:** Specify how long the Intrusion Manager waits before trying to reconnect to a unit that went offline.

Intrusion Manager - Extensions tab

Click the **Extensions** tab to view the intrusion unit models controlled by this Intrusion Manager role.

All supported *extensions* are created by default when the role is created.

Intrusion Manager - Input definitions tab

Click the **Input definitions** tab to change the icons for input types. You can specify the type of an input from the *Peripherals* page of the intrusion detection unit. The default icons are as follows:

- Burglary (▣)
- Door (🚪)
- Fence (▥)
- Fire sensor (🔥)
- Gas (☠)
- Motion sensor ())))
- Panic (❗)
- Window (▦)

Intrusion Manager - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role. All must have access to the role database.
- **Database status:** Current status of the database.
- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.
- **Database:** Name of the database instance.
- **Actions:** You can perform the following functions on the role database:

  - **Create a database (➕):** Create a new database with the option to overwrite the existing one.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications ():** Set up notifications for when the database space is running low.
  - **Resolve conflicts (⚠):** Resolve conflicts caused by imported entities.
  - **Backup/Restore ():** Back up or restore the database.
- **Authentication:** Specifies which SQL Server authentication is to be used:
  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.

Related Topics

Creating databases on page 140
Deleting databases on page 141
Viewing database information on page 145
Receiving notifications when databases are almost full on page 146
Backing up databases on page 147
Restoring databases on page 151

Map Manager configuration tabs

You configure the settings of the Map Manager role from the **Roles** view of the *System* task in Security Center Config Tool.

Map Manager - Properties tab

Click the **Properties** tab to change the default settings for this role, and configure the external resources managed by this role, such as the map providers and the KML objects.

- **Map providers:** List of third-party map providers (*GIS*) that you are licensed to use. The list of map providers also serves as a geocoding priority list. This means that the map provider at the top of the list is the first to be tried as the geocoding provider. If this provider cannot return a result, the next provider in the list is tried.

  TIP: To see whether geocoding is enabled or not on a map provider, select the map provider and click **Edit the item** (✎).
- **Map layers:** List of imported KML objects that can be displayed on any georeferenced map. Each KML object corresponds to a distinct map layer that the Security Desk users can choose to show or hide.
- **Cache location:** The cache is a folder where the map tiles are stored. When you create maps from images files, the role generates a set of small images, called *map tiles*, for each zoom level at which you need to view the map. The larger the map scale, the more map tiles the role must generate. The default folder is *C:\ProgramData\Security Center\Maps*.
- **Port:** HTTP port used by the Map Manager to communicate with client applications. (Default=8012).
- **Default map:** The system default map, also known as the global default map, is the map initially loaded for all users when opening the *Maps* task. The global default map can be overridden both at the user group and user levels, where a default map can be configured for each user and group. You can only set the global default map after creating your first map.
- **Backward compatibility:** When switched **ON** after an upgrade, client applications from Security Center 5.8 and earlier can continue to download and show image maps.

  BEST PRACTICE: Switch **Backward compatibility OFF** after all client applications have been upgraded for enhanced security.

Map Manager - Record fusion tab

Click the **Record fusion** tab to select the maps and map object types you want to use in the *Records* investigation report.

- **Maps:** Maps that are used for location correlation. At least one map object type must be selected in the bottom list.
- **Use map locations for:** The selected object types are registered in the *Record Fusion Service* as record types and can be queried from the *Records* investigation task. All map objects registered as record types can be filtered on their *Location*, *Name*, *Description*, and *Entity* attributes. For more information, see "Investigating record types" in the *Security Center User Guide*.
- **Servers:** Servers hosting this role.

Map Manager - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Map Manager role does not require a database.

- **Servers:** Servers hosting this role.

Related Topics

Creating maps on page 301
Record Fusion Service configuration tabs on page 1381

Media Gateway configuration tabs

You can configure the Media Gateway role from the *Video* task in Security Center Config Tool.

Media Gateway - Properties tab

Click the **Properties**tab to enable the RTSP protocol on the Media Gateway and to configure the stream settings used by the Media Gateway to transcode video streamed to the Web Client or Genetec™ Web App.

- **RTSP:** RTSP protocol settings.
  - **Enable:** This option is turned off by default for security reasons. Turn it on to see the other settings.
  - **Start multicast address:** Start multicast address and port number for IPv4 and IPv6. In multicast, all video sources are streamed to different multicast addresses using the same port number, because multicast switches and routers use the destination IP address to make their routing decisions. Similarly, the Media Gateway assigns that same port number to all streaming cameras, starting with the specified IP address and incrementing the IP address by 1 for each new camera it encounters.
  - **Listening port:** Incoming TCP command port used by the Media Gateway.
  - **Require TLS (RTSPS):** This option is turned off by default because RTSPS is rarely supported. However, if your client application does support RTSPS, turn it on to heighten the security of your system.
  - **User authentication:** This option is turned on by default for security reasons. When the switch is on, only authorized users can connect to the Media Gateway. When the switch is off, anyone can connect to the Media Gateway without credentials.

    NOTE: The cameras that an RTSP client application can view in the system depend on the user account the client uses to log on to Security Center. If RTSPS is disabled, you must specifically add the users you allow to access this Media Gateway role to the **Accessible to** list. Assign to each user a different password than the one used for connecting to Security Center to minimize the risks of exposing their Security Center passwords. If RTSPS is enabled, the Media Gateway uses regular Security Center credentials to validate access. Moreover, the Security Center users must have the *Log on using the SDK* privilege.
- **HTTP:** HTTP ports and URL settings.
  - **Use the default web ports of the server:** By default, the Media Gateway communicates with the Mobile Server and Web Server roles over HTTPS port 443 and HTTP port 80. These ports are defined on the servers that host the Mobile Server and the Web Server roles respectively. If your IT policy requires different ports, or there is some sort of conflict, you can change the ports. Turn off the option to use the default ports, then change the HTTP port and secure HTTP port settings.
    IMPORTANT: If you have an unsigned (invalid) SSL certificate and end-users monitor video in the Web Client using Mozilla Firefox or Microsoft Edge browsers, ensure that the ports set on the Media Gateway match the ports on the web server.
  - **Web address:** Define the suffix of the URL used by the Mobile Server and Web Server roles to connect to the Media Gateway. The format of the URL is *https://host:port/web address*, where *host* is the IP address or host name of the server that hosts the Media Gateway role, *port* is the HTTP port or the HTTPS port, and *web address* is media by default.
- **Video streaming:** Video settings for streaming video over HTTP. Only the Web Client use these settings. For streaming to mobile devices, the Media Gateway follows the settings configured for the Mobile Server role.
  - **Default live stream:** The default stream used for streaming live video. It is either one of the five standard streams: *Live*, *Recording*, *Remote*, *Low resolution*, *High resolution*, or it is *Automatic*.

With the *Automatic* option, the Media Gateway decides between the *Low resolution*, the *Live*, or the *High resolution* stream, based on the resolution of the viewing tile in the browser. The following thresholds help the Media Gateway make that decision.

  - **Low resolution to Live:** Resolution at which the Media Gateway decides to use the *Live* stream. Below this resolution, the Media Gateway uses the *Low resolution* stream.
  - **Live to High resolution:** Resolution at which the Media Gateway decides to use the *High resolution* stream.

- **Allow transcoding:** Controls whether the Media Gateway should be allowed to transcode and in what situation. Transcoding is very CPU intensive and requires high-end servers.
  - **Never:** The Media Gateway never transcodes. If the client device cannot decode the stream, the error "Unsupported codec" is displayed.
  - **Only for PTZ control and Mobile Server:** The Mobile Server role can request transcoded streams at any time. Other applications can only use transcoding to reduce video latency while the user is controlling a PTZ, otherwise an error message is displayed.
  - **Always (for unsupported devices and codecs):** The Media Gateway transcodes when:
    - The client application requests it.
    - PTZ camera is being moved (to reduce latency).
    - The codec used by the camera is not supported by the client application.
- **Maximum resolution for MJPEG transcoding:** When transcoding, downscale the resulting transcoded stream to this resolution. Stream that are not transcoded are untouched.
- **Frame rate:** Maximum frame rate of the resulting transcoded stream.

Media Gateway - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Media Gateway role does not require a database.

- **Servers:** Servers hosting this role.

Media Router configuration tabs

You configure the settings of the Media Router role from the *Video* task in Security Center Config Tool.

Media Router - Properties tab

Click the **Properties** tab to configure the stream redirectors, the start multicast endpoint, and the RTSP port for the Media Router.

- **Redirectors:** Servers assigned to host *redirector agents*, which is a software module launched by the Media Router to redirect data streams from one IP endpoint to another.
  - **Server:** Server selected to host the redirector agent.
  - **Incoming UDP port range:** Range of ports used by the redirector agent to send video using *UDP*. If the redirector agent is running behind a firewall, ensure that these ports are unlocked for inbound packets for UDP connections.
  - **Live capacity:** Limit the maximum number of live streams that can be redirected through this server (redirector). This feature prevents overloading the server with too many users who are simultaneously trying to view video that needs redirection. When the limit is reached, an error message is displayed on the client application when users request live video, stating that the live stream capacity is exceeded.
  - **Playback capacity:** Limit the maximum number of playback streams that can be redirected through this server (redirector). This feature prevents overloading the server with too many users who are simultaneously trying to view video that needs redirection. When the limit is reached, an error message is displayed on the client application when users request playback video, stating that the playback stream capacity is exceeded.
  - **Bandwidth control:** Limit the maximum bandwidth for video streams that are redirected through this server (redirector). You can also set a different bandwidth limit for live and playback video. This feature prevents overloading the network with too many video streams coming from a remote site that has limited bandwidth.
    When the limit is reached and users request a new video stream, an error message displays stating that the bandwidth limit is exceeded. If the bandwidth limit is reached and a user with a high *user level* requests a stream, the user with the lowest user level who is viewing video that is being redirected from that redirector loses their stream connection. If multiple users with the same user level are viewing redirected video streams, the user who requested the video stream last loses the stream connection.
  - **Redirection strategy:** If you have multiple network cards, you can specify the actions performed by each network card. For example, you might want to specify that video export and video transfer can only be performed by your Wireless network card. For more information, see Configuring network card usage for a redirector on page 599.
    NOTE: By default, all actions are performed on the connected network card with the highest priority.
  - **Multicast interface:** Network adaptor to use for streaming data in multicast mode.
  - **RTSP port:** Port used by the redirector agent to receive TCP commands.
    NOTE: If you configure the redirector agent on the server hosting the Media Router, the RTSP port cannot be the same as the one used by the Media Router.
  - **RTP port:** Port used by the redirector agent to stream live video data using TCP.
- **RTSP port:** Incoming TCP command port used by the Media Router.
- **Secure communication:** Encrypts all RTSP video requests. When secure communication is enabled, all video communications use RTSP over TLS, but only the RTSP control channel is encrypted for live video streaming. To encrypt the video data channel, set the camera encryption to *In transit from Archiver* or *In transit and at rest*. Video playback and video export always use RTSP over TCP, therefore the RTSP control channel and the video data channel are both encrypted.

IMPORTANT: Secure communication is enabled by default on new installations, but disabled if you upgraded from version 5.5 or earlier. When secure communication is turned on, Security Center systems older than 5.5 cannot federate your Security Center system.

- **Multicast:** In multicast, all audio and video sources are streamed to different multicast addresses while using the same port number, because multicast switches and routers use the destination IP address to make their routing decisions. Similarly, in its default configuration, the Media Router assigns that same port number to all streaming devices (microphones and cameras), starting with the specified IP address, and adding 1 for every new device it encounters.

  The multicast IP address ranges are configured separately for **Local streams** and **Federated streams** for optimization. Each range of multicast IP addresses is defined by a **Start address** and a specific port number.
- **Increment ports:** This option is turned off by default to avoid having to open too many ports on systems with low multicast traffic.

  If you have a large number of cameras streaming in multicast, turn this option on to let the Media Router increment the port number by 2 for every multicast address. This strategy is used to overcome a known Windows limitation that puts a cap on the bandwidth of a single port at around 100 Mbps. When the maximum value (65535) is reached, the port number restarts from the value that you configured.

Media Router - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role. All must have access to the role database.
- **Database status:** Current status of the database.
- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.
- **Database:** Name of the database instance.
- **Actions:** You can perform the following functions on the role database:
  - **Create a database (➕):** Create a new database with the option to overwrite the existing one.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (🔔):** Set up notifications for when the database space is running low.
  - **Resolve conflicts (⚠):** Resolve conflicts caused by imported entities.
  - **Backup/Restore (▭):** Back up or restore the database.
- **Authentication:** Specifies which SQL Server authentication is to be used:
  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.

Related Topics

Creating databases on page 140
Deleting databases on page 141
Viewing database information on page 145
Receiving notifications when databases are almost full on page 146
Backing up databases on page 147
Restoring databases on page 151
About the Media Router role on page 596

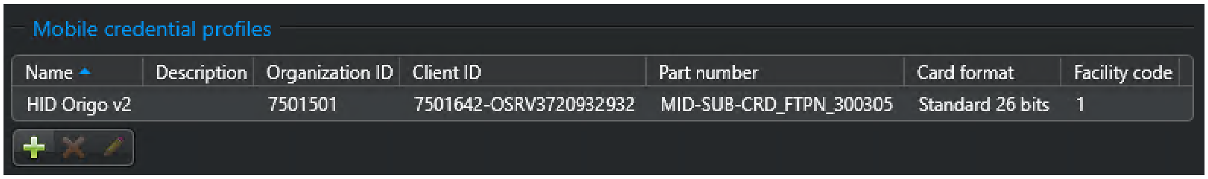
Mobile Credential Manager configuration tabs

You configure the settings of the Mobile Credential Manager role from the **Roles** view of *System* task in Security Center Config Tool.

Mobile Credential Manager - Configuration tab

Click the **Configuration** tab to configure the general settings of the Mobile Credential Manager, and create and configure mobile credential profiles.

- **General settings:**
    - **Quick mobile credential refresh interval (minutes):** How often the information for credentials that were recently updated in Security Center is polled from the provider to be displayed in Security Center.
    - **Normal mobile credential refresh interval (minutes):** How often the information for credentials that were not recently updated in Security Center is polled from the mobile credential provider to be displayed in Security Center.
    - **Automatically revoke mobile credential on deletion:** Turn this option on if you want mobile credentials to be revoked on the mobile credential provider side when you delete them from Security Center.
- **Mobile credential profiles:** Lists the mobile credential profiles you configured. You can use the buttons to add, delete, or modify them.



Mobile credential profiles

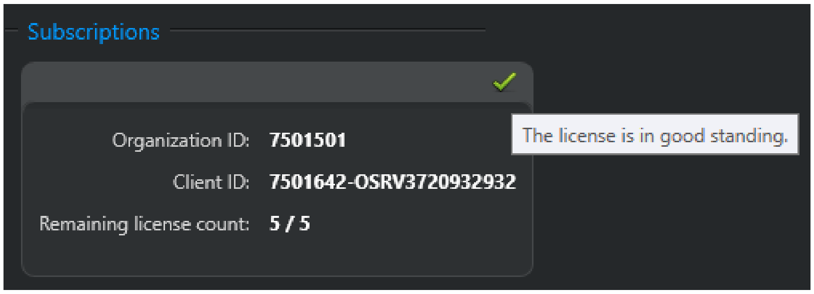
Name	Description	Organization ID	Client ID	Part number	Card format	Facility code
HID Origo v2		7501501	7501642-OSRV3720932932	MID-SUB-CRD_FTPN_300305	Standard 26 bits	1

Mobile Credential Manager - Credentials tab

Click the **Credentials** tab to view the status of your mobile credential subscriptions and configure the mobile credentials in your system.

- **Subscriptions:** Displays the **Organization ID**, **Client ID**, and **Remaining license count** for each mobile credential subscription. A mobile credential is removed from the license count when an invitation is sent.

  NOTE: An icon at the top of each subscription indicates the status of the subscription.



Subscriptions

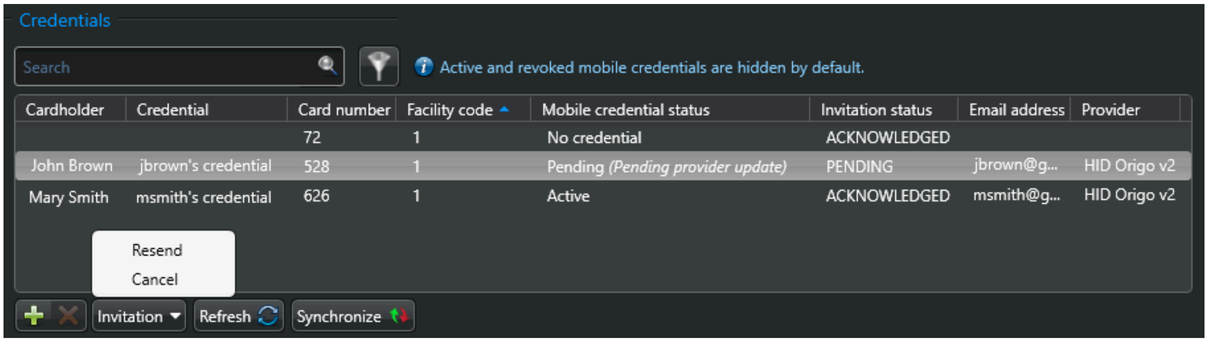
Organization ID: 7501501

Client ID: 7501642-OSRV3720932932

Remaining license count: 5 / 5

The license is in good standing.

- **Credentials:** Lists the following information about each mobile credential in your system. You can use the search box or click 🔽 to filter the list.



Credentials

Search

Active and revoked mobile credentials are hidden by default.

Cardholder	Credential	Card number	Facility code	Mobile credential status	Invitation status	Email address	Provider
		72	1	No credential	ACKNOWLEDGED		
John Brown	jbrown's credential	528	1	Pending *(Pending provider update)*	PENDING	jbrown@g...	HID Origo v2
Mary Smith	msmith's credential	626	1	Active	ACKNOWLEDGED	msmith@g...	HID Origo v2

- **Cardholder:** The cardholder to which the mobile credential is assigned.
- **Credential:** The name of the mobile credential.
- **Card number:** The card number assigned to the mobile credential by the mobile credential provider.
- **Facility code:** The facility code of the mobile credential.
- **Mobile credential status:** The status of the mobile credential.
- **Invitation status:** The status of the invitation from the mobile credential provider.
- **Email address:** The email address of the cardholder to which the mobile credential is assigned.
- **Provider:** The mobile credential provider.

You can use the buttons at the bottom of the credentials list to do the following:

- **Add an item (➕):** Create a mobile credential.
- **Remove the item (✖):** Delete a mobile credential from Security Center.

  NOTE: The mobile credential is also revoked if the **Automatically revoke mobile credential on deletion** option is on.
- **Invitation:** Resend or cancel an email invitation from the mobile credential provider to the cardholder.
- **Refresh (⟳):** Refresh the credential list to display the latest information available to the Mobile Credential Manager role.
- **Synchronize (⇅):** Get the latest credential information from the mobile credential providers.

Mobile Credential Manager - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role. All must have access to the role database.
- **Database status:** Current status of the database.
- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.
- **Database:** Name of the database instance.
- **Actions:** You can perform the following functions on the role database:
  - **Create a database (➕):** Create a new database with the option to overwrite the existing one.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (🔔):** Set up notifications for when the database space is running low.
  - **Backup/Restore (▭):** Back up or restore the database.
- **Authentication:** Specifies which SQL Server authentication is to be used:

  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.

Mobile Server configuration tabs

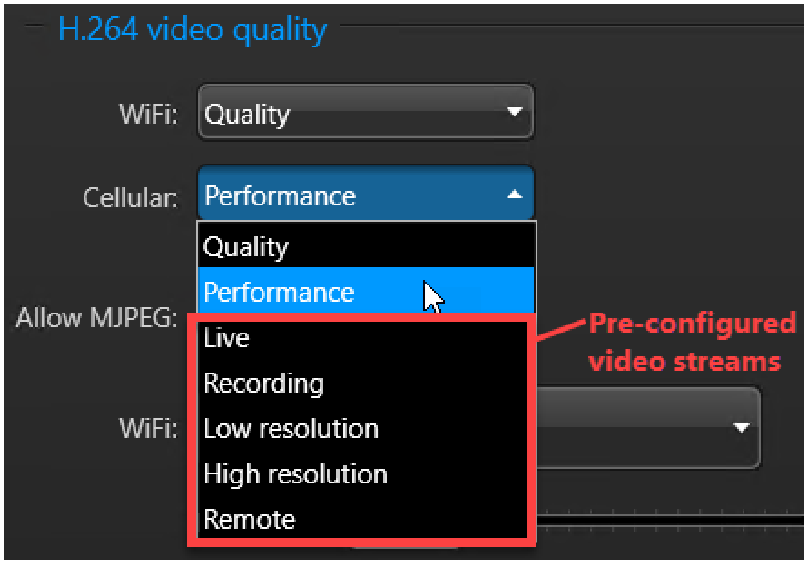
You configure the Mobile Server from the **Roles** view of *System* task in Security Center Config Tool.

Mobile Server - Properties tab

Click the **Properties** tab to configure the common Genetec™ Mobile behaviors and select the Security Center Mobile features you want to enable.

- **Web address:** Define the suffix of the URL used by Genetec Mobile to connect to the Mobile Server. The format of the URL is *host:port/web address*, where *host* is the IP address or hostname of the server hosting the Mobile Server role, *port* is HTTPS port 443 by default, and *web address* is Mobile by default. Each Mobile Server role must have a unique URL. If two roles are hosted on the same server, they must have different web addresses or use different ports.
- **Use the default secure HTTP port of the server:** By default, the Mobile Server communicates with the mobile devices over HTTPS port 443. If your IT policy requires a different port, or there is some sort of conflict, you can change this port. Turn off this option and then change the port number.
- **Maximum inbox messages per user:** Define the maximum number of messages that Genetec Mobile keeps in its inbox. If a new message is received while the inbox is full, the oldest message is deleted.
- **Session timeout:** Define the maximum period of inactivity, meaning the app is in the background, before the Mobile Server automatically logs the user off.
- **Maximum number of client sessions:** Set a limit to the number of Genetec Mobile connections that this role can handle to avoid overloading the server. The default is no limit.
- **Features:** Select the features that you want to enable in Genetec Mobile on devices connected to this Mobile Server.
  - **Alarms:** Allow Genetec Mobile users to monitor and acknowledge alarms.
  - **Device camera streaming:** Allow Genetec Mobile to enroll mobile device cameras in Security Center. Click ⚙ to configure the settings.
    - **Maximum sequence length:** Maximum duration of the streamed video. After the duration elapses, the streaming automatically stops to prevent battery drain.
    - **Port start and end index:** Port range used for mobile device cameras.
    - **Archiver:** Archiver role responsible to manage the device cameras.
    - **Location:** Area entity where the device cameras are grouped under.
  - **License plate management:** (Genetec Mobile 5.1.0 and later) Allow mobile users to view live ALPR events (reads and hits), to add license plates to hotlists, and to generate reports on reads and hits.
  - **Maps:** Allow Genetec Mobile to display Security Center entities and live events on maps.
  - **Push notifications:** Allow Genetec Mobile to receive push notifications from the Mobile Server.
  - **Threat levels:** Allow the Genetec Mobile user to display and set threat levels.
  - **Tracking:** Allow Genetec Mobile to share its device location with other users on the system so that its user can be displayed on georeferenced maps, in Security Desk, and other instances of Genetec Mobile.
  - **Video:** Allow Genetec Mobile to display video from Security Center. Click ⚙ to configure the settings.
    - **Maximum number of video streams:** Set a limit to the number of video streams that this role can handle to avoid overloading the server. The default is no limit.
    - **Limit Media Gateway role usage:** Turn on this option to assign Media Gateway roles to this Mobile Server and limit the use of the Media Gateway roles to the selected servers to accommodate your network limitations. Only the servers assigned to the selected Media Gateway roles are listed.
    - **H.264 video quality:** For cameras that support H.264 streams, choose the video stream to use when the Genetec mobile app connects over Wi-Fi and cellular networks. You can choose:

- A preconfigured stream usage: **Live**, **Recording**, **Low resolution**, **High resolution**, or **Remote**. For more info, see Configuring video streams of cameras on page 616.
- **Quality** so that the system uses the preconfigured stream usage that has the highest resolution and frame rate.
- **Performance** so that the system uses the preconfigured stream usage that requires the least amount of bandwidth.



- **Allow MJPEG:** Enable or disable MJPEG streams. When enabled, if the camera requested by Genetec Mobile does not support H.264, then video is sent in MJPEG format.
  Choose the maximum resolution and frame rate to use when sending MJPEG video over Wi-Fi and cellular networks. The mobile user can override these settings in Genetec Mobile.
  When a mobile user requests to view a camera, the Mobile Server gets all the streams configured for that camera and selects the one closest to the maximum settings. If a stream is found with a resolution close to that, the Media Gateway sends that stream to the Mobile Server which then sends it to the mobile device. If no stream is found close to the resolution, the Media Gateway must transcode the stream to get the desired resolution.
  IMPORTANT: The transcoding process is very CPU intensive and should be avoided. For every camera susceptible to be viewed by mobile users, always ensure that you have one stream configured that is close to the maximum settings configured in the Mobile Server. Alternatively, you can turn off the **MJPEG** option to avoid any possibility of transcoding.

- **Advanced settings:** These advanced settings are reserved for use by our Technical Assistance personnel.

Mobile Server - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role. All must have access to the role database.
- **Database status:** Current status of the database.
- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.
- **Database:** Name of the database instance.
- **Actions:** You can perform the following functions on the role database:

  - **Create a database (✚):** Create a new database with the option to overwrite the existing one.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications ():** Set up notifications for when the database space is running low.
  - **Resolve conflicts ():** Resolve conflicts caused by imported entities.
  - **Backup/Restore ():** Back up or restore the database.
- **Authentication:** Specifies which SQL Server authentication is to be used:
  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.

Related Topics

Creating databases on page 140
Deleting databases on page 141
Viewing database information on page 145
Receiving notifications when databases are almost full on page 146
Backing up databases on page 147
Restoring databases on page 151

Omnicast Federation configuration tabs

You configure the settings of the Omnicast™ Federation™ role from the **Roles** view of the *System* task in Security Center Config Tool.

NOTE: In Security Center 5.11.3.0 and later, Omnicast Federation is not supported and the role is in a permanent warning state.

Omnicast Federation - Identity tab

Click the **Identity** tab to view descriptive information about this role and jump to the configuration page of related entities.

- **Role group:** An advanced setting that is only necessary if you plan on hosting more than 40 Omnicast Federation roles on the same server.

  NOTE: This setting is hidden by default. To show it, click the **Name** field, and type Ctrl+Shift+A.

Omnicast Federation - Properties tab

Click the **Properties** tab to configure the connection parameters to the remote Omnicast system, and the default video stream and events you want to receive from it.

- **Connection status:** Shows the connection status of the Federation role to the remote Omnicast system. Click **Reset** to force the Federation™ role to reconnect to the remote system.
- **Directory:** Name of the Omnicast Gateway connecting you to the remote Omnicast system.
- **Version:** Version of the federated Omnicast system. This list only contains Omnicast versions that you have installed a compatibility pack for.
- **Username and password:** Credentials used by the Federation role to log on to the remote Omnicast system. The rights and privileges of that user determine what your local users can see and do on the federated remote system.
- **Default live stream:** Default video stream used for viewing live video from federated Omnicast cameras (default=**Remote**).

  If your workstation does not require specific video stream settings for Federation™, you can use the default stream settings from Security Desk instead.
- **Enable playback requests:** When this option is turned on, users can view playback video from federated Omnicast cameras.
- **Federate alarms:** When this option is turned on, alarms are received from the federated Omnicast system.
- **Federated events:** Select the events that you want to receive from the federated Omnicast system. Events are necessary if you plan to monitor the federated entities in Security Desk, or to configure event-to-actions for the federated entities.

Omnicast Federation - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Omnicast Federation™ role does not require a database.

- **Servers:** Servers hosting this role.

Record Caching Service configuration tabs

You can configure the settings of the Record Caching Service role from the **Roles** view of the *System* task in Security Center Config Tool.

Record Caching Service - Properties tab

Click the **Properties** tab to view the configuration of your *record type*. What you see on this page are the standard properties of the selected record type in the left pane.

- **Name:** Name of the record type.
- **Icon:** Icon or string expression representing this record type. By default, the first letter of the record type name is used.
- **Status:** Record type status, followed by the number fields and the current number of records.

  Click the number of fields to view the list of fields with their name and data type. The icon in front of certain fields indicates the function assigned to that field, which can be one of the following: *ID*, *Timestamp*, *Latitude*, *Longitude*, or *Location*.

  Click **Import data** to import new data from a flat file.
- **Raise event when record cached:** When enabled, the system raises the *Record updated* event every time a record from this record type is ingested.
- **Associate events to an entity:** Map that displays *Record updated* events when data is ingested. For this to work, the map must show at least one area entity represented as a polygon. The area is used for geofencing.
- **Display on map as:** Indicates whether or not to display the records from this record type on maps, either as events or as a query results. You can choose to display the records as a pin or a polygon. The *Pin preview* shows you how a record is represented on a map.

The *Record presentation* section describes how the information is presented when a record is displayed in a tile in the Genetec™ Mobile app, or in the information bubble when you click a record on a map. The *Preview* window shows you how the information looks in an information bubble.

- **Title:** Title of the data record, displayed in a larger font.
- **Description:** Description of the data record, displayed in a smaller font.
- **Displayed items:** List of items displayed in the information bubble.
  - **Item:** Either a field name or a custom expression that transforms or combines multiple fields.
  - **Name:** Label for the item.
  - **Rendered as:** Display format of the item.

  You can click ➕ to add more items or click ✖ to remove a selected item from the list.

Record Caching Service - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role. All must have access to the role database.
- **Database status:** Current status of the database.
- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.
- **Database:** Name of the database instance.
- **Actions:** You can perform the following functions on the role database:

  - **Create a database (➕):** Create a new database with the option to overwrite the existing one.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications ():** Set up notifications for when the database space is running low.
  - **Backup/Restore ():** Back up or restore the database.
  - **Cleanup ():** Configure a different retention period for each record type managed by this role.
- **Authentication:** Specifies which SQL Server authentication is to be used:
  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.

Related Topics

Creating databases on page 140
Deleting databases on page 141
Viewing database information on page 145
Receiving notifications when databases are almost full on page 146
Backing up databases on page 147
Restoring databases on page 151
Record Fusion Service configuration tabs on page 1381
Creating record types on page 258
Importing external data from flat files on page 265

Record Fusion Service configuration tabs

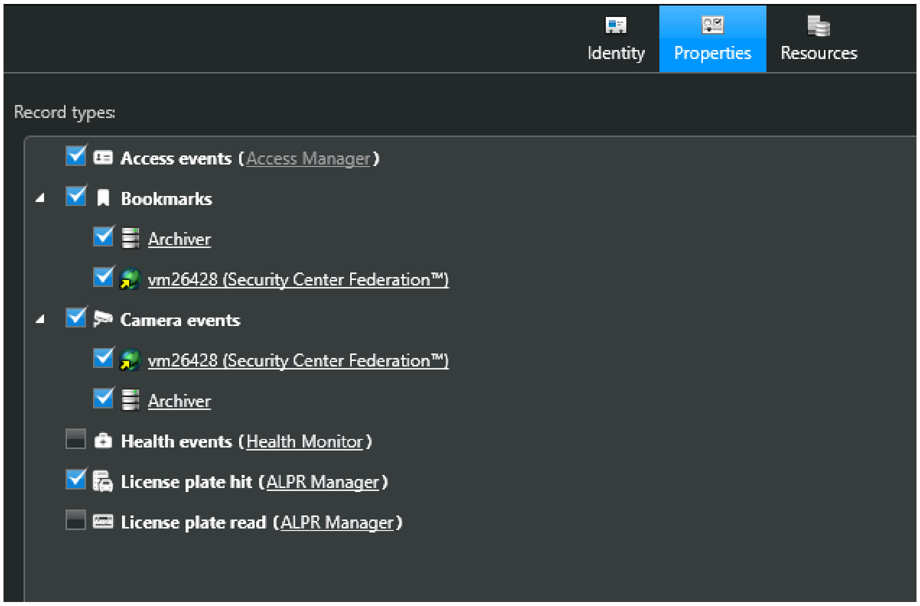
You configure the settings of the Record Fusion Service role from the **Roles** view of the *System* task in Security Center Config Tool.

Record Fusion Service - Properties tab

Click the **Properties** tab to view the list of *record types* registered in your system, and to select which sources to query when using the *Records* investigation task.

- **Name:** Name of the registered record type.
- **Source:** Name of the role that is queried for the record type.

NOTE: The source is listed after the name of the record type. If the record type has multiple sources, you can expand the record type in a tree view to select or deselect each source. The **License plate read** and **Health events** report types are deselected by default.



Record types:

- ☑ **Access events** (Access Manager)
- ☑ **Bookmarks**
  - ☑ Archiver
  - ☑ vm26428 (Security Center Federation™)
- ☑ **Camera events**
  - ☑ vm26428 (Security Center Federation™)
  - ☑ Archiver
- ☐ **Health events** (Health Monitor)
- ☑ **License plate hit** (ALPR Manager)
- ☐ **License plate read** (ALPR Manager)

Record Fusion Service - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Record Fusion Service does not require a database.

- **Servers:** Servers hosting this role.

Report Manager configuration tabs

You configure the settings of the Report Manager role from the **Roles** view of the *System* task in Security Center Config Tool.

Report Manager - Properties tab

Click the **Properties** tab to configure the default behavior of this role.

- **Maximum number of results for batch reports:** Sets the maximum number of results that can be returned by the *Email a report* or *Export report* actions.
- **Destination folder:** The destination folder for the reports that are saved using the *Export report* action. You can select a local drive or a network drive.
- **User profile for securing emails:** When selected, the access rights and privileges of the selected user profile are applied to emails sent to cardholders and external recipients. This is required because cardholders and external recipients do not have existing access rights in Security Center.

  NOTE: If a camera is blocked at a specific level, the user access level is applied to the *Email a snapshot* action.

Report Manager - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Report Manager role does not require a database.

- **Servers:** Servers hosting this role.

Security Center Federation configuration tabs

You can configure the settings of the Security Center Federation™ role from the *System* task in Security Center Config Tool.

Security Center Federation - Identity tab

Click the **Identity** tab to view descriptive information about this role and jump to the configuration page of related entities in addition to the general options.

- **Role group:** An advanced setting that is only necessary if you plan on hosting more than 100 Security Center Federation™ roles on the same server.

  NOTE: This setting is hidden by default. To show it, click the **Name** field, and type Ctrl+Shift+A.

Security Center Federation - Properties tab

Click the **Properties** tab to configure the connection parameters to the remote Security Center system, the default synchronization behavior, and the default video stream and events you want to receive from it.

- **Connection status:** Shows the connection status of the Federation™ role to the remote Security Center system.
- **State:** Shows the current state of the Federation™ role.
- **Allow untrusted connections:** (Stratocast system only) Allow connections to Security Center servers using legacy authentication.
- **Directory:** Name of the main server for the remote Security Center system.
- **Username and password:** Credentials used by the Federation™ role to log on to the remote Security Center system. The rights and privileges of that user determine what your local users can see and do on the federated remote system.
- **Resilient connection:** When this option is turned on (default=OFF), the Federation™ role attempts to reconnect to the federated Security Center Directory server after a connection interruption. After a specified period of attempting to reconnect, the connection is considered lost and the role goes into a warning state.

  NOTE: Activating Resilient connection is highly recommended for remote systems that might have an unstable connection to the cloud.
- **Reconnection timeout:** Specify the number of seconds that the Federation™ role attempts to reconnect to the Directory before the connection is considered lost.
- **Forward Directory reports:** When this option is turned on (default=OFF), you can view user activities (viewing cameras, activating the PTZ, and so on) and configuration changes performed at the federated site from the *Activity trails* and *Audit trails* reports on the Federation™ host, as long as the Federation™ user has the privileges and access rights to view them. You can also view the federated units in the *Hardware inventory* task.

  IMPORTANT: Forward Directory reports is only supported with 5.8 systems and higher (including federations). This means that if your federated system is 5.7 and lower, the Forward Directory reports option is grayed out and not available.
- **Default live stream:** Default video stream used for viewing live video from federated Security Center cameras (default=**Remote**).

  If your workstation does not require specific video stream settings for Federation™, you can use the default stream settings from Security Desk instead.
- **Enable playback requests:** When this option is turned on, users can view playback video from federated Security Center cameras.

- **Federate alarms:** When this option is turned on, alarms are received from the federated Security Center system.
- **Federate custom icons:** When this option is turned on, federated entities share custom icons with the Federation™ host. This means that entity icons in the Federation™ host appear identical to the federated system. It can take a few minutes to synchronize the custom icons.
- **Federated events:** Select the events that you want to receive from the federated Security Center system. Events are necessary if you plan to monitor the federated entities in Security Desk, or to configure event-to-actions for the federated entities.

Security Center Federation - Resources tab

Click the **Resources** tab to configure the servers assigned to this role.The Security Center Federation™ role does not require a database.

- **Servers:** Servers hosting this role.

Unit Assistant - Properties tab

Click the **Properties** tab to enable or configure the different features supported by the Unit Assistant role. It can also be used to configure advanced settings.

Diagnostic settings

- **Traceroute:** Enable this setting to monitor cameras and produce diagnostic information when there is a camera connection issue with the Archiver role. The results of the diagnostics are recorded in the *Camera events* task. Traceroute runs on each Archiver role when enabled and it can consume a small amount of resources. Make sure to validate the Archiver resources after enabling the feature.
  - **Hop timeout:** Specify the timeout, in seconds, for traceroute connection hops. The default value is 10 seconds. Increase the value if there are too many timeout errors in the report.
  - **Maximum concurrency:** Specify the maximum number of simultaneous traceroute executions allowed per Archiver role. The default value is 30.
  - **Maximum number of timed out hops:** The maximum number of hops that can time out before the execution is canceled. The default value is 3.
  - **Retention period:** Specify, in days, how long to keep traceroute entries. The default value is 30 days.

Security settings

NOTE: This section is only visible if the Certificate Signing plugin is installed on your system.

- **Security policies:**
  - **Allow renewal of expired certificates:** Turn on this setting (on by default) to allow the system to renew unit certificates automatically, even after they are expired. If you do not want expired certificates to be automatically renewed, turn off this setting. You can always manually renew expired certificates from the *Hardware inventory* task.
  - **Enable HTTPS on units after successful certificate installation:** Turn on this setting (on by default) to force the unit to switch to HTTPS after the certificate is successfully installed. The HTTPS ports configured in Security Center for the units might change during the process if the Unit Assistant can detect the correct port.
- **Notifications:** Specify, in days, how soon you want the system to trigger a warning before a certificate expires (default = 7 days).

  If you configured your system to automatically renew certificates X days before they expire, set this value to X minus N, where N is the number of days you give the system to try to automatically renew a certificate before issuing a warning. Also be sure to give yourself enough time to investigate why a certificate was not renewed after you received the warning.
- **Certificate information:**
  - **Validity period:** This is the validity period of a certificate after a renewal. This value is inherited from the CA. It can only be modified from the *Certificate profile* page.
  - **Show advanced:** Click this button to show the optional properties that you can assign to certificates created by your system. The *Country*, *State*, *Locality*, *Organization*, and *Organizational unit* help you identify certificates issued for your organization. These values can be overwritten on specific certificate renewals.
- **Public key infrastructure:** The Unit Assistant role must rely on a trusted *certificate authority (CA)* to sign the certificates it deploys. The **Endpoint** is the URL of the CA that the Unit Assistant role must connect to.

NOTE: For Security Center 5.11, the CA is the Certificate Signing role.

The syntax of the URL is as follows:

```
https://hostname:port/management
```

where *hostname* is the hostname or IP address of the server hosting the Certificate Signing role, and *port* is the port number configured in the *Properties* page of the Certificate Signing role. Make sure the server hosting the Unit Assistant role can access this URL.

IMPORTANT: To simplify the failover configuration, the URL is set by default to https://localhost:*port*/management. This assumes that both the Unit Assistant role and the Certificate Signing role are always hosted on the same server. If you choose to host the two roles on separate servers, then when a failover occurs, you must manually change the value of the URL here and restart the Unit Assistant role.

- **Advanced settings:** The advanced settings are reserved for use by Genetec Technical Assistance Center.

Unit Assistant - Certificate profile tab

Click the **Certificate profile** tab to configure the policies and the limits imposed on certificate requests applied by the CA.

NOTE: This tab is only visible if the Certificate Signing plugin is installed on your system.

- **Allowed domain name:** Must match your network domain name. Leave it blank if you do not want to include the domain name in the certificates.
- **Allowed IPv4 range:** Enter the IPv4 range of the units you expect to connect to on your network. Leave it blank if you do not want the units to use IPv4.

  The IP range must follow the CIDR convention. All units must be found within this range of IP addresses. We do not support discrete ranges of IP addresses.
- **Allowed IPv6 range:** Enter the IPv6 range of the units you expect to connect to on your network. Leave it blank if you do not want the units to use IPv6.

  The IP range must follow the CIDR convention. All units must be found within this range of IP addresses. We do not support discrete ranges of IP addresses.
- **Validity period:** Specify, in days or months, the validity period of the renewed certificates according to your security policies. We recommend a period between six months and one year.

Unit Assistant - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role. All must have access to the role database.
- **Database status:** Current status of the database.
- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.
- **Database:** Name of the database instance.
- **Actions:** You can perform the following functions on the role database:
  - **Create a database (✚):** Create a new database with the option to overwrite the existing one.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (●):** Set up notifications for when the database space is running low.
  - **Backup/Restore (▭):** Back up or restore the database.
- **Authentication:** Specifies which SQL Server authentication is to be used:
  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.

Related Topics

Creating databases on page 140

Deleting databases on page 141

Viewing database information on page 145

Receiving notifications when databases are almost full on page 146

Backing up databases on page 147

Restoring databases on page 151

Web-based SDK configuration tabs

You configure the settings of the Web-based SDK role from the **Roles** view of the *System* task in Security Center Config Tool.

Web-based SDK - Properties tab

Click the **Properties** tab to configure what the external developers need to know to use the web services.

- **Port + Base URI:** These two parameters are used to determine the address of the web service.

  For example, with Port=4590 and Base URI=WebSdk, the web service address would be “http://<computer>:4590/WebSdk/”, where <computer> is the DNS name or public IP address of the server hosting the Web-based SDK role.
- **Streaming port:** Port used to stream the events. You can configure which events to listen to.
- **Use SSL connection:** Turn this option on (default=off) to use *SSL* encryption for communications with the web service. If you are using SSL encryption, the web service address uses *https* instead of *http*.
- **SSL settings:** Settings required when you are using SSL encryption.
  - **Certificate:** Name of the certificate to use. Use the form: “CN=NameOfTheCertificate”. The certificate must be registered in Windows. You can find procedures on the web on how to do just that.
  - **Bind certificate to port:** Turn this option on (default=off) to bind the certificate to the port. This operation does the same thing as you would normally do under Windows.

Web-based SDK - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Web-based SDK role does not require a database.

- **Servers:** Servers hosting this role.

Web Server configuration tabs

You configure the Web Server from the **Roles** view of *System* task in Security Center Config Tool.

Genetec™ Web App Web Server - Properties tab

Click the **Properties** tab to configure application path, the URL, load balancing settings, port settings, and enabled features for the Genetec Web App.

- **Application path:** Define the *web address* URL segment to create the base address of your web application.
- **URL:** Identify the suffix of the URL that users enter on their browser to connect to the Genetec Web App. The format of the URL for the Genetec Web App is *https://host:port/web address*, where *host* is the IP address or host name of the server that hosts the Web Server role, *port* is HTTP port 80 (default) or HTTPS port 443 (default), and *web address* is WebApp by default. The URL of each connection must be unique.
- **Enable load balancing:** If multiple resources under the Genetec Web App role exist on your system, you can enable the load balancing feature. When enabled, the web application is made aware of all existing Genetec Web App roles and specifies which one should service that session based on the load of each role.
- **Use the default web ports of the server:** By default, the Genetec Web App communicates over HTTPS port 443 and HTTP port 80. These ports are defined on the server that hosts the Web Server role. If your IT policy requires different ports, or there is some sort of conflict, you can change the ports used by the Genetec Web App. To change the default ports, set this option to **OFF** and change the HTTP port and secure HTTP port.
- **Features:** Select the Security Center features you want to access on the Genetec Web App. If your system has multiple Media Gateway roles, click the Video feature settings button (⚙) to select the specific one you want to use for this Web Server role.
- **Advanced settings:** These advanced settings are reserved for use by our Technical Assistance personnel.

Web Server - Properties tab

Click the **Properties** tab to configure user session time, usage statistics, the URL, port settings, and the SSL certificate for the Web Client.

- **Unlimited session time:** Enable or disable the duration of a user session.(Optional) In Web Client, you can turn on the **Unlimited session time** option so users remain logged in on the Web Client as long as their browser window stays open. Otherwise, users are automatically signed out of the Web Client after 12 hours of inactivity.
- **Web address:** Define the suffix of the URL that users enter on their browser to connect to the Web Client. The format of the URL for the Web Client is *https://host:port/web address*, where *host* is the IP address or host name of the server that hosts the Web Server role, *port* is HTTP port 80 (default) or HTTPS port 443 (default), and *web address* is SecurityCenter by default. The URL of each connection must be unique.
- **Vault location:** In Web Client, when you download video, the files are packaged and temporarily stored in the Web Client vault. These temporary files are deleted when the download is complete. The default location is *ProgramData\Genetec Security Center\WebClientExports*.
- **Use the default web ports of the server:** By default, the Web Client communicates over HTTPS port 443 and HTTP port 80. These ports are defined on the server that hosts the Web Server role. If your IT policy requires different ports, or there is some sort of conflict, you can change the ports used by the Web Client. To change the default ports, set this option to **OFF** and change the HTTP port and secure HTTP port.

  IMPORTANT: If you have an unsigned (invalid) SSL certificate and end-users monitor video in the Web Client using Mozilla Firefox or Microsoft Edge browsers, ensure that the ports set on the Media Gateway match the ports on the web server.

- **Media Gateway:** If your system has multiple Media Gateway roles, select the specific one you want to use for this Web Server role.
- **Communication settings:** View the URL and the SSL certificate in use.
  - Click the URL to open the Web Client in your default web browser.
  - Click **View** to see detailed information about the certificate and to install the certificate.

  The SSL certificate provides a secure HTTP connection to the Web Client. You can continue using the self-signed SSL certificate that is installed with the Web Server role, or install a signed certificate from a Certificate Authority such as VeriSign. In both cases, communications are encrypted and secure. However, Web Client users are notified by their Internet browser that the self-signed certificate is not valid until the certificate is installed on each computer that runs a Web Client session.
- **Advanced settings:** These advanced settings are reserved for use by our Technical Assistance personnel.

Web Server - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Web Server role does not require a database. Ideally, each role is assigned to a single server. You can add more than one server for failover and load balancing.

- **Servers:** Servers hosting this role.

Zone Manager configuration tabs

You configure the settings of the Zone Manager role from the **Roles** view of the *System* task in Security Center Config Tool.

Zone Manager - Properties tab

Click the **Properties** tab to configure the retention period of the zone events in the database.

- **Keep events:** Specify how long to keep the zone events logged by the Zone Manager in the database, before they are deleted.

Zone Manager - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role. All must have access to the role database.
- **Database status:** Current status of the database.
- **Database server:** Name of the SQL Server service. The value (local)\SQLEXPRESS corresponds to *Microsoft SQL Server Express Edition* installed by default with Security Center Server.
- **Database:** Name of the database instance.
- **Actions:** You can perform the following functions on the role database:
  - **Create a database (✚):** Create a new database with the option to overwrite the existing one.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications ():** Set up notifications for when the database space is running low.
  - **Resolve conflicts ():** Resolve conflicts caused by imported entities.
  - **Backup/Restore ():** Back up or restore the database.
- **Authentication:** Specifies which SQL Server authentication is to be used:
  - **Windows:** (Default) Use Windows authentication when the role server and the database server are on the same domain.
  - **SQL Server:** Use SQL Server authentication when the role server and the database server are not on the same domain. You must specify a username and password in this case.
- **Database security:** Security options for communication between the role and its database server.
  - **Encrypt connections:** (Default) Uses Transport Layer Security (TLS) protocol for all transactions between the role and the database server. This option prevents eavesdropping and requires no setup on your part.
  - **Validate certificate:** Authenticates the database server before opening a connection. This is the most secure communication method and prevents *man-in-the-middle* attacks. The *Encrypt connections* option must first be enabled.

    NOTE: You must deploy a valid identity certificate on the database server. A valid certificate is signed by a certificate authority (CA) that is trusted by all servers hosting the role and that is not expired.

Related Topics

Creating databases on page 140
Deleting databases on page 141
Viewing database information on page 145

Receiving notifications when databases are almost full on page 146

Backing up databases on page 147

Restoring databases on page 151

59

Administration tasks

This section lists the options in Security Center administration tasks that have a General settings view, where you can configure general or solution-specific settings for your system.

This section includes the following topics:

ALPR task - General settings view

(Only visible to users with the *ALPR management* > *View general settings* privileges) This section lists the settings found in the *General settings* page in the *ALPR* task.

General settings - Applications page

The *Applications* page lets you configure how Security Desk displays maps in the *Monitoring* and *Route playback* tasks. You can also limit the number of logon attempts in Genetec Patroller™, enforce Patroller privacy settings, and set the attributes a Patroller user must enter when enforcing a hit.

- **Map type:** Display the type of map system supported by your Security Center license.
- **Color for reads:** Click to select the color used to show *license plate reads* on maps.
- **Require reason when generating ALPR report:** When switched to **On**, a *Reason required* dialog is displayed when generating any report that contains ALPR data. This ensures that the reason for the ALPR search is recorded and included in Activity trail (Report generated) audit logs to comply with State laws.
- **List ALPR units that were offline during the Reads report period:** When switched to **On**, the Reads report indicates that the selected units were offline during the queried time.

  NOTE: This settings saved locally. For each computer running Security Desk, you must enable this setting in Config Tool.
- **Initial longitude/latitude:** Set the default starting location for map view in Security Desk. You can type the coordinates in the fields or click Select and zoom in on a location and click Select. A red pushpin appears to indicate the selected position.
- **Logon attempts before lockdown:** You can specify the number of unsuccessful logon attempts a Patroller can make before the account is locked out. For example, if the limit is set to 3, Patroller users have three attempts to log on to Patroller with their username and password. On the fourth attempt, their accounts will be locked and they won't be able to logon. Users with locked accounts must contact their administrators in order to have the password reset. Patroller must be connected to the Security Center server for the password to be reset.
- **Privacy:** Configure Patroller to obscure license plate numbers, or exclude plate, context, or wheel images from reads and hits so that the information is not stored in the ALPR Manager database.
  - **License plate, context, or wheel images:** When switched to *On*, images are not sent to Security Center or included in offloaded data.
  - **License plate:** When switched to *On*, the plate number text string is replaced by asterisks (*) when sent to Security Center or in the offloaded data.
- **Enforced hit attributes:** Create text entry fields that Patroller users must enter text in when they *enforce* a hit. The information from the enforced hit text fields can be queried in the Security Desk hits report.

General settings - Hotlist page

The *Hotlist* page allows you to define the customized attributes, reasons, and categories that will appear in Patroller when the user adds a *New wanted* entry, or rejects or accepts a hit. The settings are downloaded to Patroller along with the selected hotlists when Patroller connects to Security Center. These settings are also available as filter options for hit reports in Security Desk.

- **New wanted attributes:** A new wanted is a hotlist item that is manually entered by the Patroller user. The new wanted attributes are attributes other than the standard ones (plate number, plate issuing state, category) that the Patroller user is asked to specify when entering a new wanted item in the Patroller.
- **New wanted categories:** List of hotlist categories that a Patroller user can pick from when entering a new wanted item. The category is the attribute that says why a license plate number is wanted in a hotlist.

- **Hit reject reasons:** List of reasons for rejecting hotlist hits. These values also become available as Reject reason filter options for generating hit reports in Security Desk.
- **Hit accept reasons:** A form that contains information Patroller users must provide when they accept a hit. The information from the hit form can be queried in the Security Desk Hit report.
- **Enable "No infraction" button:** Select this option to enable the *No infraction* button in the Patroller hit survey. This button allows the Patroller user to skip the hit survey after enforcing a hit.

General settings - Overtime rule page

The *Overtime rule* page allows you to define the custom reject reasons for overtime hits. The values defined here are downloaded to Patrollers and are available as Reject reason filter options for generating hit reports in Security Desk.

One category is pre-configured for you when you install Security Center.

General settings - Permit page

The *Permit* page allows you to define the custom reject reasons for permit hits, and to select the minimum elapsed time for shared permit violations (University Parking Enforcement and City Parking Enforcement). The values defined here are downloaded to patrol vehicles and are available as Reject reason filter options for generating hit reports in Security Desk.

One category is pre-configured for you when you install Security Center.

- **Hit reject reasons:** List of reasons for rejecting permit hits or shared permit hits. These values also become available as Reject reason filter options for generating hits reports in Security Desk.
- **Maximum elapsed time for shared permit violation:** This parameter defines the time period used by University Parking Enforcement patrol vehicles to generate shared permit hits. A shared permit hit is generated when two vehicles sharing the same permit ID are parked in the same parking area within the specified time period.

  For example, let's say you're using the default 120 minutes (two hours), and license plates ABC123 and XYZ456 are sharing the same parking permit. If Patroller reads plate ABC123 at 9:00 am, and then reads plate XYZ456 at 11:01 am, Patroller does **not** raise a hit because the time exceeds the 120 minutes.

General settings - Annotation fields page

The *Annotation fields* page allows you to define additional selectors to appear in Security Desk *Reads* or *Hits* report. To be valid, the selector must relate exactly to the information contained in the actual read or hit.

For example, if you configure *CarModel* and *CarColor* as an Enforced hit attribute, the Patroller user will be asked to enter the car's model and color when enforcing a hit, and the information will be stored with the hit. Specifying *CarColor* as an *Annotation* field will allow the values entered by the user to be displayed in a *Hits* report. For more information about the Enforecd hit attribute, see the *AutoVu™ Deployment Guides*.

You can also add user custom fields to annotation fields in order to associate a user's metadata with individual reads and hits. This allows you to query and filter for the user custom fields in Security Desk *Reads* and *Hits* reports.

Related Topics

Generating reports on page 57

Access control task - General settings view

(Only visible to users with the *Task privileges* > *Administration* > *Access control* > *General settings* privilege) This section lists the settings found on the *General settings* page in the *Access control* task.

The *General settings* page in the *Access control* task lets you configure the general settings pertaining to access control, and to install and configure custom card formats.

- **Visitors:**
  - **Cardholder groups can escort visitors:** Turn this option on (default=on) to assign a cardholder group as a visitor host. Any of the cardholders that can escort visitors in the selected group can act as the visitor host.
  - **Limit visitors for single host:** Turn this option on (default=off) to set the threshold above which a second host must be added. There is no limit to the visitor number for two-host delegations.
  - **Maximum visitors for single host:** This option is enabled when **Limit visitors for single host** is on.
- **Miscellaneous:**
  - **Trigger event 'Entity is expiring soon':** Turn this option on (default=off) to have Security Center generate the *Entity is expiring soon* event *n* days before a cardholder or a credential expires, which can trigger an action to warn someone about the upcoming expiry.
  - **Create incident before door state override:** Turn this option on (default=off) to prompt the Security Desk user to report an incident every time they lock or unlock a door manually, or override the unlock schedule assigned to the door.
  - **Maximum picture file size:** Set the maximum file size (default=20 KB) for pictures (such as a cardholder picture) stored in the Directory database to save disk space.
- **Credentials:**
  - **Card request reasons:** Add reasons that users can choose from to explain why they are requesting a credential card to be printed (for example, no printer on site).
  - **Custom card formats:** Lists the custom card formats defined in your system. You can add, delete, or modify them.
  - **Mobile credential profiles:** Lists the mobile credential profiles defined in your system. You can add, delete, or modify them.

    NOTE: When the Mobile Credential Manager role is created, these settings are disabled. You can configure the mobile credential profiles on the *Configuration* page of the role instead.

Related Topics

Receiving notifications when cardholders are expiring on page 844

Adding reasons for credential card requests on page 872

Defining the maximum file size of pictures on page 823

Creating custom card formats on page 884

Setting up mobile credential profiles on page 876

System task - General settings - Custom fields page

(Only visible to users with the *Modify custom field definitions* privilege) The *Custom fields* page in the *General settings* view is where you define custom fields and custom data types for your system entities.

Custom fields tab

The *Custom fields* tab lists all custom fields defined in your system and allows you to add new ones.

Each custom field is characterized by the following properties:

- **Entity icon/Field name:** Custom field name and the entity type using it.
- **Data type:** Custom field data type. The default data types are:
  - **Text:** Alphanumeric text.
  - **Numeric:** Integers in the range -2147483648 to 2147483647.
  - **Decimal:** Real numbers from -1E28 to 1E28.
  - **Date:** Gregorian calendar date.
  - **Date/Time:** Gregorian calendar date and time.
  - **Boolean:** Boolean data, represented by a check box.
  - **Image:** Image file. The supported formats are: bmp, jpg, gif, and png.
  - **Entity:** Security Center entity.
- **Default value:** Preset default values are provided for certain data types. This column displays the default value that was selected when defining the custom field. The selected value appears when the field is displayed in the specific entity.
- **Mandatory:** A value must be provided with this type of field, otherwise the system will not accept your changes.
- **Value must be unique:** Indicates a key field. This option does not apply to fields using custom data types.
- **Group name/Priority:** Name the custom field is grouped under, and the field's order of appearance within the group. *No group (1)* is the default value. Custom fields that belong to no group appear first in the entity's custom field page.
- **Owner:** Name of the Global Cardholder Synchronizer role when the custom field is part of is part of a shared *global entity* definition.

Custom data types tab

The *Custom data types* tab lists all custom data types defined in your system and allows you to add new ones.

Each custom data type is characterized by the following properties:

- **Data type:** Name of the custom data type.
- **Description:** Optional data type description.
- **Values:** Enumeration of acceptable values (text strings) for this data type.
- **Owner:** Name of the Global Cardholder Synchronizer role when the custom data type is part of a shared *global entity* definition.

System task - General settings - Events page

(Only visible to users with the *Modify custom events* privilege) The *Events* page allows you to define event colors and custom events.

Custom events tab

The *Custom events* tab allows you to view and add custom events to your system.

- **Custom event:** Name of the custom event.
- **Value:** Unique number to identify the custom event from other custom events.

Event colors tab

The *Event colors* tab allows you to assign different colors to different *system events*.

- **Event:** Event to assign a color to.
- **Color:** Assigned color for that event in Security Desk.

System task - General settings - Actions page

(Only visible to users with the *Modify event-to-actions* privilege) The *Actions* page allows you to create event-to-actions for your system, and search for the ones that have already been defined by source entity (name and type), event type, and action type.

- **Entity:** Source entity, or the entity the event is attached to.
- **Event:** Name of the event that triggers the action.
- **Action:** Name of the action triggered by the event.
- **Arguments:** Additional information required for the action. For example, if the action is *Trigger alarm*, the argument is the alarm type that is triggered. Or, if the action is *Send a message*, the argument is the email recipient.
- **Details:** Additional details about the action.
- **Schedule:** Schedule when this event-to-action applies. Event occurring outside the time range covered by the schedule do not trigger any action.

System task - General settings - Logical ID page

(Only visible to users with the *Modify logical IDs of entities* privilege) The *Logical ID* page allows you to view and assign logical IDs to all entities defined in your system.

- **Show logical ID for:** Different groups of entity types. Logical IDs must be unique across all entities of a same group. The groups are listed in the drop-down list.
- **Hide unassigned logical IDs:** Select this option to only show entities with a logical ID assigned.
- **Name:** Name of the entity, public task, or workstation.
- **ID:** Logical ID assigned to the entity, public task, or workstation.
- **Alarm monitoring:** Assign a logical ID to the *Alarm monitoring* task in Security Desk. This allows the Security Desk user to open the Alarm monitoring task using a keyboard shortcut.

System task - General settings - User password settings page

On the *User password settings* page, you can enforce a minimum complexity for all user passwords and configure expiry notification periods for advanced passwords. This page is only visible to users with the *Modify user password settings* privilege.

- **Enforce a minimum number of:** Add minimum requirements to user passwords. You can enforce minimums for the following types of characters:
  - Total characters
  - Upper case letters
  - Lower case letters
  - Numerical characters
  - Special characters
- **Expiry notification period:** Select how many days before the password is going to expire to notify the user (0 - 30 days).

System task - General settings - Activity trails page

(Only visible to users with the *Modify activity trails* privilege) The *Activity trails* page allows you to select which types of user-related activity (events triggered by users) are recorded in the database, and available for reporting in the *Activity trails* task.

System task - General settings - Audio page

(Only visible to users with the *Modify audio files* privilege) The *Audio* page shows all the sound bites (WAV files) available to your system that can alert you when you receive a new alarm, or that you can use with the *Play a sound* action.

- **Play:** Play the sound bite.
- **Stop:** Stop playing the sound bite.

IMPORTANT: Only WAV files can be used. MP3 audio files are not supported.

System task - General settings - Threat levels page

(Only visible to users with the *View threat levels* privilege) The *Threat levels* page lists all threat levels configured in your system, allows you to add new ones, and allows you to modify and delete existing ones.

- **Threat level:** Threat level name.
- **Description:** Threat level description.
- **Color:** Color identifying this threat level. The Security Desk background turns to this color when the threat level is set at the system level.
- **Activation actions:** Number of actions in the threat level activation list. These actions are executed by the system when the threat level is set.
- **Deactivation actions:** Number of actions in the threat level deactivation list. These actions are executed by the system when the threat level is cleared.

System task - General settings - Incident categories page

(Only visible to users with the *Modify incident categories* privilege) The *Incident categories* page allows you to define categories that can then be selected when reporting incidents in Security Desk.

- **Add category:** The green plus sign allows you to type in categories that can serve as a logical grouping of your incidents such as theft, internal affairs, suspicious activities, etc. They will be used in Security Desk when the incident is created.
- **Remove category:** The red X allows you to delete the selected category.
- **Edit category:** The pencil allows you to modify the selected category name.

System task - General settings - Features page

(Only visible to users with the *Modify enabled features* privilege) To simplify the user interface, the *Features* page allows you to turn off features you are not using in your system, although they are supported by your license. You can only select from features that are supported by your license. Unsupported features are not listed.

System task - General settings - Updates page

(Only visible to users with the *Access GUS web page* privilege) To help you monitor and update your Security Center products with the Genetec™ Update Service (GUS), the *Updates* page provides access to the GUS application from Config Tool.

GUS is automatically installed with Security Center. You can use GUS to do the following:

- Update your Genetec™ products when a new release becomes available.
- Check for updates at regular intervals.
- Download update packages in the background. Updates must be manually installed.
- See when the system was last checked for updates.
- Automatically refresh the license in the background to ensure it is valid and the expiration date is updated.

  NOTE: Applies to subscription systems only.
- Enable various features, such as the Genetec Improvement Program.
- Review your firmware versions, get notified of vulnerabilities or recommended upgrades, and download firmware updates as recommended by Security Center.
- Automatically update the license after a major Security Center upgrade.

For more information about using GUS, see the *Genetec™ Update Service User Guide*

60

Events and actions

This section includes the following topics:

Event types

All events in Security Center are associated with a *source entity*, which is the main focus of the event.

NOTE: When specifying the source entity (**From** list) in the *Event-to-action* dialog box, note that events that apply to doors also apply to areas, and events that apply to cardholders also apply to cardholder groups and visitors. To receive *health events*, you must configure them in the Health Monitor role's *Properties* page.

Security Center supports the following event types:

Event	Source entity	Description
A door of an interlock has an unlock schedule configured	area	A door that is part of an interlock configuration has an unlock schedule configured.
A door of an interlock is in maintenance mode	area	A door that is part of an interlock configuration is in maintenance mode.
Ability to write on a drive as been restored	Archiver or Auxiliary Archiver role	Ability to write on a drive has been restored.
AC fail	access control unit or intrusion detection unit	AC (alternating current) has failed.
Access denied	cardholder, credential, door, or elevator	A cardholder is denied access (any reason).
Access denied: A second cardholder is required	door	Two cardholders must present their credentials within a certain delay of each other and the delay has expired. This event only applies to doors controlled by Synergis™ units.
Access denied: Antipassback violation	door	A cardholder requested access to an area that they have already entered, or requested access to leave an area that they were never in.
Access denied: Card and PIN timeout	door or elevator	A card and PIN are required to enter an area, and the cardholder did not enter the PIN within the allotted time.
Access denied: Companion was denied	door or elevator	Two-person rule is enforced, and one of the cardholders was denied access.
Access denied: Denied by access rule	door or elevator	The cardholder is denied access according to the access rule.
Access denied: Escort not supported by this unit model	door or elevator	The visitor escort rule is enforced on an area, but the unit controlling its doors does not support this feature.
Access denied: Expired credential	cardholder, credential, door, or elevator	An expired credential has been used.
Access denied: First-person-in rule supervisor absent	door or elevator	The first-person-in rule has been enforced on the area, and no supervisor has arrived yet.
Access denied: Host is required	door or elevator	The visitor escort rule is enforced and the visitor badged before the host.

Event	Source entity	Description
Access denied: Inactive cardholder	cardholder, door, or elevator	A cardholder with an inactive profile has attempted to access a door or elevator.
Access denied: Inactive credential	cardholder, credential, door, or elevator	A credential with an inactive profile has been used.
Access denied: Insufficient privileges	door or elevator	The cardholder is denied access because they do not have the required security clearance. This event only applies to doors controlled by Synergis units.
Access denied: Interlock	door	Access is denied because of an interlock constraint.
Access denied: Invalid PIN	door or elevator	The cardholder entered an invalid PIN.
Access denied: Lost credential	cardholder, credential, door, or elevator	A credential that has been declared as lost has been used.
Access denied: Max occupancy reached	door or elevator	The cardholder is denied because the area is at its occupancy limit.
Access denied: No access rule assigned	door or elevator	The cardholder is denied access because they are not assigned any access rights.
Access denied: Out of schedule	door or elevator	The access rule associated with this cardholder does not apply during the date or time specified in the schedule.
Access denied: Stolen credential	cardholder, credential, door, or elevator	A credential that has been declared as stolen has been used.
Access denied: Unassigned credential	credential, door, or elevator	A credential that has not been assigned to a cardholder has been used.
Access denied: Unknown credential	door or elevator	A credential that is unknown in the Security Center system has been used.
Access denied: Valid card, inactive PIN	door or elevator	A card and PIN are required to enter an area, and the cardholder entered an inactive PIN.
Access denied: Valid card, invalid PIN	door or elevator	A card and PIN are required to enter an area, and the cardholder entered an invalid PIN.
Access granted	cardholder, door, or elevator	Access has been granted through a door to a cardholder according to the access rules governing the door, elevator, or area. For a perimeter door of an interlock: When an authorized cardholder accesses a door of an interlock, Security Center might generate an *Access granted* event for the door even though the door does not unlock (due to another perimeter door already being open).
Adaptive motion triggered	camera (video analytics)	Motion has been detected on a camera equipped with video analytics capabilities.

Event	Source entity	Description
Agent started	Wearable Camera Manager role	Health event generated when a role agent starts.
Agent stopped	Wearable Camera Manager role	Health event generated when a role agent stops.
Agent stopped unexpectedly	Wearable Camera Manager role	Health event generated when a role agent stops unexpectedly.
Alarm acknowledged	alarm	An alarm has been acknowledged by a user, or auto-acknowledged by the system.
Alarm acknowledged (alternate)	alarm	An alarm has been acknowledged by a user using the alternate mode.
Alarm being investigated	alarm	An alarm with a acknowledgment condition that is still active has been put into the *under investigation* state.
Alarm condition cleared	alarm	The acknowledgment condition of an alarm has been cleared.
Alarm context changed	alarm	The **Context** field of an alarm has been edited by a user.
Alarm forcibly acknowledged	alarm	An alarm has been forcibly acknowledged by a user with special privileges.
Alarm trigger rate high	Directory role	Health event generated when the alarm trigger rate rises above the *high* threshold configured in the Health Monitor role's *Properties* page for this event.
Alarm trigger rate normal	Directory role	Health event generated when the alarm trigger rate drops below the *normal* threshold configured in the Health Monitor role's *Properties* page for this event.
Alarm triggered	alarm	An alarm has been triggered.
An interlock cannot be in hard antipassback mode	area	An interlock cannot be in hard antipassback mode. This is an illegal configuration.
An interlock cannot have a perimeter door with no door sensor configured	area	Interlock cannot be enforced if the system cannot tell whether a door is open or not.
An interlock cannot have only one perimeter door	area	You need at least two perimeter doors for interlock to be applied.
Antipassback disabled: Invalid settings	area	Antipassback disabled: Invalid settings.
Antipassback disabled: Not supported when unit is not in server mode	area	Units have not been set to server mode. Antipassback is available according to the unit’s operating mode. For more information about unit limitations, see the *Security Center Release Notes.*

Event	Source entity	Description
Antipassback violation	area, cardholder, or visitor	An access request was made to enter an area with a credential that is already inside the area, or to exit an area with a credential that was never in the area.
Antipassback violation forgiven	cardholder or visitor	A security operator has granted access to a cardholder responsible for a passback violation.
Application connected	Security Desk	Health event generated when a user connects to the Directory through Security Desk.
Application disconnected by user	Security Desk	Health event generated when a user disconnects his Security Desk from the Directory.
Application disconnected unexpectedly	Security Desk	Health event generated when a Security Desk application is disconnected from the Directory, but not by the user (network issue or application crash).
Application lost	application or role	An application or a role has lost its connection to the Directory.
Application started	Security Desk	Health event generated when a Security Desk application starts.
Application stopped	Security Desk	Health event generated when a Security Desk application is stopped manually. Stopping Security Desk and disconnecting it from the Directory are not necessarily done at the same time. For example, Security Desk can run without being connected to the Directory.
Application stopped unexpectedly	Security Desk	Health event generated when a Security Desk application is stopped unexpectedly, for example, by a crash.
Archive backup failed	Archiver role or camera	Health event generated when a **Backup** archive transfer operation failed.
Archive backup succeeded	Archiver role or camera	Health event generated when a **Backup** archive transfer operation succeeded.
Archive duplication canceled	Archiver role or camera	Health event generated when a **Duplicate archives** archive transfer operation is canceled.
Archive folder path is too long	Archiver or Auxiliary Archiver role	The disk base path for video archives has exceeded the maximum length permitted by the operating system.

Event	Source entity	Description
Archive transfer sequence imported	camera	A new video sequence is made available for use in the Archiver. The type of transfer and the start and end time of the imported sequence is shown in the description. The possible transfer types are: • Consolidation • Duplicate • Import (for offline device) • EdgeTrickling
Archiving disk changed	Archiver or Auxiliary Archiver role	The **Allotted space** on one of the disks assigned for archive storage for this Archiver has been used up, and the Archiver has switched to the next disk in line. The names of the previous disk and current disk are indicated in the **Description** field.
Archiving queue full	camera	A camera (video encoder) is streaming video faster than the Archiver is able to write the video packets to disk. A problem with the Archiver database also triggers this event. The name of the camera whose packets are lost is indicated in the **Description** field.
Archiving started	Archiver or Auxiliary Archiver role	Health event generated when the Archiver role is ready to archive video.
Archiving stopped	Archiver or Auxiliary Archiver role	Archiving has stopped because the disks allocated for archiving are full. This event always accompanies a *Disk full* event.
Asset moved	asset	An asset has been moved.
Asset offline	asset	The RFID tag of an asset has gone offline.
Asset online	asset	The RFID tag of an asset has been put online.
Audio alarm	camera	A sound has been picked up by a microphone associated with a camera.
Audio analytics event	camera (video analytics)	An audio analytics event has been detected on a camera equipped with audio analytics capabilities.
Badge printing job canceled	cardholder or visitor	A user has canceled a badge printing job.
Badge printing job completed	cardholder or visitor	A user has completed a badge printing job.
Badge printing job queued	cardholder or visitor	A user has queued a badge printing job.
Battery fail	access control unit or intrusion detection unit	The unit battery has failed.
Below max occupancy	area	Number of people in the area has dropped under the maximum occupancy limit.
Block camera started	camera	A user has blocked a video stream from other users in the system.

Event	Source entity	Description
Block camera stopped	camera	A user has unblocked a video stream from other users in the system.
Camera recording problem	camera	Health event generated when the camera is not able to record its video.
Camera recording recovered	camera	Health event generated when the camera is able to record again.
Camera tampering	camera (video analytics)	A dysfunction has occurred, potentially due to camera tampering, resulting in a partial or complete obstruction of the camera view, a sudden change of the field of view, or a loss of focus.
Cannot write on the specified location	Archiver or Auxiliary Archiver role	The Archiver cannot write to a specific drive. The path to the drive is indicated in the **Description** field.
Cannot write to any drive	Archiver or Auxiliary Archiver role	The Archiver is unable to write to any of the disk drives. This situation can arise for the following reasons: When write accesses to shared drives are revoked. When shared drives are inaccessible. When shared drives no longer exist. When this happens, archiving is stopped. The Archiver re-evaluates the drive status every 30 seconds.
Certificate error	access control and video unit	Health event generated by the Unit Assistant role when there is a problem with the certificate of the unit it manages.
Certificate valid	access control and video unit	Health event generated by the Unit Assistant role when the certificate is valid after having a warning or an error.
Certificate warning	access control and video unit	Health event generated by the Unit Assistant role when the certificate has a non-critical issue. For example, when the certificate is about to expire.
Connection failed	AD role, Federation™ role, or GCS role	Health event generated when the role is not able to connect to the remote component.
Connection restored	AD role, Federation™ role, or GCS role	Health event generated when the role is able to connect to the remote component again.
Connection to camera established	camera	Health event generated when the Archiver role connects to the camera.
Connection to camera stopped by user	camera	Health event generated when the Archiver role disconnects from the camera through a user action. For example, role stopped by the user.
Connection to camera stopped unexpectedly	camera	Health event generated when the disconnection of the Archiver role from the camera is not intentional. For example, the role crashed, network disconnection, and so on.

Event	Source entity	Description
Connection to unit established	unit	Health event generated when the role connects to the unit.
Connection to unit stopped by user	unit	Health event generated when the role disconnects from the unit through a user action. For example, role stopped by the user.
Connection to unit stopped unexpectedly	unit	Health event generated when the disconnection of the role from the unit is not intentional. For example, the role crashed, network disconnection, and so on.
Convenience time started	parking rule	The convenience time portion of the parking session has begun.
CPU usage high	server	Health event generated when the CPU usage of the server rises above the threshold configured in the Health Monitor role's *Properties* page for this event.
CPU usage normal	server	Health event generated when the CPU usage of the server drops below the threshold configured in the Health Monitor role's *Properties* page for this event.
Crowd detected	camera (video analytics)	A crowd or queue has been detected on a camera equipped with video analytics capabilities.
Custom event	(system-wide)	A custom event is an event added after the initial system installation. Events defined at system installation are called system events. Custom events can be user-defined or automatically added through plugin installations. Unlike system events, custom events can be renamed and deleted.
Database automatic backup failed	Directory role	Health event generated when the backup and restore feature is not working.
Database automatic backup restored	Directory role	Health event generated when the backup and restore feature was successful.
Database lost	Any role using a database	The connection to the role database was lost. If this event is related to a role database, it might be because the database server is down or cannot be reached by the role server. If the event is related to the Directory database, the only action you can use is *Send an email* because all other actions require a working connection the Directory database.
Database recovered	Any role using a database	The connection to the role database has been recovered.
Database restore failed	Directory Manager role	Health event generated when the Directory database failover backup and restore feature failed.

Event	Source entity	Description
Database restore succeeded	Directory Manager role	Health event generated when the Directory database failover backup and restore feature was successful.
Database space low	Any role using a database	Health event generated when the available disk space drops below the threshold configured in the Health Monitor role's *Properties* page for this event.
Database space normal	Any role using a database	Health event generated when the available disk space rises above the threshold configured in the Health Monitor role's *Properties* page for this event.
Deadbolt locked	zone	The deadbolt on a door has been locked.
Deadbolt unlocked	zone	The deadbolt on a door has been unlocked.
Direction alarm	camera (video analytics)	A direction alarm has been triggered on a camera equipped with video analytics capabilities.
Directory started	Directory role	Health event generated when the Directory role starts. This can only happen if you have more than one Directory server.
Directory stopped by user	Directory role	Health event generated when the Directory role does a clean shutdown. For example, when Genetec™ Server is stopped in Windows services.
Directory stopped unexpectedly	Directory role	Health event generated when the Directory role stopped unintentionally. For example, during a server crash.
Disk access restored	Archiver or Auxiliary Archiver role	The role regained access to its disks.
Disk access unauthorized	Archiver or Auxiliary Archiver role	The role is not able to access its disks.
Disk load threshold exceeded	Archiver or Auxiliary Archiver role	The disk space allocated for archiving has exceeded its load threshold (default=90%). This is caused by under-evaluating the disk space required, or by another application that is taking more disk space than it should. If 100% of the allotted disk space is used, the Archiver starts to delete old archive files prematurely to free disk space for new archive files, starting with the oldest files.
Disks full	Archiver or Auxiliary Archiver role	All disks allotted for archiving are full and the Archiver is unable to free disk space by deleting existing video files. This event can occur when another application has used up all the disk space reserved for Security Center, or when the **Delete oldest files when disks full** option is not selected in the Server Admin. When this happens, archiving is stopped. The Archiver re-evaluates the disk space every 30 seconds.

Event	Source entity	Description
Door closed	door	The door has closed. For this event to be generated, the door must be equipped with a door sensor.
Door forced open	door	The door is locked but the door sensor indicates that the door is open.
Door locked	door	The door is considered locked in Security Center.
Door maintenance completed	door	The door has been taken out of maintenance mode.
Door maintenance started	door	The door has been put into maintenance mode.
Door manually unlocked	door	In Security Desk, a user has manually unlocked a door.
Door offline: Device is offline	door	One or more devices associated to this door has gone offline.
Door online	door	The door is back online after being offline.
Door opened	door	The door has opened. For this event to be generated, the door must be equipped with a door sensor.
Door open too long	door	The door has been held open for too long. To enable this event, you must set the **Trigger event** to **ON** in the *Door held* section of the door's *Properties* page in Config Tool.
Door secured	door	The door has been properly closed and locked after a *Door unsecured* event. For this event to be generated, the door must be equipped with a door sensor, a door lock, and a lock sensor.
Door test completed successfully	door	The door test has been completed successfully.
Door test failed	door	The door test has failed.
Door test failed: Aborted	door	The door test has been aborted.
Door test failed: Canceled because door is unsecured	door	The door test has been canceled because the door is not secured.
Door test failed: Canceled because of shunted readers	door	The door test has been canceled because readers are shunted.
Door test failed: Door failed to relock	door	The door test has failed because the door did not relock.
Door test failed: Door failed to unlock	door	The door test has failed because the door did not unlock.
Door test failed: Error occurred	door	The door test has failed because an error occurred.

Event	Source entity	Description
Door test started	door	The door test has started.
Door unlocked	door	The door has been unlocked.
Door unsecured	door	The door has been unlocked, but the door lock indicates that the door is locked. For this event to be generated, the door must be equipped with a door sensor, a door lock, and a lock sensor.
Doorknob in place	zone	The doorknob is in place and the door is closed.
Doorknob rotated	zone	The doorknob has rotated.
Double-badge off	cardholder, credential, or door	The door has been locked and an associated event has stopped.
Double-badge on	cardholder, credential, or door	The door has been unlocked and an associated event has been triggered.
Duplicating archives failed	Archiver role or camera	Health event generated when a **Duplicate archives** archive transfer operation failed.
Duplicating archives partially failed	Archiver role or camera	Health event generated when a **Duplicate archives** archive transfer operation failed half-way through.
Duplicating archives succeeded	Archiver role or camera	Health event generated when a **Duplicate archives** archive transfer operation succeeded.
Duplicating archives will retry	Archiver role or camera	Health event generated when a **Duplicate archives** archive transfer operation failed but will retry later.
Duress PIN entered	cardholder or door	A cardholder entered a duress PIN at a door.
Edge storage medium failure	camera or video unit	After a unit was restarted, the video that was recorded on the edge could not be accessed.
Elevator offline: Device is offline	elevator	One or more devices associated to this elevator has gone offline.
End of camera tampering	camera (video analytics)	A dysfunction, which might have been caused by camera tampering, has been resolved.
Entity has expired	cardholder or credential	A credential or its associated cardholder has expired (its status is now *Expired*).
Entity is expiring soon	credential	Security Center generates this event to warn you that the expiry date of an entity is approaching. The number of days of advance warning provided by this event must be set.
Entity is offline	server, role, or unit	Health event generated when an entity goes offline (red).
Entity is online	server, role, or unit	Health event generated when an entity is back online (black).

Event	Source entity	Description
Entity warning	any entity	A health warning has been issued for this entity.
Entry assumed	cardholder or door	A cardholder was granted access to a door or area, and it is assumed that they entered because no door sensor is configured.
Entry detected	cardholder or door	A cardholder was granted access to a door or area, and their entry is detected. For this event to be generated, you must configure an entry sensor on the door side where you want entry to be detected. If no Entry Sensors are configured on the door, the event will be generated based on the Door Sensor input.
Evacuation ended	area	An evacuation from the area has ended. This event is generated from the Evacuation Assistant plugin.
Evacuation started	area	An evacuation from the area has been started. This event is generated from the Evacuation Assistant plugin.
Face detected	camera (video analytics)	A face has been detected on a camera equipped with video analytics capabilities.
Face recognized	camera (video analytics)	A face on a *hotlist* has been recognized by a camera equipped with video analytics capabilities.
Failed to create a signed token	Directory role	Health event generated when the system cannot generate a token for authentication.
File deleted	camera	A video file associated to a camera has been deleted because the retention period has ended, or the archive storage disk was full.
Files deleted before cloud upload because disk is full	camera	Video archives are deleted before cloud upload because the archive storage disk is full.
Files deleted before cloud upload because retention period exceeded	camera	Video archives are deleted before cloud upload because the local retention period has ended.
Firmware upgrade canceled	access control unit	A firmware upgrade on an access control unit has been canceled.
Firmware upgrade failed	access control unit	A firmware upgrade on an access control unit has failed.
Firmware upgrade scheduled	access control unit	A firmware upgrade on an access control unit has been scheduled.
Firmware upgrade started	access control unit	A firmware upgrade on an access control unit has started.
Firmware upgrade succeeded	access control unit	A firmware upgrade on an access control unit has completed successfully.
First person in	area	A cardholder has entered an empty area.

Event	Source entity	Description
Floor accessed	elevator	An elevator floor button has been pressed.
Glass break	zone	Glass has broken.
Hardware tamper	access control unit, door, elevator, or zone	The tamper input on a unit has been triggered.
Health event	Health monitor role	A health event has occurred.
Heat map changed	camera (video analytics)	A change has been detected in a heat map area on a camera equipped with video analytics capabilities.
Input alarm activated	input on intrusion detection unit	The input has entered an *alarm* state.
Input alarm restored	input on intrusion detection unit	The input has left an *alarm* state.
Input bypassed	input on intrusion detection unit	The input has entered a *bypassed* state.
Input bypass restored	input on intrusion detection unit	The input has left a *bypassed* state.
Input state changed: Input active	input on camera, access control unit, or intrusion detection unit	The input has entered an *active* state.
Input state changed: Input normal	input on camera, access control unit, or intrusion detection unit	The input has entered a *normal* state.
Input state changed: Input trouble	input on access control unit or intrusion detection unit	The input has entered a *trouble* state.
Input trouble - open	access control or intrusion detection unit	Supervised input has entered a *trouble* state (open circuit).
Input trouble - short	access control or intrusion detection unit	Supervised input has entered a *trouble* state (short circuit).
Interface module AC fail state active	door	The AC (alternating current) of an interface module has failed.
Interface module AC fail state restored	door	The AC (alternating current) of an interface module has been restored.
Interface module battery fail state active	door	The battery of an interface module has failed.
Interface module battery fail state restored	door	The battery of an interface module has been restored.
Interface module firmware upgrade canceled	access control unit	A firmware upgrade on an interface module has been canceled.

Event	Source entity	Description
Interface module firmware upgrade failed	access control unit	A firmware upgrade request has failed, or there are firmware upgrades past their scheduled start time after the Access Manager role is restarted.
Interface module firmware upgrade package transfer started	access control unit	A firmware upgrade request has been sent to the Synergis™ Cloud Link unit.
Interface module firmware upgrade scheduled	access control unit	A firmware upgrade on an interface module has been scheduled.
Interface module firmware upgrade started	access control unit	A firmware upgrade on an interface module has started.
Interface module firmware upgrade succeeded	access control unit	A firmware upgrade on an interface module has succeeded.
Interface module offline	access control unit	The interface module has gone offline.
Interface module online	access control unit	The interface module has come online.
Interface module tamper state active	door	The tamper input of an interface module has been triggered.
Interface module tamper state restored	door	The tamper input of an interface module has returned to normal.
Interlock is not supported by the unit	area	Interlock is enabled on an area but the access control unit controlling the doors does not support this feature.
Interlock lockdown input active	area	Interlock lockdown has been turned on.
Interlock lockdown input normal	area	Interlock lockdown has been turned off.
Interlock override input active	area	Interlock override is on.
Interlock override input normal	area	Interlock override is off.
Intrusion alarm silenced	intrusion detection area	Intrusion alarm has been silenced.
Intrusion detection area alarm activated	intrusion detection area	Intrusion detection area alarm activated.
Intrusion detection area arming	intrusion detection area	Intrusion detection area is being armed.
Intrusion detection area arming postponed	intrusion detection area	Intrusion detection area arming is postponed.
Intrusion detection area canceled alarm	intrusion detection area	Intrusion detection area alarm is canceled.

Event	Source entity	Description
Intrusion detection area canceled postponed request	intrusion detection area	Intrusion detection area postponed request is canceled.
Intrusion detection area disarm request	intrusion detection area	Intrusion detection area postponed request is canceled.
Intrusion detection area disarmed	intrusion detection area	Intrusion detection area is disarmed.
Intrusion detection area duress	intrusion detection area	Intrusion detection area is disarmed with duress.
Intrusion detection area entry delay activated	intrusion detection area	Intrusion detection area entry delay activated.
Intrusion detection area forced arming	intrusion detection area	Intrusion detection area is forcefully armed.
Intrusion detection area input bypass activated	intrusion detection area	Intrusion detection area input bypass is activated.
Intrusion detection area input bypass deactivated	intrusion detection area	Intrusion detection area input bypass is deactivated.
Intrusion detection area input trouble	intrusion detection area	Intrusion detection area input trouble.
Intrusion detection area master arm request	intrusion detection area	Intrusion detection area master arm request is issued.
Intrusion detection area master armed	intrusion detection area	Intrusion detection area is master armed.
Intrusion detection area perimeter arm request	intrusion detection area	Intrusion detection area perimeter arm request is issued.
Intrusion detection area perimeter armed	intrusion detection area	Intrusion detection area is perimeter armed.
Intrusion detection area postponed arming request	intrusion detection area	Intrusion detection area arming request is postponed.
Intrusion detection unit input bypass activated	intrusion detection unit	Intrusion detection unit input bypass is activated.
Intrusion detection unit input bypass deactivated	intrusion detection unit	Intrusion detection unit input bypass is deactivated.
Intrusion detection unit input trouble	intrusion detection unit	Intrusion detection unit input trouble.
Intrusion detection unit tamper	intrusion detection unit	Intrusion detection unit has been tampered with.
Invalid configuration in unit	video unit	The configuration of the unit is invalid.

Event	Source entity	Description
Invalid custom encryption values	Archiver or Auxiliary Archiver role	This warning is issued by the Archiver on start-up and every 5 minutes if one of the custom encryption values (initial fingerprint or encryption key) specified in the Server Admin is invalid.
Inventory reset	parking zone	The inventory of a parking zone has been reset to zero so that the reported parking zone occupancy can be re-initialized.
Last person out	area	The last cardholder has exited an area.
License plate hit	Any hit rule	A license plate read has been matched to a hotlist, an overtime rule, or a permit restriction.
License plate read	ALPR unit or Genetec Patroller™	A license plate has been read.
Live bookmark added	camera	A user has added a bookmark to a live video.
Live streaming started	camera	Live streaming from a mobile phone camera has started.
Live streaming stopped	camera	Live streaming from a mobile phone camera has stopped.
Lock released	zone	Event related to a zone entity.
Lock secured	zone	Event related to a zone entity.
Loitering	camera (video analytics)	Loitering activity has been detected in the camera footage.
Low battery	asset	The battery on the RFID tag of an asset is about to run out.
Macro aborted	macro	Execution of a macro has failed.
Macro completed	macro	Execution of a macro has been completed normally.
Macro started	macro	Execution of a macro has begun.
Main database lost	Directory Manager role	Health event generated when the Directory database is lost.
Main database recovered	Directory Manager role	Health event generated when the Directory database has been recovered.
Manual station activated	door	Someone has pulled the door emergency release (manual pull station).
Manual station reverted to normal state	door	The door emergency release (manual pull station) has been restored to it normal operating position.
Maximum occupancy exceeded	area	Number of people in the area now exceeds the maximum occupancy limit.

Event	Source entity	Description
Maximum occupancy reached	area	Number of people in the area has reached the maximum occupancy limit.
Memory usage high	server	Health event generated when the memory usage rises above the high threshold configured in the Health Monitor role's *Properties* page for this event.
Memory usage normal	server	Health event generated when the memory usage drops below the normal threshold configured in the Health Monitor role's *Properties* page for this event.
Missing tail host	door	The tail host of a two-host visitor delegation did not badge.
Motion	camera	There is motion detected.
Motion off	camera	This event is issued following a *Motion on* event when motion (measured in terms of number of motion blocks) has dropped below the “motion off threshold” for at least 5 seconds.
Motion on	camera	This event is issued when positive motion detection has been made.
Multiple units are configured for the interlock	area	All doors that are part of an interlock configuration must be controlled by the same unit.
Mustering ended	area	An evacuation has ended and people are no longer evacuating to the area. This event is generated from the Evacuation Assistant plugin only occurs for the last evacuation to the area.
Mustering started	area	An evacuation is in progress and people are evacuating to the area. This event is generated from the Evacuation Assistant plugin and only occurs for the first evacuation to the area.
No entry detected	cardholder or door	A cardholder was granted access to a door or area, but no entry is detected. For this event to be generated, you must configure a door sensor on the door side where you want entry to be detected.
No match	ALPR unit, hotlist	A vehicle has not been matched to the hotlist associated to the Sharp unit.
No RTP packet lost in the last minute	camera	The Archiver has received all the RTP packets in the last minute.
Object condition changed	camera (video analytics)	An object has suddenly changed direction or speed, such as when a person starts running or slips.
Object count changed	camera (video analytics)	A change has been detected in the object count on a camera equipped with video analytics capabilities.

Event	Source entity	Description
Object count reached	camera (video analytics)	An object count limit has been reached for the object count on a camera equipped with video analytics capabilities.
Object crossed line	camera (video analytics)	An object has crossed a predefined tripwire.
Object detected	camera (video analytics)	An object is in the camera field of view.
Object detected in field	camera (video analytics)	An object has been detected in a zone that is being monitored for intrusion on a camera equipped with video analytics capabilities.
Object direction changed	camera (video analytics)	An object has been detected changing direction on a camera equipped with video analytics capabilities.
Object entered	camera (video analytics)	An object has entered the camera field of view.
Object exited	camera (video analytics)	An object has exited the camera field of view.
Object following route	camera (video analytics)	An object is following a predetermined route, in a specific direction.
Object left	camera (video analytics)	An object has entered and exited the camera field of view.
Object merged	camera (video analytics)	Two separate objects in the camera field of view have merged.
Object removed	camera (video analytics)	An object has been removed from the camera field of view.
Object separated	camera (video analytics)	An object within the camera field of view has separated into two objects.
Object stopped	camera (video analytics)	A moving object has stopped.
Object velocity changed	camera (video analytics)	An object has been detected changing speed on a camera equipped with video analytics capabilities.
Offload failed	ALPR Manager, Patroller	An offload from Patroller to Security Center has failed.
Offload successful	ALPR Manager, Patroller	An offload from Patroller to Security Center was successful.
Paid time started	parking rule	Parking time has been purchased through connected pay stations or mobile apps.
Parking zone capacity threshold reached	parking zone	The parking zone capacity has reached the capacity threshold that is defined in the ALPR Manager.

Event	Source entity	Description
People count reset	area	The number of people counted in an area has been reset to 0.
Person added to area	area	A person has been added to an area.
Person falling	camera (video analytics)	A person falling has been detected in the camera.
Person removed from area	area	A person has been removed from an area.
Person running	camera (video analytics)	A person running has been detected in the camera.
Person sliding	camera (video analytics)	A person sliding has been detected in the camera.
Playback bookmark added	camera	A user has added a bookmark to a recorded video.
Protection threshold exceeded	Archiver or Auxiliary Archiver role	The **Protected video threshold** configured from the Archiver has been exceeded. You can monitor the percentage of disk space occupied by protected video files from the Statistics page in the Archiver's Resources tab in Config Tool.
PTZ activated	camera (PTZ)	A user started using the PTZ after it has been idle. The field indicates the user who activated the PTZ. This event is regenerated every time a different user takes control of the PTZ, even when the PTZ is still active.
PTZ locked	camera (PTZ)	A user has tried to move the PTZ while it is being locked by another user with a higher PTZ priority. The field indicates the machine, application type, and user who currently holds the lock.
PTZ stopped	camera (PTZ)	The PTZ has not been manipulated by any user after a predetermined period of time. The field indicates the user who last used the PTZ.
PTZ zoom started	camera (PTZ)	A user started zooming the PTZ. The Description field indicates the user who performed the zoom. Subsequent *PTZ zoom by user* events are generated if another user zooms the PTZ, or if the original user zooms the PTZ after the **Idle delay** has expired.
PTZ zoom stopped	camera (PTZ)	The PTZ has not been zoomed by any user after a predetermined period of time. The field indicates the user who last zoomed the PTZ.

Event	Source entity	Description
Receiving RTP packets from multiple sources	camera	The Archiver is receiving more than one video stream for the same camera. **IMPORTANT:** When this rare situation arises, the Archiver cannot tell which stream is the correct stream by looking at the source IP address because of the NAT (Network Address Translation), so an arbitrary choice is made. This can result in the wrong video stream being archived. However, the source IP address and port number of both streams are indicated in the **Description** field, and the two sources are labeled *Archived* and *Rejected*. You can find the faulty unit that is causing this conflict.
Record updated	(typically an area, but can be any type of entity)	This event is raised by the Record Fusion Service when an event with contextual information linked to a *record type* is triggered in the system, such as when data is ingested through the Record Caching Service role.
Record cache ingestion failed	Record Caching Service role	An operation to import data into a *record cache*, triggered by one of the *Ingest* actions, has ended with an error. Partial data might have been saved. See *Ingest event*, *Ingest file*, and *Ingest from web request* in Action types on page 1434.
Record cache ingestion finished	Record Caching Service role	An operation to import data into a record cache, triggered by one of the *Ingest* actions, has completed successfully.
Record cache ingestion started	Record Caching Service role	An operation to import data into a record cache, triggered by one of the *Ingest* actions, has started.
Recording problem	camera	There is a problem recording the camera. The problem might be due to an error writing to disk, an error writing to the Archiver database, or the fact that the camera is not streaming video when it should.
Recording started (alarm)	camera	The recording on a camera has been started as the result of an alarm being triggered.
Recording started (continuous)	camera	The recording on a camera has been started by a continuous archiving schedule.
Recording started (external)	camera	The recording on a camera has been started by the *Start recording* action. This action could have been triggered by another event or executed from a macro.
Recording started (motion)	camera	The recording on a camera has been started through motion detection.
Recording started (user)	camera	The recording on a camera has been started manually by a user.
Recording stopped (alarm)	camera	The recording on a camera has stopped because the alarm recording time has elapsed.

Event	Source entity	Description
Recording stopped (continuous)	camera	The recording on a camera has stopped because it is no longer covered by a continuous archiving schedule.
Recording stopped (external)	camera	The recording on a camera has been stopped by the *Stop recording* action. This action could have been triggered by another event or executed from a macro.
Recording stopped (motion)	camera	The recording on a camera has stopped because the motion has ceased.
Recording stopped (user)	camera	The recording on a camera has been stopped manually by a user.
Remaining archive disk space low	Archiver or Auxiliary Archiver role	Health event generated when the archiving disk space usage rises above the threshold configured in the Health Monitor role's *Properties* page for this event.
Remaining archive disk space normal	Archiver or Auxiliary Archiver role	Health event generated when the archiving disk space usage drops below the threshold configured in the Health Monitor role's *Properties* page for this event.
Request to exit	door	Someone has pressed the door release button or has triggered a request to exit motion detector. The *Request to exit* event has special filtering to make this feature compatible with motion detection request to exit hardware. Set these properties in the **Config Tool** > **Door** > **Properties** tab.
Request to exit normal	door	No request to exit is being made.
Retrieving archives from units failed	Archiver role or officer	Health event generated when the retrieval of video archives from wearable cameras has failed.
Retrieving archives from units partially failed	Archiver role or officer	Health event generated when the retrieval of video archives from some of the wearable cameras has failed.
Retrieving archives from units succeeded	Archiver role or officer	Health event generated when the retrieval of video archives from wearable cameras has succeeded.
Role started	any role	Health event generated when a role starts.
Role stopped by user	any role	Health event generated when a role is stopped by a user.
Role stopped unexpectedly	any role	Health event generated when a role is stopped unexpectedly. For example, the role crashed.
RTP packet loss high	Officer or Security Desk	Health event generated when the ratio of lost RTP packets rises above the threshold configured in the Health Monitor role's *Properties* page for this event.

Event	Source entity	Description
RTP packet loss normal	Officer or Security Desk	Health event generated when the ratio of lost RTP packets drops below the threshold configured in the Health Monitor role's *Properties* page for this event.
RTP packets lost	camera	There are RTP packets that the Archiver never received. This could happen if the packets have been lost on the network, or if the Archiver does not have enough CPU to process all the packets received on the network card. The field indicates the number of packets lost since the last time this event was issued (no more than once every minute).
Scheduled controlled access	elevator	The schedule for controlled access to elevator floors now applies.
Scheduled free access	elevator	The schedule for free access to elevator floors now applies.
Scheduled lock	door	The door unlock schedule has expired, the lock is now re-asserted (door is locked).
Scheduled unlock	door	The door lock is unlocked due to a programmed unlock schedule.
Schedule unlock ignored: first-person-in rule supervisor absent	door	The door unlock schedule is ignored because the restriction imposed by the first-person-in rule has not yet been satisfied.
Server started	server	Health event generated when a Genetec™ Server service starts.
Server stopped by user	server	Health event generated when a Genetec™ Server service is stopped by a user.
Server stopped unexpectedly	server	Health event generated when a Genetec™ Server service is stopped unexpectedly.
Session completed	parking zone	The vehicle has exited the parking zone.
Session started	parking zone	The vehicle has entered the parking zone.
Signal lost	camera	The camera signal has been lost.
Signal recovered	camera	The camera signal has been recovered.
Signed token creation is ready	Directory role	Health event generated when the system successfully created a token for authentication.
Supervisor in: access rule activated	door	First-person-in rule is enforced on an area, and a supervisor has just badged in, allowing all cardholders with the correct access rights to enter the area.

Event	Source entity	Description
Supervisor in: unlocking schedule activated	door	First-person-in rule is enforced on an area, and a supervisor has just badged in, allowing anyone to enter the area.
Synchronization completed: External system	Active Directory role	The synchronization of an external system has completed.
Synchronization error: External system	Active Directory role	The synchronization of an external system has resulted in an error.
Synchronization failed	Active Directory role	Health event generated when the synchronization of an Active Directory has failed.
Synchronization partially completed due to some conflicts: External system	Active Directory role	The synchronization of an external system was only partially completed.
Synchronization recovered	Active Directory role	Health event generated when the synchronization of an Active Directory has recovered.
Synchronization started: External system	Active Directory role	The synchronization of an external system has started.
Tailgating	camera (video analytics)	Two people have entered a secured area following each other very closely.
Temperature alarm	video unit	The temperature of the video unit has risen above the safety level.
Threat level cleared	threat level	A threat level has been cleared.
Threat level set	threat level	A threat level has been set.
Transmission lost	camera	The Archiver is still connected to the camera, but it has not received any video packets for more than 5 seconds.
Transmission recovered	camera	The Archiver has started to receive video packets from the camera again.
Undefined video analytics event	camera (video analytics)	A generic video analytic event has been issued, but it is not yet mapped to a Security Center event. **TIP:** You can check for additional sub-type information in the analytic metadata.
Unit connected	unit	The connection to a unit has been established or restored.
Unit failed to respond to edge video request	camera	Event related to a camera that is recording directly on the unit.
Unit lost	unit	The connection to a unit has been lost.
Unit synchronization failed	access control unit	The synchronization of the unit with the Access Manager has failed.

Event	Source entity	Description
Unit synchronization started	access control unit	The synchronization of the unit with the Access Manager has started.
Unit synchronization succeeded	access control unit	The synchronization of the unit with the Access Manager has completed successfully.
Unit time in sync with time server	video unit	Health event generated when the unit time is in sync with the time server.
Unit time out of sync with time server	video unit	Health event generated when the unit time is out of sync with the time server.
Unit warning activated	access control unit	The Synergis Cloud Link unit has gone into a warning state. The reason for the warning is detailed in the event description.
Unit warning deactivated	access control unit	The Synergis Cloud Link unit is no longer in a warning state. The latest reason for the warning is detailed in the event description.
Update failed	Patroller, Mobile Sharp	An update on Patroller or a Mobile Sharp unit has failed, or a file could not be synchronized on a Patroller computer.
Update installation completed	Patroller, Mobile Sharp	An update has completed on Patroller or a Mobile Sharp unit, and no reboot is required.
Update installation started	Patroller, Mobile Sharp	A user has started an updated on Patroller by clicking the “Update” icon.
Update published	Patroller, Mobile Sharp	An update has been processed, and is ready to be deployed to Patroller.
Update uninstallation completed	Patroller, Mobile Sharp	A rollback on Patroller or a Mobile Sharp unit has completed.
Update uninstallation started	Patroller, Mobile Sharp	A user has started a rollback on Patroller by clicking the “Rollback” icon.
User logged off	user	A user has logged off of a Security Center application.
User logged on	user	A user has logged on to a Security Center application.
User logon failed	user	User logon attempt failed.
Validating paid time	parking rule	The convenience time or the paid time has expired for the parking session.
Video signal lost	camera	Health event generated when the camera signal has been lost.
Video signal recovered	camera	Health event generated when the camera signal has been recovered.

Event	Source entity	Description
Violation detected	parking rule	The convenience time, the grace period, or the paid time has expired for the parking session.
Violation enforced	parking rule	The vehicle in violation has been ticketed.
Visitor astray	door	A visitor did not badge within the allotted time after the delegation's host or a previous visitor.
VRM connection attempt	Archiver role	The Archiver has attempted to connect to a VRM unit.
VRM connection failure	Archiver role	The Archiver has failed to connect to a VRM unit.
Window closed	zone	A physical window has closed.
Window opened	zone	A physical window has opened.
Zone armed	zone	A zone has been armed.
Zone disarmed	zone	A zone has been disarmed.
Zone maintenance completed	I/O zone	An I/O zone has been taken out of maintenance mode.
Zone maintenance started	I/O zone	An I/O zone has been put into maintenance mode.
Zone offline	I/O zone	An I/O zone is offline.

For a list of events that can be used with KiwiVision video analytics, see "Events to monitor in Security Desk" in the *KiwiVision™ User Guide for Security Center*.

Related Topics

Event types that can require acknowledgment conditions on page 1184
Selecting health events to monitor on page 364

Action types

All actions in Security Center are associated with a target entity, which is the main entity affected by the action. Additional parameters are indicated in the *Description* column. All parameters must be configured for an action to be valid.

Action	Description
Add bookmark	Adds a *bookmark* to a *camera* recording. • **Camera:** Select the camera. • **Message:** Bookmark text.
Arm intrusion detection area	Arms an *intrusion detection area*. • **Intrusion detection area:** Select an intrusion detection area. • **Master:** Arms all sensors in the selected intrusion detection area. Any sensor can trigger the alarm when activated. • **Perimeter:** Arms only the sensors designated to be on the perimeter. Activity on sensors inside the area, such as motion detectors, is ignored. • **Instant:** Arms the area immediately. • **Delay:** Arms the area after a delay. If you do not specify a duration, the panel default is used. • **Arming mode:** ◦ **Normal:** Arms the intrusion detection area normally. Areas with active or troubled sensors remain disarmed. ◦ **Force:** If the area is not ready for normal arming, this option forcefully arms the area. Force temporarily ignores active or troubled sensors during the arming sequence. If an ignored sensor ever returns to a normal state while armed, future activity can trigger the alarm. ◦ **Bypass:** If the area is not ready for normal arming, this option automatically bypasses active or troubled sensors before arming the area. Sensors remain bypassed while the area is armed. Disarming the area removes the bypass.
Arm zone	Arms a *virtual zone*. • **Zone:** Select a virtual zone.
Block and unblock video	Blocks or unblocks a camera from other users in the system. • **Block/Unblock:** Select whether the action should block or unblock the camera. • **Camera:** Select the camera. • **End:** Select how long to block the video for: ◦ **For:** The video is blocked from users for the selected amount of time. ◦ **Indefinitely:** The video is blocked from users until you manually unblock it. • **User level:** Select a minimum user level. All users with a level lower than the one you select are blocked from viewing video.
Cancel postpone intrusion detection area arming	Cancels the postponed arming of an *intrusion detection area*. • **Intrusion detection area:** Select the intrusion detection area.

Action	Description
Clear tasks	Clears the task list in the specified Security Desk monitors. • **Destination:** Select one of the following: • **User:** All monitors of all Security Desk applications connected with the specified username. • **Monitor:** Specific Security Desk monitor identified by a machine name and a monitor ID.
Disarm intrusion detection area	Disarms an *intrusion detection area*. • **Intrusion detection area:** Select the intrusion detection area.
Disarm zone	Disarms a *virtual zone*. • **Zone:** Select a virtual zone.
Disarm a camera on an analog monitor	Displays a camera in an analog monitor in a canvas tile. • **Camera:** Select which camera to display in the analog monitor. The camera must be supported by the analog monitor, and use the same video format. • **Analog monitor:** Select an analog monitor to display the camera in.
Display an entity in the Security Desk	Displays a list of entities in the Security Desk *canvas* of selected *users*, in terms of one entity per tile. This action is ignored if a user does not have a *Monitoring* task open in Security Desk. • **Recipients:** Select the users. • **Entities:** List of entities to display. Each entity is displayed in a separate tile. • **Display options:** Select one of the following: • **View in a free tile:** Only use free tiles. • **Force display in tiles:** Display in free tiles first. When there are no more free tiles, use the busy tiles following the tile ID sequence. • **Enable camera audio:** This option enables audio automatically when associated video is displayed. The selected camera must support audio.
Email a report	Sends a report (based on a saved reporting task) as an email attachment to a list of *users*, cardholders, or specified email addresses. • **Report:** Select a saved public task. • **Recipients:** Select the users, user groups, cardholders, or cardholder groups to send the report to. You can only select cardholders if you have the *Send an email to cardholders and external recipients* privilege. • **External Recipients:** This field is available if the user has the *Send an email to cardholders and external recipients* privilege. Enter one or more email addresses for recipients outside of Security Center. Use commas, semi-colons, or new lines to separate multiple addresses. **NOTE:** When saving the action, the external recipients list is saved comma separated on one line. **IMPORTANT:** For cardholders and external recipients, you must first set the **User profile for securing emails** in Report Manager to enable or restrict access rights. • **Export format:** Report format, either *PDF*, *Excel*, or *CSV*.

Action	Description
Email a snapshot	Sends a series of snapshots of a video feed as an email attachment to a list of users, cardholders, or specified email addresses. • **Camera:** Select the camera. • **Snapshots:** Select how many seconds before (maximum -300 seconds) or after (maximum 5 seconds) the defined *Recurrence time* to email the snapshot. • **Recipients:** Select the users, user groups, cardholders, or cardholder groups to receive the snapshot. You can only select cardholders if you have the *Send an email to cardholders and external recipients* privilege. An email address must be defined in the properties of the entity: user, user group, cardholder, or cardholder group. • **External Recipients:** This field is available if the user has the *Send an email to cardholders and external recipients* privilege. Enter one or more email addresses for recipients outside of Security Center. Use commas, semi-colons, or new lines to separate multiple addresses. **NOTE:** When saving the action, the external recipients list is saved comma separated on one line. **IMPORTANT:** For cardholders and external recipients, you must first set the **User profile for securing emails** in Report Manager to enable or restrict access rights. • **Export format:** Available image formats: PNG, GIF, JPEG, or Bitmap. **NOTE:** To send snapshots, the **Enable thumbnail requests** option must be turned on in the **Resources** tab of the Archiver or Auxiliary Archiver that is managing the camera.
Export report	Generates and saves a report specified by a public task. • **Report:** Select a public task. • **What to export:** • **Data:** Export the data and select the export format (Excel, CSV, PDF). • **Charts:** Export any associated charts and select the export format (PNG, JPEG). • **Orientation:** (PDF only) Select whether the PDF file should be in portrait or landscape mode. • **Overwrite existing file:** Select whether to overwrite a previously saved report in the destination folder. The destination folder is a property of the Report Manager role.
Forgive antipassback violation	Forgives an *antipassback* violation for a *cardholder*, or *cardholder group*. • **Entity:** Select a cardholder or cardholder group.
Go home	Commands the PTZ camera to go to its home position. Not all PTZ cameras support this feature. • **Camera:** Select a PTZ camera.
Go to preset	Commands the PTZ camera to go to the specified preset position. • **Camera:** Select a PTZ camera. • **Preset:** Preset position (number) to go to.

Action	Description
Import from file	Imports a file and sends the import results to a *user*. This action is equivalent to using the *Import tool* for importing cardholders and credentials. • **Recipient:** Select a user. • **File name:** Opens the Import tool window, where you can select the file that is used to import the data. **NOTE:** Consider the following when using the action in a scheduled task: • If you are using a network path, you must enter it manually and include the full file name of the CSV file, including the suffix. • By default, the CSV source file is automatically deleted after a successful scheduled import; you must generate a new source file for the next scheduled import. • If the import fails, the source CSV file is renamed to include the word "Errors" in the file name. You can use the Windows Event Viewer to see why the import failed.
Ingest event	Saves the event to a system *record type* so you can you can perform correlation queries using the *Unified report* investigation task. • **Role:** Select the Record Caching Service role used to manage the cached data. **NOTE:** The event is stored to a system record type named after the event that triggered this action. Regardless of the event type, the data format for this record type is always as follows: • **Id:** Unique ID of the event. • **Timestamp:** Event timestamp. • **Latitude:** (When available) Latitude. Available on ALPR events and camera events, when the video unit has a geo-location. • **Longitude:** (When available) Longitude. Available on ALPR events and camera events, when the video unit has a geo-location. • **Event type:** Name of the event in English, without spaces. For example, for the *Access denied* event, the value of this field would be "AccessDenied". • **Source entity:** GUID representing the internal ID of the source entity. • **Payload:** Serialized XML version of all event properties and data. The XML string can be exported to an external system if necessary.
Ingest file	Import records from data files through a specified record type. • **Role:** Select the Record Caching Service used to manage the cached data. • **Record type:** Select the record type used to store the cached data. • **Path:** Select the data file to import. If you specify a folder, all data files matching the format of the specified record type are imported. • **Execution timeout:** The maximum time allotted for the execution of the import operation. The system imports the records in batches. If the timeout occurs before the entire operation is complete, only the last batch of inserts that has not yet been committed is rolled back. Set the timeout value to "0" if you do not want the operation to time out. • **Delete files after:** Enable this option to delete the files that are imported successfully. This option prevents you from importing the same file twice.

Action	Description
Ingest from web request	Import records from an external web system through a specified record type. • **Role:** Select the Record Caching Service used to manage the cached data. • **Record type:** Select the record type used to store the cached data. • **URL:** URL of an external web system which returns properly formatted JSON records. • **Execution timeout:** The maximum time allotted for the execution of the import operation. The system imports the records in batches. If the timeout occurs before the entire operation is completed, only the last batch of inserts that has not yet been committed is rolled back. Set the timeout value to "0" if you do not want the operation to time out. • **Request method:** Select either **HTTP GET** (default) or **HTTP POST**. For more information, see HTTP request methods. • **HTTP POST payload:** Enter the payload body of the HTTP POST request. Use it to pass arguments to the external API call. • **Auth header:** The HTTP header needed for authentication to the external system.
Override with event recording quality	Sets the *Boost quality on event recording* to **ON** for the selection camera and applies the custom boost quality recording settings. Selecting this option overrides the general settings for event recording. The effect of this action lasts as long as it is not modified by another action, such as *Recording quality as standard configuration*, or until the Archiver restarts. • **Camera:** Select a camera.
Override with manual recording quality	Sets the *Boost quality on manual recording* to **ON** for the selection camera and applies the custom boost quality recording settings. Selecting this option overrides the general settings for event recording. The effect of this action lasts as long as it is not modified by another action, such as *Recording quality as standard configuration*, or until the Archiver restarts. • **Camera:** Select a camera.
Play a sound	Plays a sound bite in a user or user group's Security Desk. This action is ignored if the user is not running Security Desk. • **User, User group:** Select a user or user group. • **Sound to play:** Sound file (*.wav*) to play. For the user to hear the sound bite, the sound file must be installed on the PC where Security Desk is running. The standard alert sound files that come with the installation are located in *C:\Program files\Genetec Security Center 5.11\Audio*.
Postpone intrusion detection area arming	Postpones the intrusion detection area arming. • **Arming mode:** Either *Master arm* or *Perimeter arm*. • **Intrusion detection area:** Select the intrusion detection area. • **Postpone for:** Set how long to postpone the arming for, in seconds. • **Arming delay:** Set the arming delay in seconds.
Reboot unit	Restarts a unit. • **Entity:** Select a video unit or access control unit to restart.

Action	Description
Recording quality as standard configuration	Cancels the effect of the *Override with manual recording quality* and *Override with event recording quality* actions and restores the standard recording configuration. • **Camera:** Select a camera.
Reset area people count	Resets the people counter in an *area*. • **Area:** Select an area.
Reset external system	Forces the Omnicast™ Federation™ role to reconnect to the remote Omnicast system. • **Role:** Select an Omnicast Federation™ role.
Reset parking zone inventory	Resets the parking zone inventory to zero so that the reported parking zone occupancy can be re-initialized.
Run a macro	Starts the execution of a *macro*. • **Macro:** Select a macro. • **Context:** Specific value settings for the context variables.
Run a pattern	Commands the PTZ camera to run the specified pattern. • **Camera:** Select a PTZ camera. • **Pattern:** Pattern number to run.
Send a message	Sends a pop-up message to a user's Security Desk. This action is ignored if the user is not running Security Desk. • **Recipients:** Select a user or user group. • **Message:** Text to be to displayed in the pop-up message. • **Has timeout:** Select how long the message is shown for.
Send an email	Sends an email to users, cardholders, or specified email addresses. The selected user must have an email address configured, and the mail server must be properly configured for Security Center, or the action is ignored. • **Recipients:** Select a user, user group, cardholder, or cardholder group. • **External Recipients:** This field is available if the user has the *Send an email to cardholders and external recipients* privilege. Enter one or more email addresses for recipients outside of Security Center. Use commas, semi-colons, or new lines to separate multiple addresses. **NOTE:** When saving the action, the external recipients list is saved comma separated on one line. • **Message:** The email text to be sent to the recipient.
Send task	Sends and adds a public task to a Security Desk application. • **Task:** Select a saved public task to send. • **Destination:** Select one of the following: • **User:** All Security Desk connected with that user. • **Monitor:** Specific Security Desk monitor identified by a machine name and a monitor ID.

Action	Description
Set reader mode	Sets the reader mode for accessing doors. - **Location:** Select an area, door, or elevator. - **Reader mode:** Select whether access is granted using *Card and PIN* or *Card or PIN* for the selected area, door, or elevator. This action only works with door controllers and readers that support this feature.
Set the door maintenance mode	Sets the *Unlocked for maintenance* status of a *door* to on or off. - **Door:** Select a door. - **Maintenance:** Desired maintenance mode: on or off.
Set threat level	Sets a threat level on your Security Center system, or on specific areas. - **Area:** Select which areas to set the threat level on. Can be your entire system, or specific areas. - **Threat level:** Select which threat level to set.
Shunt reader	Sets the reader of a door or elevator as **Shunted** or **Active**. - **Location:** Select a door or elevator. - **Reader side:** For door readers, select **Enter**, **Exit**, or **Both sides** as the **Reader side**. - **Reader:** Select whether you want the reader to be **Shunted** or **Active**.
Silence buzzer	Resets the buzzer output defined for a door. This action sets the **Buzzer** option to **None** in the **Hardware** tab of a door in Config Tool. - **Door:** Select a door.
Sound buzzer	Sets the Buzzer output defined for a door. The buzzer sound is specified under the **Buzzer** option in the **Hardware** tab of a door in Config Tool. - **Door:** Select a door.
Start applying video protection	Starts protecting upcoming video recordings against deletion. The protection is applied on all *video files* needed to store the protected *video sequence*. Because no video file can be partially protected, the actual length of the protected video sequence depends on the granularity of the video files. When multiple *Start applying video protection* actions are applied on the same video file, the longest protection period is kept. - **Camera:** Select a camera. - **Keep protected for:** Duration of the video protection. - **Specific:** Sets the protection period in number of days. - **Infinite:** The protection can only be removed manually from the *Archive storage details* task. - **Protect video for next:** Duration of the video to protect. - **Specific:** Sets the duration in minutes and hours. - **Infinite:** All future recordings are protected until the action *Stop applying video protection* is executed.

Action	Description
Start recording	Starts recording on the specified camera. This action is ignored if the camera is not on an active recording schedule. Recordings started by this action cannot be stopped manually by a user. • **Camera:** Select a camera. • **Recording duration:** Sets the duration of the video recording. • **Default:** Sets the duration to follow the value defined in *Default manual recording length* configured for the camera. • **Infinite:** The recording can only be stopped by the *Stop recording* action. • **Specific:** Sets the recording duration in seconds, minutes, and hours.
Start transfer	Starts an archive transfer. • **Transfer group:** Select a transfer group to begin the transfer for. The transfer can consist of retrieving video recordings from units, duplicating video archives from one Archiver to another Archiver, or backing up archives to a specified location.
Stop applying video protection	Stops protecting upcoming video recordings against deletion. This action does not affect the *video archives* that are already protected. • **Camera:** Select a camera. • **Stop in:** Sets the video protection to stop **Now** or in a **Specific** amount of time in minutes and hours.
Stop recording	Stops recording on the specified camera. This action only works if the recording was started by the *Start recording* action. • **Camera:** Select a camera. • **Stop in:** Sets the recording to stop **Now** or in a **Specific** amount of time in seconds, minutes and hours.
Stop transfer	Stops an archive transfer. • **Transfer group:** Select a transfer group to stop the transfer for.
Synchronize role	Starts a synchronization process on the specified role: *Active Directory* or *Global Cardholder Synchronizer*. • **Role:** Select a role that needs synchronization. • **Get image:** (Active Directory role only) Enable this option if image attributes are to be synchronized as well.
Temporarily override unlock schedules	Temporarily locks or unlocks a door for a given period. • **Door:** Select a door. • **Lock mode:** Select *Unlocked* or *Locked*. • **For:** Amount of time in minutes or hours. • **From/To:** Date and time range to unlock the door.

Action	Description
Trigger alarm	Triggers an alarm. This action might generate additional events, depending on the alarm configuration. • **Alarm:** Select an alarm. • **Acknowledgment condition:** Event type that must be triggered before the alarm can be acknowledged. • **User acknowledgment required:** Select whether the alarm must be manually acknowledged, or if it is automatically acknowledged by the system after the acknowledgment condition is cleared.
Trigger intrusion alarm	Triggers a physical alarm on an intrusion detection area. • **Recipient type:** Type of alarm trigger, either the intrusion detection area or a specific alarm input. • **Intrusion detection area:** Select an intrusion detection area.
Trigger output	Triggers an *output behavior* on an output pin of a *unit*. For example, an action can be configured to trigger the output pin of a unit (controller or input/output module). • **Output relay:** Select an output pin (unit). • **Output behavior:** Select the output behavior to trigger.
Trigger past read matching	Triggers the ALPR Manager role to compare new or updated hotlists against previously captured license plate reads.
Unlock door explicitly	Temporarily unlocks a door for five seconds, or the *Standard grant time* configured for that door. • **Door:** Select a door.
Unlock area perimeter doors explicitly	Temporarily unlocks an area's perimeter doors for five seconds, or the *Standard grant time* configured for those doors. • **Area:** Select an area.
Update unit password	Sends password update requests to the selected units through their roles. The passwords are automatically generated by the system. • **Entities:** Add one or more units. **NOTE:** The system does not validate whether the selected units supports password update or not.
Upgrade firmware	Upgrades ALPR unit firmware.

Related Topics

Report Manager configuration tabs on page 1382

Appendices

Appendices

This section includes the following topics:

A

License options

This section includes the following topics:

Viewing license information

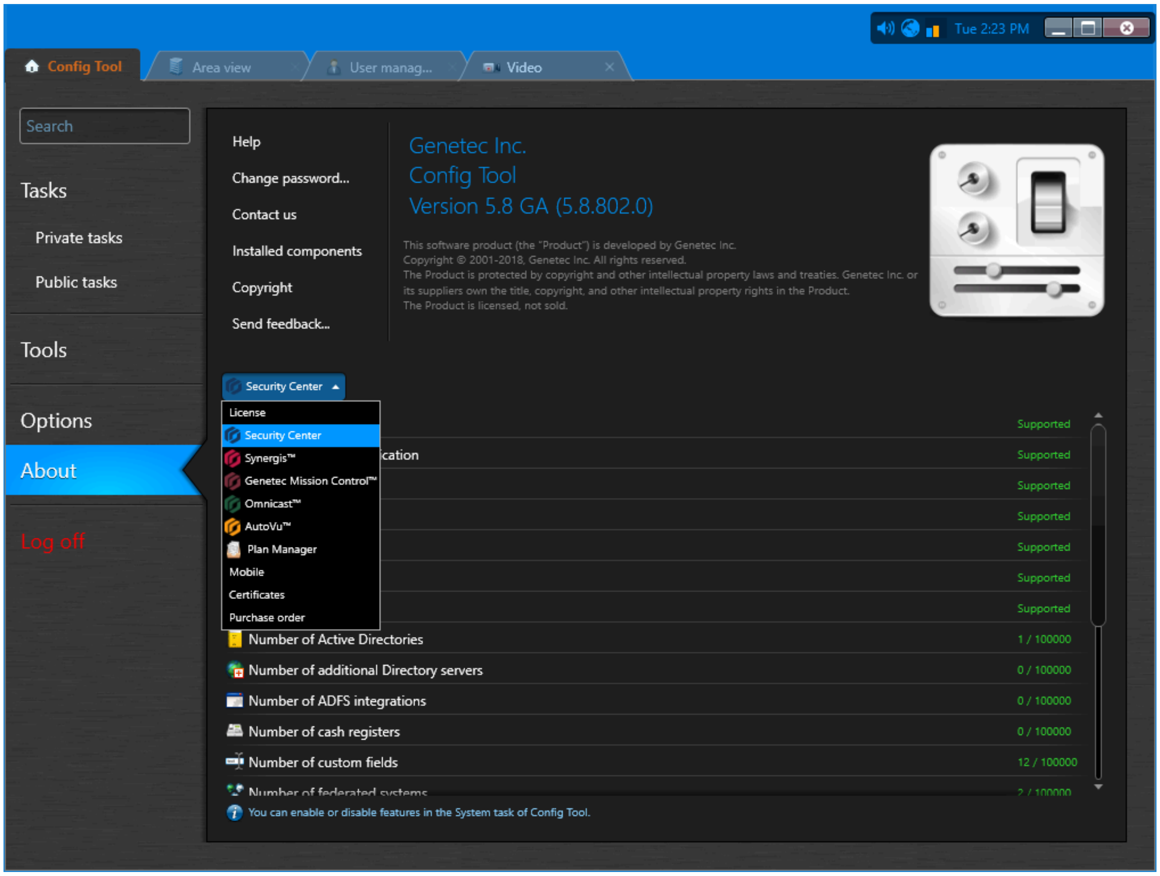
You can view information about your purchased license from the About page in Config Tool or from the Server Admin. This includes information such as your SMA number, license expiration date supported features, and more.

To view license information from Config Tool:

1 Log on to Security Center using Config Tool.

2 From the homepage, click **About**.

If you do not see your license options, maximize the Config Tool window or click the **License** list.



Genetec Inc.
Config Tool
Version 5.8 GA (5.8.802.0)

This software product (the "Product") is developed by Genetec Inc.
Copyright © 2001-2018, Genetec Inc. All rights reserved.
The Product is protected by copyright and other intellectual property laws and treaties. Genetec Inc. or its suppliers own the title, copyright, and other intellectual property rights in the Product.
The Product is licensed, not sold.

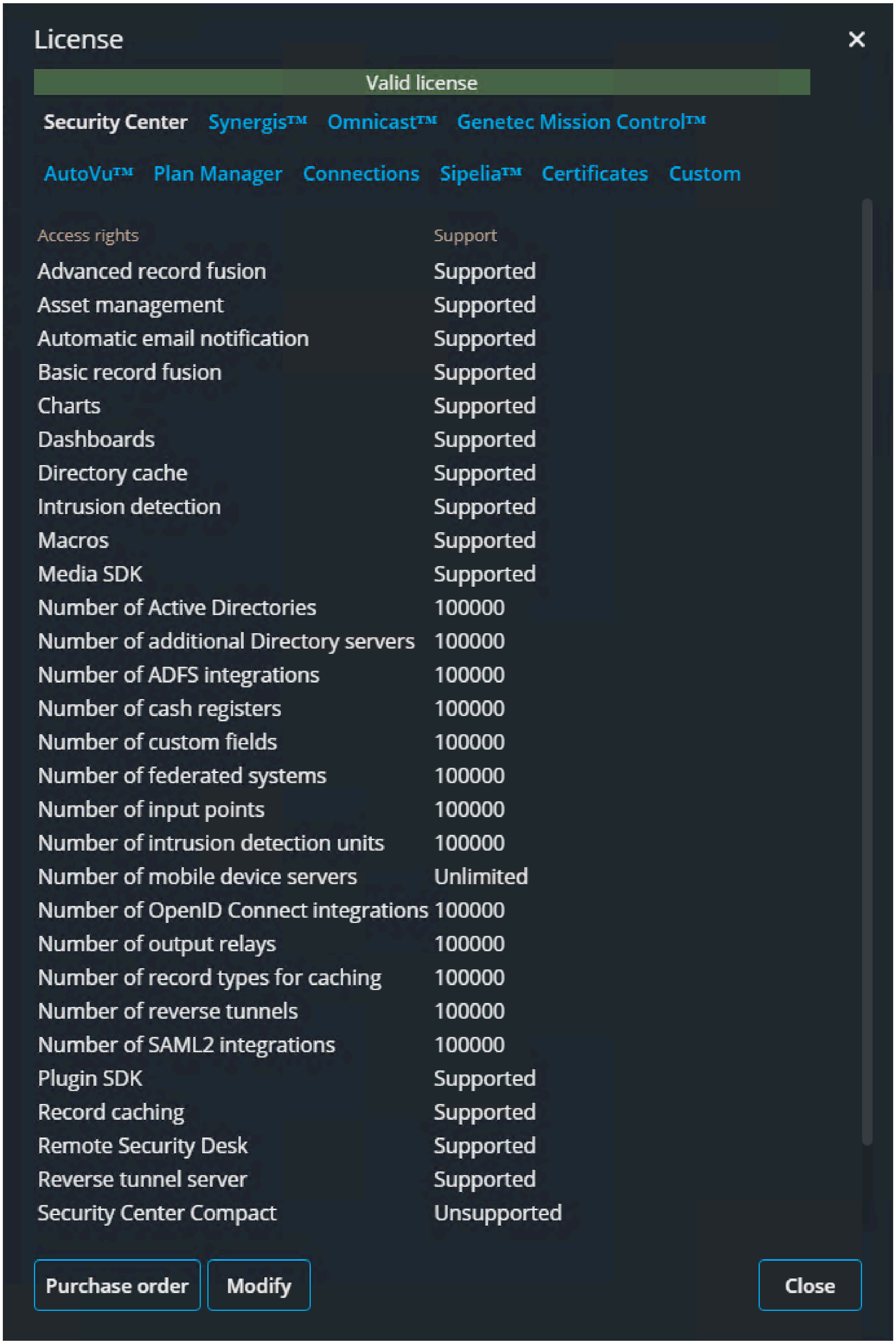
	Supported
ication	Supported
	Supported
	Supported
	Supported
	Supported
	Supported
Number of Active Directories	1 / 100000
Number of additional Directory servers	0 / 100000
Number of ADFS integrations	0 / 100000
Number of cash registers	0 / 100000
Number of custom fields	12 / 100000
Number of federated systems	2 / 100000

You can enable or disable features in the System task of Config Tool.

To view license information from Server Admin:

1 Log on to your main server using Server Admin.

2 In the *License* section of the *Overview* page, click **Details**.



Access rights	Support
Advanced record fusion	Supported
Asset management	Supported
Automatic email notification	Supported
Basic record fusion	Supported
Charts	Supported
Dashboards	Supported
Directory cache	Supported
Intrusion detection	Supported
Macros	Supported
Media SDK	Supported
Number of Active Directories	100000
Number of additional Directory servers	100000
Number of ADFS integrations	100000
Number of cash registers	100000
Number of custom fields	100000
Number of federated systems	100000
Number of input points	100000
Number of intrusion detection units	100000
Number of mobile device servers	Unlimited
Number of OpenID Connect integrations	100000
Number of output relays	100000
Number of record types for caching	100000
Number of reverse tunnels	100000
Number of SAML2 integrations	100000
Plugin SDK	Supported
Record caching	Supported
Remote Security Desk	Supported
Reverse tunnel server	Supported
Security Center Compact	Unsupported

3 Click a license category to view the options under that category.

License options in Security Center

This section describes the meaning of all Security Center license options.

Security Center license options

The generic Security Center license options are the following:

- **Advanced record fusion:** For future use.
- **Asset management:** Allows for the use of asset management add-ons in Security Center. These add-ons enable users to manage and assign access rights to third-party assets, and monitor and report on them in Security Desk.
- **Automatic email notification:** Allows you to set up an email server for email notifications, including:
  - Receiving email notifications from the Watchdog.
  - Using *Send an email* and *Email a report* actions.
- **Basic record fusion:** Enables the Record Fusion Service role and the *Records* investigation task.
- **Charts:** Allows you to generate visual reports.
- **Dashboards:** Allows you to work with custom dashboards.
- **Intrusion detection:** Allows you to use intrusion detection functionality in Security Center, such as adding Intrusion Manager roles and intrusion detection units in Config Tool, and receive intrusion alarms in Security Desk.
- **Macros:** Allows you to create macros in your system.
- **Media SDK:** Allows you to create Media SDK roles.
- **Number of Active Directories:** Maximum number of Active Directory domains that can be synchronized with your system.
- **Number of additional Directory servers:** Maximum number of Directory servers you can have in addition to your main server to set up a high availability system.
- **Number of ADFS integrations:** Maximum number of *identity providers* that can be connected to your system using the WS-Trust and WS-Federation protocols.
- **Number of cash registers:** Maximum number of cash registers that you can import from an external point of sale system.
- **Number of custom fields:** Maximum number of custom fields that you are allowed to define.
- **Number of federated systems:** Maximum number of federated systems allowed, counting both Omnicastâ„¢ 4.x and Security Center systems.
- **Number of input points:** Maximum number of inputs that can be configured for doors, elevators, and zones. Only inputs found on dedicated I/O subpanels such as the HID V200 or the Mercury MR16IN, are counted. The integrated inputs found on controller boards are not counted.
- **Number of intrusion detection units:** Maximum number of intrusion panels supported on your system.
- **Number of mobile device servers:** Maximum number of Mobile Servers allowed on your system.
- **Number of OpenID Connect integrations:** Maximum number of identity providers that can be connected to your system using the OpenID Connect protocol.
- **Number of output relays:** Maximum number of outputs that can be configured for doors, elevators, and zones. Only relays found on dedicated I/O subpanels such as the HID V300 or the Mercury MR16OUT, are counted. The integrated outputs found on controller boards are not counted.
- **Number of record types for caching:** Maximum number of custom record types that you can create in your system. The *Record caching* option must be supported.
- **Number of reverse tunnels:** Maximum number of reverse tunnels you can create on your reverse tunnel server.

- **Number of SAML2 integrations:** Maximum number of identity providers that can be connected to your system using the SAML2 protocol.
- **Plugin SDK:** Allows you to create plugin roles.
- **Record caching:** Allows you to import data from external sources using the Record Caching Service role.
- **Remote Security Desk:** Allows you to remotely monitor and control other Security Desk workstations and monitors, using the *Remote* task on your local Security Desk.
- **Threat level:** Allows you to create threat levels in Config Tool, as well as set threat levels in Security Desk.
- **Web SDK:** Allows you to create Web-based SDK roles.

Synergisâ„¢ license options

The *Synergis*™ access control options are the following:

- **Antipassback:** Allows you to configure areas with antipassback restrictions.
- **Badge template:** Allows you to define badge templates in your system.
- **Card requests:** Allows users to request card credentials to be printed by other users on the system. Also allows you to create request reasons in Config Tool.
- **Import tool:** Allows you to import cardholders and credentials from a flat file.
- **Maximum occupancy:** Allows you to control how many people are in a given area.
- **Number of Mobile Credential Managers:** Maximum number of Mobile Credential Manager instances in your system.
- **Number of Access Managers:** Maximum number of Access Manager roles that can be created on your system.
- **Number of cardholders and visitors:** Maximum number of cardholders and visitors allowed on your system, including those imported from Active Directories.
- **Number of Global Cardholder Synchronizers:** Maximum number of Global Cardholder Synchronizer roles running on *sharing guest* systems that are allowed to connect to the *sharing host* at the same time. This license option is used by the *sharing host* to limit the number of connections.
- **Number of readers:** Maximum number of readers that can be configured for doors and elevators on your system.
- **People counting:** Allows you to use the *People counting* task in Security Desk.
- **Smart card encoding:** Allows you encode smart cards.
- **USB enrollment reader:** Allows you to detect and use USB readers on your system.
- **Visitors:** Allows you to use the *Visitor management* task in Security Desk.

Omnicast license options

The *Omnicast*™ license options are the following:

- **Archiver encryption:** Allows you to encrypt video streams.
- **Audio:** Allows your system to stream audio and enables all audio features on your system.
- **Camera blocking:** Allows you to block video from other users on the system.
- **Edge recording:** Enables the capability to transfer data from edge recording units to the Archiver.
- **Forensic search:** Enables the *Forensic search* task in Security Desk.
- **Hardware acceleration:** Allows you to use the hardware acceleration feature for video decoding.
- **Number of Auxiliary Archivers:** Number of Auxiliary Archiver roles allowed on your system.
- **Number of cameras and analog monitors:** Maximum number of cameras and analog monitors allowed on your system. Cameras and analog monitors managed locally by your system and those federated from remote systems are counted. Cameras and analog monitors are also cumulative. For example, if you use 5 cameras and 5 analog monitors simultaneously, they will count for 10 entities in the license.

- **Number of CCTV keyboards:** Number of CCTV keyboards allowed on your system.
- **Number of DVR inputs:** Number of video inputs from DVRs (digital video recorders) allowed on your system.
- **Number of integrity-monitored cameras:** Maximum number of cameras (both native and federated) that can be monitored for tampering.
- **Number of Media Gateway RTSP streams:** Maximum number of video streams that can be requested simultaneously from the Media Gateway role.
- **Number of OVReady cameras:** Maximum number of OVReady cameras (with *video analytics* capabilities) allowed on your system.
- **Number of panoramic cameras:** Number of panoramic cameras allowed on your system.
- **Number of privacy-protected streams:** Number of privacy-protected video streams allowed on your system.
- **Number of promotional cameras:** Number of video channels allowed on your system according to a commercial promotion available at the time of purchase. Video units eligible for such a promotion are using these promotional licenses first. For example, if you purchase camera connections when a promotion applies, the next eligible cameras you add to your system will use the promotional camera licenses up to the limit of *Number of promotional cameras*. When this limit is reached, the next eligible cameras added will use regular camera connections. This applies to the current *Analog Camera Promotion*.
- **Number of restricted cameras:** Number of *restricted cameras allowed* on your system. Restricted cameras also require a regular camera license. To view a list of manufacturers that require a restricted license, use the **Restricted** *License Type* filter on the Supported Device List.
- **Number of standby Archiver servers:** Total number of standby servers assigned to Archiver roles in the system.

Genetec Mission Controlâ„¢ license options

For the *Genetec Mission Control*™ license options, see the Mission Control Ordering Guide.

AutoVuâ„¢ license options

The *AutoVu*™ ALPR license options are the following:

- **Geocoder:** Type of map engine used by the ALPR Manager for geocoding *BeNomad*.
- **Number of endpoints for the AutoVuâ„¢ Data Exporter:** Maximum number of external endpoints supported by your system to securely export ALPR events.
- **Number of fixed Sharp analytic streams:** Maximum number of fixed Sharp units allowed on your system.
- **Number of JSON2 endpoints for the AutoVuâ„¢ Data Exporter:** Maximum number of external JSON2 endpoints supported by your system to securely export ALPR events.
- **Number of LPR Managers:** Maximum number of LPR Manager roles allowed on your system.
- **Number of parking zones:** Maximum number of physical parking lots that can be managed in Security Center using AutoVuâ„¢ Free-Flow.
- **Number of Patrollers - City Parking Enforcement:** Maximum number of Patrollers configured for City Parking Enforcement allowed on your system.
- **Number of Patrollers - Law Enforcement:** Maximum number of Patrollers configured for Law Enforcement allowed on your system.
- **Number of Patrollers - MLPI:** Maximum number of Patrollers configured for Mobile License Plate Inventory allowed on your system.
- **Number of Patrollers - University Parking Enforcement:** Maximum number of Patrollers configured for University Parking Enforcement allowed on your system.

- **Number of Patrollers equipped with maps:** Maximum number of Patrollers equipped with maps allowed on your system.
- **Security Desk map:** Type of map engine supported in Security Desk: *Bing* or *BeNomad*.
- **XML import:** Allows you to import data from third-party applications.

Plan Manager options

The Plan Manager license is required to use maps in Security Center. The Map Manager role replaced the Plan Manager role in Security Center 5.4 GA. The license options are as follows:

- **Plan Manager Advanced:** Allows you to use maps in Advanced mode.
- **Plan Manager ArcGIS:** Allows you to use ArcGIS maps.
- **Plan Manager Basic:** Allows you to use maps in Basic mode.
- **Plan Manager Standard:** Allows you to use maps in Standard mode.

Connection options

- **Number of mobile devices:** Maximum number of simultaneous Mobile app connections allowed on your system.
- **Number of Security Desk connections:** Maximum number of simultaneous Security Desk connections allowed on your system.
- **Number of Genetecâ„¢ Web App and Web Client connections:** Maximum number of Genetec Web App and Web Client connections allowed on your system.

Certificate license options

The certificate license options. Each certificate is identified by an application or plugin name and the publisher name. The option specifies the maximum number of simultaneous connections from each type of application allowed on your system.

B

Default Security Center ports

This section includes the following topics:

Ports used by core applications in Security Center

The following table lists the default network ports that must be opened to allow proper communication between the core applications and services in Security Center.

For a visual representation of the ports, see the *Security Center Network Diagram - Platform*.

IMPORTANT: Exposing Security Center to the Internet is strongly discouraged without hardening your system first. Before exposing your system, implement the advanced security level described in the *Security Center Hardening Guide* to help protect your system from Internet threats. Alternatively, use a trusted VPN for remote connections.

Port usage	Inbound port	Outbound port	Protocol	Executable file
Directory				
Client and server connections	TCP 5500	TCP 5500	TLS 1.2	SecurityDesk.exe ConfigTool.exe
Config Tool				
Genetec™ Server/Directory communication		TCP 5500	TLS 1.2	GenetecServer.exe
Map download requests to Map Manager		TCP 8012	HTTPS	GenetecMapManager.exe
• Authentication role communication • Communication with GTAP for Genetec™ Advantage validation and feedback		TCP 443	HTTPS TLS 1.2	ConfigTool.exe
Security Desk				
Genetec™ Server/Directory communication		TCP 5500	TLS 1.2	GenetecServer.exe
Map download requests to Map Manager		TCP 8012	HTTPS	GenetecMapManager.exe
Authentication role communication		TCP 443	HTTPS TLS 1.2	SecurityDesk.exe
SDK				
Genetec™ Server/Directory communication		TCP 5500	TLS 1.2	GenetecServer.exe
Map download requests to Map Manager		TCP 8012	HTTPS	GenetecMapManager.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
All roles				
Genetec™ Server/Directory communication **NOTE:** Previously port 4502. If port 4502 was the server port before upgrading from 5.3 or earlier, 4502 remains the server port after the upgrade.	TCP 5500	TCP 5500	Genetec Inc. proprietary protocol	GenetecServer.exe
REST/Server Admin communication[1]	TCP 80	TCP 80	HTTP	GenetecInterface.exe
Secured REST/Server Admin/Authentication role communication[1]	TCP 443	TCP 443	HTTPS	GenetecInterface.exe
Outgoing connections to the SQL Database Engine hosted on another server. Only required for roles that must connect to a database on another server. Not required if SQL Server is running on the same machine or if the role has no database.		TCP 1433	Microsoft Tabular Data Stream Protocol (TDS)	Role-dependent
Outgoing connections to the SQL Server Browser service for SQL Server connection information. Only required for roles that must connect to a named database instance on another server. Not required for roles configured to connect to their database using a specific port.		UDP 1434	Microsoft SQL Server Resolution Protocol (SSRP)	Role-dependent
Map Manager				
Requests for map download from client applications[1]	TCP 8012		HTTPS	GenetecMapManager.exe
Mobile Server				

Port usage	Inbound port	Outbound port	Protocol	Executable file
Communication from mobile clients	TCP 443		HTTPS	GenetecMobileRole.exe GenetecMobileAgent.exe
Communication from Archiver for video streaming and storage	TCP 9000-10000		HTTP	GenetecMobileRole.exe GenetecMobileAgent.exe
Record Caching Service				
REST/Server Admin communication[1]	TCP 80	TCP 80	HTTP	GenetecIngestion.exe
Secured REST/Server Admin/Authentication role communication[1]	TCP 443	TCP 443	HTTPS	GenetecIngestion.exe
Unit Assistant				
Communication with Archiver roles	TCP 5500	TCP 5500	Genetec Inc. proprietary protocol	GenetecUnitAssistantRole.exe
Wearable Camera Manager				
Configurable in the UI		TCP 48830	Genetec Clearance™ protocol	GenetecBwcManagerRole.exe
Configurable in a config file		TCP 48831, 48832, 48833	Clearance protocol	GenetecBwcAgentService.exe
Web Server				
Initial connection between server hosting Web Server role and browser used for Web Client **NOTE:** Redirected to HTTPS port after initial connection.	TCP 80	TCP 80	HTTP	GenetecWebClient.exe
• Connection between server hosting Web Server role and browser used for Web Client • Secured REST/Server Admin/Authentication role communication[1]	TCP 443	TCP 443	HTTPS	GenetecWebClient.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Web Client video requests to Media Gateway		TCP 443	HTTPS	GenetecWebClient.exe
Genetec Web App video requests to Media Gateway		TCP 443	HTTPS	Genetec.WebApp.Console.exe
Genetec™ Update Service (GUS)				
GUS Sidecar requires port TCP 4596 to communicate with the GUS on the same machine. Sidecar ports are not used outside of the local machine.			N/A	GenetecUpdaterService.Sidecar.exe
Deprecated. Formerly used to access the GUS web page. Redirects to TCP 4595 in the latest GUS version[1]	TCP 4594		N/A	GenetecUpdateService.exe
Secure communication with the GUS web page, and other GUS servers[1]	TCP 4595	TCP 4595	HTTPS	GenetecUpdateService.exe
Communication with Microsoft Azure and Genetec Inc.[1]	TCP 443	TCP 443	HTTPS	GenetecUpdateService.exe GenetecUpdaterService.Sidecar.exe
SQL Server				
Incoming connections to the SQL Database Engine from roles on other servers	TCP 1433		Microsoft Tabular Data Stream Protocol (TDS)	sqlservr.exe
Incoming connections to the SQL Server Browser service for SQL Server connection information	UDP 1434		Microsoft SQL Server Resolution Protocol (SSRP)	sqlbrowser.exe
System Availability Monitor Agent (SAMA)				
Legacy port for communication with Security Center servers[1]		TCP 4592	HTTP	Genetec.HealthMonitor.Agent.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Communication with Security Center servers[1]		TCP 443	HTTPS	Genetec.HealthMonitor.Agent.exe
Connection to the Health Service in the Cloud[1]		TCP 443	HTTPS	Genetec.HealthMonitor.Agent.exe

[1] These ports use Windows System components to handle HTTP requests. Microsoft components using http.sys require the following rule: *dir="in" protocol="6" lport="<SPECIFY PORT USED HERE: CAN BE 80, 443, or CUSTOM>" binary="System"*.

Ports used by AutoVu applications in Security Center

The following tables lists the default network ports that must be opened to allow proper communication between Security Center and external AutoVu™ components when AutoVu is enabled in your system.

For a visual representation of the ports, see the *Security Center Network Diagram - ALPR*.

IMPORTANT: Exposing the AutoVu system to the internet is strongly discouraged without hardening your system first. Before exposing your system, implement the advanced security level described in the *Security Center Hardening Guide* to help protect your system from Internet-based threats.

Port usage	Inbound port	Outbound port	Protocol	Executable file
Sharp unit				
SSH port for SharpOS 14 (optional)	TCP 22		HTTP	Sharp unit
Video port (Security Center extension HTTP) Communication port (HTTP for SharpOS 12.7 and lower)	TCP 80		HTTP	Sharp unit
Secure port (LPM protocol, video, Genetec protocol)	TCP 443		HTTPS	Sharp unit
RTSP video requests	TCP 554 UDP 554		RTSP	Sharp unit
Appliance discovery service	UDP 2728		UDP	Sharp unit
RDP access port (optional)	TCP 3389		TCP	Sharp unit
Silverlight ports and image feed service (for Sharp models earlier than SharpV)	TCP 4502-4534		HTTP	Sharp unit
Control port (Mobile installation)	TCP 4545		HTTP	Sharp unit
Discovery port	UDP 5000		UDP	Sharp unit
Control port (Fixed installation)	TCP 8001		HTTP	Sharp unit
Cloud (PIP)		TCP 443	PIP	Sharp unit
Syslog (on demand)		UDP 514		Sharp unit

Port usage	Inbound port	Outbound port	Protocol	Executable file
LPM protocol communication		TCP 10001	HTTPS	Sharp unit
Extensions				
FTP file upload. Only used when the FTP extension is configured.		TCP 21	FTP	Sharp unit
HTTP file upload. Only used when the HTTP extension is configured.		Any port	HTTP\HTTPS	Sharp unit
ALPR Manager				
Genetec Patroller™ communication and fixed Sharp units (not used for **LPM protocol** connections)	TCP 8731		HTTP	GenetecLicensePlateManager.exe
LPM protocol listening port	TCP 10001		HTTPS	GenetecLicensePlateManager.exe
Secure communication port for DataExporter		TCP 443	HTTPS	GenetecLicensePlateManager.exe
Fixed Sharp unit discovery		UDP 5000	N/A	GenetecLicensePlateManager.exe
RabbitMQ communication port when used by DataExporter (optional)		TCP 5671	HTTPS	GenetecLicensePlateManager.exe
Sharp control port (used for **Live** connections, not **LPM protocol** connections)		TCP 8001	HTTP	GenetecLicensePlateManager.exe
Communication with Pay-by-Plate Sync plugin		TCP 8787	HTTP	GenetecLicensePlateManager.exe
		TCP 8788	HTTPS	GenetecLicensePlateManager.exe
Archiver[1]				
Default Media Router RTSP port	TCP 554		RTSP	GenetecArchiverAgent32.exe
Default Archiver port	TCP 555		RTSP	GenetecArchiverAgent32.exe
Patroller (in-vehicle computer)				

Port usage	Inbound port	Outbound port	Protocol	Executable file
Communication with mobile Sharp units	TCP 4545		HTTP	Patroller.exe
Time synchronization service for Sharp units	TCP 4546		SNTP	Patroller.exe
Communication with Simple Host	TCP 8001		HTTP	Patroller.exe
Communication with Pay-by-Plate Sync plugin	TCP 8787		HTTP	Patroller.exe
Communication with Curb Sense and Plate Link		TCP 443	HTTPS	Patroller.exe
Communication with mobile Sharp units		TCP 4545	HTTPS	Patroller.exe
Sharp camera discovery		UDP 5000	UDP	Patroller.exe PatrollerConfigTool.exe
ALPR Manager connection		TCP 8731	HTTP and message-level encryption	Patroller.exe
Pay-by-Plate Sync				
Communication with Free-Flow and Patroller	TCP 8787		HTTP	GenetecPlugin.exe for Pay-by-Plate Sync
Secure communication with Free-Flow	TCP 8788		HTTPS	GenetecPlugin.exe for Pay-by-Plate Sync
Communication with Free-Flow and Patroller		TCP 8787	HTTP	GenetecPlugin.exe for ALPR Manager
Secure communication with Free-Flow		TCP 8788	HTTPS	GenetecPlugin.exe for ALPR Manager

[1] You can also add a SharpV to Security Center as a standard video unit using separate Archiver and Media Router roles. For more information on adding a video unit, see Ports used by Omnicast applications in Security Center on page 1460.

Ports used by Omnicast applications in Security Center

The following table lists the default network ports that must be opened to allow proper communication between Security Center and external IP video devices when Omnicast™ is enabled in your system.

For a visual representation of the ports, see the *Security Center Network Diagram - Video*.

.

IMPORTANT: Exposing Security Center to the Internet is strongly discouraged without hardening your system first. Before exposing your system, implement the advanced security level described in the *Security Center Hardening Guide* to help protect your system from Internet threats. Alternatively, use a trusted VPN for remote connections.

Port usage	Inbound port	Outbound port	Protocol	Executable file
Archiver				
Communication with Cloud Storage		TCP 80[4], 443[4]	HTTPS TLS 1.2	GenetecArchiverAgent32.exe
Communication between the Archiver and the Media Router to announce content		TCP 554	RTSP over TLS when secure communication enabled	GenetecArchiverAgent32.exe
Live and playback stream requests	TCP 555[1]		RTSP over TLS when secure communication enabled	GenetecArchiverAgent32.exe
Edge playback stream requests	TCP 605[1]		RTSP	GenetecVideoUnitControl32.exe
Mobile device streaming through the Mobile Server		TCP 9000-10000	HTTP	GenetecVideoUnitControl32.exe
Communication between the primary Archiver and failover servers	TCP 5500	TCP 5500	TLS 1.2	GenetecArchiver.exe GenetecArchiverAgent32.exe GenetecVideoUnitControl32.exe
Telnet console connection requests	TCP 5602[1]		Telnet	GenetecArchiverAgent32.exe
Audio from client applications	UDP 6000-6500		RTP	GenetecVideoUnitControl32.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Live unicast streaming from IP cameras	UDP 15000–19999[2]		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecVideoUnitControl32.exe
Live video and audio multicast streaming	UDP 47806, 47807	UDP 47806, 47807	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecArchiverAgent32.exe GenetecVideoUnitControl32.exe
Vendor-specific ports for cameras	TCP & UDP	TCP Common ports include: • TCP 80 • TCP 443 • TCP 554 • TCP 322	• TCP 80: HTTP • TCP 443: HTTPS • TCP 554: RTSP • TCP 322: RTSP over TLS when secure communication enabled	GenetecVideoUnitControl32.exe
Redirector				
Live and playback stream requests	TCP 560		RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Communication with Media Router (Security Center Federation™)		TCP 554	RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Communication with Archiver		TCP 555	RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Communication with Auxiliary Archiver		TCP 558	RTSP over TLS when secure communication enabled	GenetecRedirector.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Cloud playback requests		TCP 570[4]	RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Edge playback stream requests		TCP 605	RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Communication with Privacy Protector™		TCP 754	RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Stream requests to other redirectors		TCP 560	RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Media transmission to client applications	TCP 960[3]	UDP 6000-6500 TCP 960[3]	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecRedirector.exe
Media transmission to other redirectors	UDP 8000–12000	UDP 8000–12000	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecRedirector.exe
Live video and audio multicast streaming	UDP 47806, 47807	UDP 47806, 47807	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecRedirector.exe
Live video multicast streaming (Security Center Federation™)	UDP 65246	UDP 65246	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecRedirector.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Auxiliary Archiver				
Live and playback stream requests	TCP 558		RTSP over TLS when secure communication enabled	GenetecAuxiliaryArchiver.exe
Unicast media streams	UDP 6000-6500		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecAuxiliaryArchiver.exe
Live video and audio multicast streaming	UDP 47806, 47807		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecAuxiliaryArchiver.exe
Live video multicast streaming (Security Center Federation™)	UDP 65246		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecAuxiliaryArchiver.exe
Live stream requests		TCP 554, 555, 560	RTSP over TLS when secure communication enabled	GenetecAuxiliaryArchiver.exe
Media transmission		TCP 960[3]	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecAuxiliaryArchiver.exe
Cloud Playback				
Live and playback video requests from within Security Center	TCP 570		RTSP over TLS when secure communication enabled	GenetecCloudPlaybackRole.exe GenetecCloudPlaybackAgent.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Communication with Cloud Storage		TCP 80, 443	TLS 1.2	GenetecCloudPlaybackRole.exe GenetecCloudPlaybackAgent.exe
Media Router				
Live and playback stream requests, and announce requests	TCP 554		RTSP over TLS when secure communication enabled	GenetecMediaRouter.exe
Federated Media Router stream requests		TCP 554	RTSP over TLS when secure communication enabled	GenetecMediaRouter.exe
Media Gateway				
Live and playback stream requests from RTSP clients	TCP 654		RTSP over TLS when secure communication enabled	Genetec.MediaGateway.exe
Incoming stream requests from mobile and web clients	TCP 80, 443		• TCP 80: HTTP • TCP 443: HTTPS	Genetec.MediaGateway.exe
Communication between the Media Gateway agents and the Media Gateway role	TCP 5500	TCP 5500	TLS 1.2	Genetec.MediaGateway.exe
Live video unicast streams	UDP 6000-6500		SRTP when using encryption *in transit and at rest*	Genetec.MediaComponent32.exe
Live video and audio multicast streaming	UDP 47806, 47807	UDP 51914	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	Genetec.MediaComponent32.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Live video multicast streaming (Security Center Federation™)	UDP 65246		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	Genetec.MediaComponent32.exe
Live and playback video requests		TCP 554, 555, 558, 560, 605	RTSP over TLS when secure communication enabled	Genetec.MediaComponent32.exe
Media transmission		TCP 960[3]	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecAuxiliaryArchiver.exe
Cloud playback requests		TCP 570[4]	RTSP over TLS when secure communication enabled	Genetec.MediaComponent32.exe
Omnicast Federation™				
Connection to remote Omnicast 4.x systems.		TCP 5001-5002	TCP	GenetecOmnicastFederation32.exe
Security Center Federation™				
Connection to remote Security Center systems		TCP 5500	TLS 1.2	GenetecSecurityCenterFederation.exe
Security Desk				
Unicast media streams	UDP 6000–6200		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	SecurityDesk.exe Genetec.MediaComponent32.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Live video and audio multicast streaming	UDP 47806, 47807		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	SecurityDesk.exe Genetec.MediaComponent32.exe
Live video multicast streaming (Security Center Federation™)	UDP 65246		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	SecurityDesk.exe Genetec.MediaComponent32.exe
Live and playback video and audio requests		TCP 554, 555, 558, 560, 605	RTSP over TLS when secure communication enabled	SecurityDesk.exe Genetec.MediaComponent32.exe
Media transmission		TCP 960[3]	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	SecurityDesk.exe Genetec.MediaComponent32.exe
Cloud playback requests		TCP 570[4]	RTSP over TLS when secure communication enabled	SecurityDesk.exe Genetec.MediaComponent32.exe
Config Tool				
Unicast media streams	UDP 6000–6200		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	ConfigTool.exe Genetec.MediaComponent32.exe
Live video and audio multicast streaming	UDP 47806, 47807		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	ConfigTool.exe Genetec.MediaComponent32.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Live video multicast streaming (Security Center Federation™)	UDP 65246		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	ConfigTool.exe Genetec.MediaComponent32.exe
Live video and audio requests		TCP 554, 555, 560	RTSP over TLS when secure communication enabled	ConfigTool.exe Genetec.MediaComponent32.exe
Media transmission		TCP 960[3]	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	ConfigTool.exe Genetec.MediaComponent32.exe
Unit discovery with the Unit enrollment tool		Vendor-specific TCP and UDP ports	Vendor-specific	ConfigTool.exe Genetec.MediaComponent32.exe
Cloud Storage reporting and configuration		TCP 80[4], 443[4]	HTTP	ConfigTool.exe

[1] Applies to servers hosting one Archiver role. If multiple Archiver roles are hosted on the same server, each additional role uses the next free port.

[2] You can have multiple Archiver agents on the same server. Each Archiver agent assigns a unique UDP port to each video unit it controls. To ensure that the UDP port assignment on a server is unique, each additional Archiver agent on the same server adds 5000 to its starting UDP port number. For example, the first Archiver agent uses ports 15000-19999, the second one uses ports 20000-24999, the third one uses ports 25000-29999, and so on.

NOTE: You can manually assign live streaming reception UDP ports from the **Resource** tab of the Archiver role.

[3] TCP port 960 applies to new installations of Security Center 5.8 and later. In Security Center 5.6 and 5.7, TCP port 5004 was used instead of TCP port 960. Therefore, any system upgraded to 5.11 through 5.6 or 5.7 continues to use TCP port 5004.

[4] In the context of Cloud Storage, ports TCP 80, 443, and 570 are only used when Cloud Storage is enabled.

Related Topics

Archiver: Resources tab on page 1344

Ports used by KiwiVision modules in Security Center

The following tables list the default network ports that must be opened to allow proper communication between Security Center and external IP video devices when KiwiVision™ is enabled in your system.

For a visual representation of the ports, see the *Security Center Network Diagram - KiwiVision*.

IMPORTANT: Exposing Security Center to the Internet is strongly discouraged without hardening your system first. Before exposing your system, implement the advanced security level described in the *Security Center Hardening Guide* to help protect your system from Internet threats. Alternatively, use a trusted VPN for remote connections.

KiwiVision Privacy Protector™ and KiwiVision Camera Integrity Monitor modules

Port usage	Inbound port	Outbound port	Protocol	Executable file
Live video requests	TCP 754		RTSP over TLS when using Secure communication	Genetec.MediaProcessor.exe
Live video unicast streams	UDP 7000-7500		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	Genetec.MediaProcessor.exe
Live video multicast streaming	UDP 47806	UDP 47806	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	Genetec.MediaProcessor.exe
Live video multicast streaming (Security Center Federation™)	UDP 65246	UDP 65246	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	Genetec.MediaProcessor.exe
Live video requests		TCP 554, 555, 560	RTSP over TLS when using Secure communication	Genetec.MediaProcessor.exe
Media transmission		TCP 960[1]	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	Genetec.MediaProcessor.exe

KiwiVision Security video analytics and KiwiVision People Counter modules

Port usage	Inbound port	Outbound port	Protocol	Executable file
KiwiVision Manager				
Communication with KiwiVision Manager database		TCP 1433	Microsoft Tabular Data Stream Protocol (TDS)	GenetecPlugin.exe
		UDP 1434	Microsoft SQL Server Resolution Protocol (SSRP)	GenetecPlugin.exe
KiwiVision Analyzer				
Live video unicast streams	UDP 6000–6500		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecPlugin.exe
Live video multicast streaming	UDP 47806	UDP 47806	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecPlugin.exe
Live video multicast streaming (Security Center Federation™)	UDP 65246	UDP 65246	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecPlugin.exe
Live and playback video requests		TCP 554, 560, 960[1]	RTSP over TLS when using Secure communication	GenetecPlugin.exe
Communication with KiwiVision Manager database		TCP 1433	Microsoft Tabular Data Stream Protocol (TDS)	GenetecPlugin.exe
		UDP 1434	Microsoft SQL Server Resolution Protocol (SSRP)	GenetecPlugin.exe
SQL Server				

Port usage	Inbound port	Outbound port	Protocol	Executable file
Incoming connections to the SQL Database Engine from KiwiVision Manager and Analyzer roles on other servers	TCP 1433		Microsoft Tabular Data Stream Protocol (TDS)	sqlservr.exe
Incoming connections to the SQL Server Browser service for SQL Server connection information	UDP 1434		Microsoft SQL Server Resolution Protocol (SSRP)	sqlbrowser.exe

[1] TCP port 960 applies to new installations of Security Center 5.8 and later. In Security Center 5.6 and 5.7, TCP port 5004 was used instead of TCP port 960. Therefore, any system upgraded to 5.11 through 5.6 or 5.7 continues to use TCP port 5004.

Ports used by Synergis applications in Security Center

The following table lists the default network ports that must be opened to allow proper communication between Security Center and external IP access control devices when Synergis™ is enabled in your system.

For a visual representation of the ports, see the *Security Center Network Diagram - Access control*.

IMPORTANT: Exposing Security Center to the Internet is strongly discouraged without hardening your system first. Before exposing your system, implement the advanced security level described in the *Security Center Hardening Guide* to help protect your system from Internet threats. Alternatively, use a trusted VPN for remote connections.

Port usage	Inbound port	Outbound port	Protocol	Executable file
Access Manager				
Synergis extension - discovery		UDP 2000	Genetec Inc. proprietary protocol	GenetecAccessManager.exe
Secure communication with Synergis units and HID units		TCP 443	HTTPS TLS 1.2	GenetecAccessManager.exe
HID extension - FTP data and command[1]	TCP 20	TCP 21	FTP	GenetecAccessManager.exe
HID extension - SSH[1]		TCP 22	SSH	GenetecAccessManager.exe
HID extension - Telnet[1]		TCP 23	Telnet	GenetecAccessManager.exe
HID extension - HTTP communication		TCP 80	HTTP	GenetecAccessManager.exe
HID extension - VertX OPIN protocol		TCP 4050/4433[2]	• TCP 4050: Proprietary • TCP 4433: HTTPS TLS 1.2	GenetecAccessManager.exe
HID extension - VertX discovery[3]	UDP 4070	UDP 4070	N/A	GenetecAccessManager.exe
Remote syslog server[4]	UDP 514		N/A	GenetecAccessManager.exe
Global Cardholder Synchronizer				
Connection to sharing host		TCP 5500	TLS 1.2	GenetecGlobalCardholderManagement.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Mobile Credential Manager				
Secure communication (HTTPS) with the portal of the mobile credential provider **NOTE:** Security Desk, Config Tool, and the Mobile Credential Manager role all need access to the following URLs: https://api.origo.hidglobal.com https://ma.api.assaabloy.com/credential-management/		TCP 443	HTTPS TLS 1.2	GenetecMobileCredentialManager.exe

[1] Not used if HID units are configured with **Secure mode**. As a best practice, enable secure mode on all HID units.

[2] Legacy HID units or EVO units running a firmware version earlier than 3.7 use port 4050. HID EVO units running in secure mode with firmware 3.7 and later user port 4433.

[3] The discovery port of an HID unit is fixed at 4070. After it is discovered, the unit is assigned to an Access Manager that uses the ports shown in the previous table to control it.

For more information about initial HID hardware setup, download the documentation from http://www.HIDglobal.com.

[4] Starting in Security Center 5.10.1.0, this port is no longer enabled by default.

C

HID reference

This section includes the following topics:

Supported HID hardware

HID Global has two product lines. The newer product line is called EVO, and the older one is called Legacy. There are two product families in each product line: VertX and Edge. Products from different families cannot mix. Security Center supports them all.

About HID controllers

The Access Manager communicates directly with HID controllers over an IP network. Therefore, all HID controllers are called *access control units* in Security Center. For more information, refer to HID documentation.

Platform differences between EVO and Legacy

Characteristics	EVO	Legacy
Processor / Speed	ARM9 / 200 Mips	ETRAX / 100 Mips
RAM	64 MB	32 MB
Operating system	Linux 2.6	Linux 2.4
Secure shell and protocol	Yes	No
Maximum event buffer	99,999	5,000

Limitations

On a *Card and PIN* door controlled by an HID Edge EVO unit, if a host lookup is necessary (an unknown credential is entered and the unit must query the Access Manager before making a decision), the cardholder must wait a few seconds after presenting their card, before entering their PIN. Entering the PIN too quickly might result in a denied access because the first few digits of the PIN might not have been registered by the unit.

Supported HID VertX controllers

HID has two lines of VertX controllers: EVO (newer) and Legacy. The newer line of controllers have significantly more processing power and memory than the older line. Both lines of controllers use the same interface modules (V100, V200, V300) that remain unchanged.

In the following tables, we compare the characteristics of the EVO controllers with that of their Legacy counterparts. For more information, refer to HID documentation.

VertX platform differences between EVO and Legacy

Characteristics	EVO	Legacy
Flash memory	256 MB	8 MB
Maximum cardholder capacity	250,000	44,000
Offline cardholder capacity with Security Center[1]	65,000[2]	22,000[2, 3]
Power supply[4]	12 – 24 VDC	12 – 18 VDC
Operating temperature range	32 ° – 120 ° F (0 ° – 49 ° C)	32 ° – 122 ° F (0 ° – 50 ° C)
Humidity tolerance	5% to 85% non-condensing	5% to 95% non-condensing

[1] In Security Center, a cardholder can have multiple credentials. A cardholder with two credentials is counted as two by HID.

[2] With Security Center, the unit's cardholder capacity is lower than its maximum cardholder capacity. This is partly because extra memory is used as cache to allow unit synchronization to be performed without affecting normal operation.

[3] Up to 125,000 credentials with full memory upgrade.

[4] VertX V1000 EVO and Legacy and V2000 EVO and Legacy are non-PoE devices. Do not connect J1 (Ethernet port) to a PoE-capable port. If you must connect these controllers to a PoE-capable port, make sure to disable the power of the PoE port before connecting.

VertX V1000 differences between EVO and Legacy

Characteristics	EVO	Legacy
Maximum current at 12 – 24 VDC per unit	1 A	1 A
Average operating current at 12 VDC	210 mA	140 mA
Downstream device capacity[4]	Up to 32 interface modules (or 64 readers)	Up to 32 interface modules (or 64 readers)
Downstream device compatibility	VertX V100, V200, V300	VertX V100, V200, V300
RTC backup	Coin cell battery	Coin cell battery

Characteristics	EVO	Legacy
RS-232 ports	1	2
USB ports	1 (reserved for future use)	0

[4] HID states that a V1000 controller can support a maximum of 32 downstream interface modules (16 on each RS-485 serial bus). However, the performance tests run by Genetec Inc. indicate that as a “best practice”, 20 downstream interface modules should not be exceeded (10 per serial bus).

VertX V2000 differences between EVO and Legacy

Characteristics	EVO	Legacy
Maximum current at 12 – 24 VDC per unit	1 A	1 A
Average operating current at 12 VDC (0 reader)	125 mA	160 mA
Average operating current at 12 VDC (2 readers)	625 mA	660 mA
Relay outputs	30 VDC, 2 A	30 VDC, 2 A

Supported HID VertX sub-panels

The HID VertX sub-panels, also known as *interface panels*, can be used with either HID VertX V1000 network controllers or Synergis™ appliances.

For more information, see the HID datasheets on the Genetec™ Resource center.

VertX V100

Characteristics	Specifications
Power supply	9 – 18 VDC
Average operating current at 12 VDC (0 readers)	60 mA
Average operating current at 12 VDC (2 readers)	600 mA
Operating temperature range	32 ° – 122 ° F (0 ° – 50 ° C)
Humidity	5% to 95% non-condensing

VertX V200

Characteristics	Specifications
Power supply	9 – 18 VDC
Average operating current at 12 VDC	50 mA
Resistors for input supervision	1 – 10 kohm
Operating temperature range	32 ° – 122 ° F (0 ° – 50 ° C)
Humidity	5% to 95% non-condensing

VertX V300

Characteristics	Specifications
Power supply	9 – 18 VDC
Average operating current at 12 VDC	60 mA
Relay rating	2 A @ 30 VDC (maximum load)
Operating temperature range	32 ° – 122 ° F (0 ° – 50 ° C)
Humidity	5% to 95% non-condensing

Cable specifications

When attaching the interface modules to their controllers, make sure you do not exceed the recommended cable lengths.

Cable type	Maximum length	Description
Wiegand	500 ft. (152 m) to reader	ALPHA 1299C, 22AWG, 9-conductor, stranded, overall shield. Fewer conductors needed if all control lines are not used.
RS-485	4000 ft. (1220 m) to controller	Belden 3105A, 22AWG twisted pair, shielded 100 Ω cable, or equivalent.
Ethernet	328 ft. (100 m)	Cat5, Cat5E and Cat6.
Hi-O CAN bus	100 ft. (30 m)	22AWG gauge. Maximum between drops 30 ft. (10 m).

Supported HID Edge controllers

HID has two lines of Edge controllers: EVO (newer) and Legacy. The newer line of controllers can take an optional 2nd reader and have enhanced power efficiency (12 to 24 VDC), therefore, can support 12 V or 24 V locks.

In the following series of tables, we compare the characteristics of the EVO controllers to their Legacy counterparts. For more information, refer to HID documentation.

Edge platform differences between EVO and Legacy

Characteristics	EVO	Legacy
Flash memory	128 MB	8 MB
Maximum cardholder capacity	125,000	44,000
Offline cardholder capacity with Security Center[1]	65,000[2]	22,000[2]
Power over Ethernet (PoE) standard	802.3af	802.3af
RTC backup	Super-cap (2-5 days) No replacement required	Battery (3-5 days) Requires replacement
Tamper	Optical and external switch	Mechanical and external switch
Door communication	Discrete I/O, Wiegand, Hi-O	Discrete I/O, Wiegand
Mounting holes and wiring termination	US Single-Gang, EU/ASIA 60 mm	US Single-Gang
Standby condition currrent	85 – 180 mA	1 A
Maximum current	1.5 A	1.5 A
Maximum combined output rating	1.2 A	700 mA
Operating temperature range	32 ° – 120 ° F (0 ° – 49 ° C)	32 ° – 120 ° F (0 ° – 49 ° C)
Humidity	5% to 85% non-condensing	5% to 85% non-condensing

[1] In Security Center, a cardholder can have multiple credentials. A cardholder with two credentials is counted as two by HID.

[2] With Security Center, the unit's cardholder capacity is lower than its maximum cardholder capacity. This is partly because extra memory is used as cache to allow unit synchronization to be performed without affecting normal operation.

Edge controller differences between EVO and Legacy

Characteristics	EVO (EH400-K)	Legacy (E400)
Lock power provided by controller	12 V or 24 V	12 V

Characteristics	EVO (EH400-K)	Legacy (E400)
Reader power provided by controller	12 V	12 V
Input power	PoE, 12 V, 24 V	PoE, 12 V
Device periphery power using PoE	340 mA @ 24 V	700 mA @ 12 V
I/O reading (2 Readers)	Yes	No
Inputs/Outputs	5 inputs & 2 outputs	5 inputs & 2 outputs

Edge reader/controller differences between EVO and Legacy

Characteristics	EVO (EHR40-K, EHRP40-K)	Legacy (ER40, ERP40)
Input power	PoE, 12 V, 24 V	PoE, 12 V
Device periphery power using PoE	310 mA @ 24 V	600 mA @ 12 V
13.56 MHz "Smart card" credential compatibility	iCLASS	iCLASS
125 kHz "Prox" credential compatibility	HID Prox, Indala, EM4102, AWID	HID Prox
Inputs/Outputs	5 inputs & 2 outputs	5 inputs & 2 outputs
Packaging: number of pieces to install	2	1
Only secure side access to lock output	Yes	No

Supported HID Edge interface modules

The HID Edge interface modules, also known as *interface panels* and *sub-panels*, can only be used with HID Edge EVO controllers.

Security Center 5.11 supports the following interface modules with HID Edge EVO controllers:

- EDWM-M Door & Wiegand Module
- EDM-M Door Module
- EWM-M Wiegand Module
- EIM-M Input Module
- ELM Lock Module

Supported HID controller firmware in Security Center

We recommend a specific firmware version for each generation of HID controllers, old (Legacy) and new (EVO). Using earlier firmware versions might cause issues with your system.

Security Center works best when the HID controllers are running the recommended certified firmware versions.

Supported firmware	Legacy controllers	EVO controllers
Recommended certified firmware	2.2.7.568	3.8.0.105[1]
Minimum supported firmware	2.2.7.568	3.5.x

[1] As of Security Center 5.8, HID units running firmware version 3.7.0.108 or later in secure mode communicate with the Access Manager using TLS 1.2 encryption over TCP port 4433. HID units running an earlier firmware version or in regular mode communicate with the Access Manager using HID encryption.

For more information about port changes, see "Ports used by Synergis™ applications" in the *Default ports used by Security Center 5.11* document.

Previously supported firmware versions

To learn about issues with the previously supported firmware versions, see *Limitations in Security Center*.

Upgrading HID EVO firmware

Specific upgrade paths must be followed to upgrade the following HID EVO units from the firmware versions indicated to the recommended firmware version:

- Edge EVO: 2.3.1.603 or 2.3.1.605
- VertXEVO: 2.3.1.542 or 2.3.1.673

HID hardware installation do's and don'ts

For your safety and for getting the best performance out of your equipment, follow the recommended mounting and wiring instructions.

Mounting recommendations

- The controllers and interface modules must always be mounted in a secure area.
- Mount using the four mounting screws (provided) or other appropriate fasteners. Place the fasteners in the corner holes of the base.
- The VertX devices can be stacked with or without the cover. Do not remove the plastic base. Make sure you position the VertX devices in such a way as to provide room for wiring, air-flow and cable runs.

Wiring recommendations

CAUTION: VertX controllers and interface modules are sensitive to Electrostatic Discharges (ESD). Exercise precautions while handling the circuit board assembly by using proper grounding straps at all times.

- Power and alarm input connections (all VertX devices): Connect power by providing 12 VDC to the P7 connector. +12 VDC goes to Pin 1 and ground to Pin 2. Connect the *Bat Fail* and *AC Fail* inputs to battery low/failure and AC failure contacts provided on the power supply. Connect the *Tamper* input to a tamper switch on the enclosure.

  NOTE: Connect the data return line to the same ground as the reader power if the reader is not powered by the VertX controller's 12 VDC.
- The VertX controller should have a separate power supply than the mag lock and other devices such as the PIR (Passive Infrared Sensor).
- The relay output should be protected with a diode. On a PoE powered Edge controller, a non-protected relay could cause the unit to restart or go into read-only mode.
- If in-rush current with mag lock exceeds the specifications, a snubber circuit on the relay output should be added.
- Configure the tamper input to its proper state (NO/NC) even if it’s going to be disabled.
- For setups with REX mechanism built in the door handle, it is recommended to increase the debounce time for the door sensor to avoid false *Door forced open* events.
- The door sensor is by default set to NC and unsupervised, while all other inputs are by default set to NO and unsupervised (no EOL resistors). Any input can be configured as NO or NC, as well as supervised or unsupervised. They can be configured for supervisory resistors of 1 to 6 kΩ. The supervised inputs should be configured in Security Center through Config Tool and pushed to the VertX interface modules by the Access Manager. The default supervised input configuration is done using two EOL 2 kΩ resistors.
- By default, doors relock on door open. For double doors, it is recommended to set a minimum action time on the relay to maintain it active for the whole duration of the grant time.
- A V300 interface module dedicated to elevator control should only be used for elevator control and should not be used to trigger non-elevator related outputs.

Network recommendations

- It is recommended to set a static IP address on the HID controller. The discovery process is different for controllers that have a DHCP-assigned IP address. Discovery for DCHP address through multiple VLAN is not supported. If the Access Manager is on a different VLAN than the HID controller, the controller's IP address cannot be assigned by DCHP.
- It is recommended to isolate the controller on the network from broadcast traffic or unhandled multicast.
- The maximum number of character for the controller name should be 15, without spaces and special characters.
- All HID controllers have the same factory-assigned IP address 169.254.242.121. You can always log on to an HID unit from your computer using a network cable. The default logon username and password for

Legacy units are root/pass. The default logon username for EVO units is admin and the password is blank, unless it was already set.

HID VertX V1000 RS-485 connections

The VertX V1000 controller has two RS-485 serial buses with two ports each.

The two RS-485 serial buses are labeled **P3** and **P4**. Each serial bus has a 10-pin connector divided into two ports, labeled **Port 1** and **Port 2** on the **P3** bus, and **Port 3** and **Port 4** on the **P4** bus. Having two ports on each bus provides the option of splitting each RS-485 bus into two physical connections, allowing a total of four physical connections.

The followings are the do's and don'ts.

- The interface modules must be connected to the RS-485 serial buses using the daisy chain topology, not the star topology.
- Use only the "In" ports on the interface modules. This eliminates the possibility of many interface modules dropping offline because one interface module died or lost power.
- Terminate appropriately. The RS-485 serial bus expects a 120 Ω resistor to "terminate" the ends of the loop. All the devices (including the V1000 controller) have jumpers for this.
- The termination jumpers on the V1000 should be in the "Out" position if there are no interface modules attached to the port. If there are interface modules attached, then the termination jumper should be in the "In" position.
- All interface modules, except the ends of the serial chains, must have their termination jumpers in the "Out" position.
- The dial on the interface module indicates its physical address (factory default=0) to the controller it is attached to. Do not duplicate addresses on the same serial bus.
- It is recommended to wire the RS-485 to the position of the **P9** terminal block of the Vx00-series interface module. This is especially important when the RS-485 communication is in a "daisy chain" configuration. If the RS-485 is wired In and Out, and power is lost, or the **P9** terminal block is unplugged on a Vx00-series interface module, RS-485 communications will be lost to downstream Vx00-series interface modules.

HID VertX V1000 I/O behavior

The following applies to HID VertX V1000 controller inputs and outputs:

- By default, the door monitor input is configured as normally closed (NC), and not supervised (no EOL resistors). As a result, if nothing is connected to the door monitor input, the unit emits beeps to signal that the door is open. To correct this, connect the door monitor input to an actual door monitor, or reconfigure the input to normally open (NO).
- All other inputs are configured as normally open (NO), not supervised (no EOL resistors).
- It is not recommended to use HID VertX V1000 controller inputs and outputs for special purpose requirements such as:
  - A door: REX, door sensor, door lock
  - Interlock override or lockdown
  - Elevator control floor tracking
  - Door buzzer
  - I/O linking (*Hardware zone*)

  Instead, you should use the inputs and outputs from the V1000’s sub-panels (V200’s, V300’s) for these purposes.
- Any unused inputs (including AC Fail, Battery Fail and REX) can be used for other purposes except the *Tamper* and *Door Monitor* inputs. These two types of inputs can only be used for their specified purpose.
- The states of HID output relays cannot be shown in the *System status* task.

HID I/O linking considerations

Whenever a change is made to *I/O linking* on an HID unit, an internal task (called IOLinker) must be restarted in order to take the new configuration into consideration. When this happens, all output relays controlled by the unit are set to the *Normal* state for half a second before they return to their expected state. This behavior may cause temporary disruptions to the operation of your system.

The following actions applied to entities controlled by HID units may cause the output relays to reset:

- Overriding the unlock schedules of a door from Security Desk.
- Changing the unlock schedules assigned to a door.
- Changing the unlock schedule exceptions on a door.
- Configuring readers on a door that has unlock schedules assigned.
- Changing the *Door held* option of a door.
- Changing the *Door forced* option of a door.
- Changing the *Interlock* restrictions on an area using an HID controlled doors on its perimeter.
- Configuring exceptions to the floor operating schedules of an elevator.
- Configuring an event-to-action to trigger an output based on the inputs of a *hardware zone* controlled by the same HID unit.

Related Topics

Door configuration tabs on page 1268

Selecting who has access to doors on page 785

Selecting who has access to elevators on page 791

Configuring hardware zone settings on page 1205

HID Power and Comm LEDs

HID units are equipped with two status LEDs labeled as Power and Comm. You can find these LEDs on top of the face plate for V1000s and V2000s. For Edge and Edge Plus devices, the LEDs are found on the bottom of the unit.

V1000, V2000, and Edge Reader Power and Comm LEDs

LED indicator	State	Description
Power	Off	Check input voltage to the unit
	Solid red	No network activity
	Blinking (red/off)	Network activity
Comm	Solid green	All interfaces found (such as V100, V200, V300)
	Solid red	No interfaces found
	Blinking (red/green)	Some interfaces were found (the duty cycle changes according to the number of interfaces found).
	Blinking (amber/green)	The unit is in *Locate me* mode (somebody clicked **Identity**)

For VertX V1000 units: If the Comm LED indicator is off, update the firmware for the interface (V100) part of the unit.

VertX interface boards (sub-panels) V100, V200, V300

LED indicator	State	Description
Power	Solid red	OK
	Anything other than solid red	Check input voltage
Comm	Blinking (red/green)	RS-485 bus activity
	Amber	Firmware download in progress

If the Comm LED indicator for an interface board is off, check the wiring for the RS-485 bus. If the issue persists, update the firmware.

HID features and models supported by Security Center

This section lists the Security Center access control features that are supported by each HID unit model.

Supported keypad reader options

Card and PIN operation depends on the type of unit and the keypad reader installed.

For both HID iCLASS and Prox readers, the *Keypad configuration setting* option is selected at the time of purchase. Supported options include the following:

- Option 00: “Keypad configuration setting option” of 00 = Buffer one key, no parity, 4-bit message.
- Option 14: “Keypad configuration setting option” of 14 = Buffer one to five keys (Standard 26-bit output). This reader option is also known as “Galaxy Mode”.

Unit type	HID keypad reader option	Online operation	Offline operation	Observation
V1000 with V100 V2000 EdgePlus E400	Option 14	Card or PIN.	Card or PIN.	The keypad readers can be used to enroll PINs.
	Option 00	Card or PIN. Card and PIN on schedule. When off-schedule, operation reverts to card only.		The reader cannot be used to enroll PINs for credential creation.
EdgeReader ER40 EdgeReader ERP40 EdgeReader ERW400	These units cannot be ordered with a keypad.	Card only.	Card only.	—

For HID SmartID keypad readers (SK10), the following option is required to support card and PIN functionality:

- Option 02PIN-0000: “Pincode Wiegand 4 bit per key no parity”.

Supported PIN length

By default, HID controllers only accept PIN numbers up to 5 digit long. You can increase this limit to 8 digits for readers using *Card and PIN* mode, and to 15 digits for readers using *Card* or *PIN* mode.

Supported readers

HID units support most industry standard card readers that output card data using the Wiegand protocol (up to 128-bit card formats).

HID SmartID readers (MIFARE and DESFire) are also supported.

Support for Power over Ethernet (PoE)

The following Legacy and EVO units support PoE (15.4W):

Unit type	Support
HID Legacy/EVO V1000	Not supported
HID Legacy/EVO V2000	Not supported
HID Legacy EdgeReader/EdgePlus	Supported
HID EVO Edge	Supported

Supported cardholder and reader capacity

The number of *cardholders* (or *credentials*) that a unit can support offline is as follows:

Unit type	Supported number of cardholders
HID Legacy V1000 with V100	22,000, up to 125,000 cardholders with full memory upgrade.
HID EVO V1000 with V100	65,000. No memory upgrade is possible.
HID Legacy V2000	22,000, up to 125,000 cardholders with full memory upgrade.
HID EVO V2000	65,000. No memory upgrade is possible.
HID Legacy EdgeReader/EdgePlus	22,000 cardholders (maximum). No memory upgrades are possible.
HID EVO Edge	65,000. No memory upgrade is possible.

The number of readers that a unit can support is as follows:

Unit type	Supported number of readers
HID Legacy/EVO V1000 with V100	64 readers with 32 V100 reader interface modules[1] 32 doors configured as card in/card out 64 doors configured as card in/REX out
HID Legacy/EVO V2000	2 readers 1 door configured as card in/card out 2 doors configured as card in/REX out
HID Legacy EdgeReader/EdgePlus	1 reader 1 door configured as card in/REX out
HID EVO Edge	2 readers 1 door configured as card in/REX out or card in/card out

[1] HID states that a V1000 controller can support a maximum of 32 downstream interface modules (16 on each RS-485 serial bus). However, the performance tests run by Genetec Inc. indicate that as a “best practice”, 20 downstream interface modules should not be exceeded (10 per serial bus).

Enabling long PIN support on HID units

You can enable the long PIN (longer than 5 digits) support on HID controllers (legacy and EVO) by changing a configuration file (gconfig) on the servers hosting the Access Manager role.

What you should know

By default, HID controllers only accept PIN numbers up to 5 digit long. You can increase this limit to 8 digits for readers using Card and PIN mode, and to 15 digits for readers using Card or PIN mode.

To enable long PIN support on HID controllers:

1 Create the *VertXConfig.gconfig* file with the following content:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <Vertx MaximumPinLength="nn"/>
</configuration>
```

where nn is the maximum PIN length in digits.

If this file already exists, simply add the tag MaximumPinLength=”nn”.

2 Copy this file to the Security Center installation folder, on all servers hosting the Access Manager role.

The default is *C:\Program Files (x86)\Genetec Security Center 5.x\ConfigurationFiles* on a 64-bit machine.

The next time you synchronize a unit (HID controller) with the Access Manager, the unit will accept PIN numbers up to the maximum PIN length. For every PIN credential that is longer than the specified maximum, a warning message will be issued during synchronization, and the PIN will not be synchronized to the unit.

To synchronize a unit:

1 Connect to Security Center with Config Tool.

2 Open the *Access control* task, and go to the *Roles and units* page.

3 Select a unit (HID controller), select **Synchronization**, and then click **Synchronize now**.

Supported HID unit configurations

This section describes the supported HID access control unit configurations in Security Center.

General vs. dedicated inputs

When a controller is used to control a door, some inputs must be used only for their intended purpose (dedicated inputs). For example, if a door has a REX sensor or a door sensor, the controller's inputs intended for these sensors must be used.

Input	When used as	Required configuration
Request-to-Exit	Request-to-Exit input signal.	• Set **Unlock on REX** to ON in the **Door** > **Properties** tab to generate *Request to exit* events when the input is triggered. Events are logged, and can be used for event-to-actions. • Assign the REX input to a door side in the **Door** > **Hardware** tab to program the controller to react to the REX input by releasing the lock.
	General purpose input (for zone monitoring for example)	• Set **Unlock on REX** to OFF in the **Door** > **Properties** tab. • Configure the input for a zone, interlock, etc.
Door monitor	Door position sensor input (door open or door closed)	• Assign this input to the **Door sensor** in the **Door** > **Hardware** tab. **NOTE:** This input cannot be used for any other purpose.

HID door configuration with readers

A door with a reader assigned to a V2000, V100, or an Edge device, must have all inputs (for example door contact, REX) and outputs (for example door lock) associated to that same device. Inputs and outputs must not be distributed across several devices.

HID door configuration with two door sensors

It is not recommended to configure a door with two door sensors (or door contacts) without physically wiring the sensors in series. In the Security Center, only a single door sensor should be configured per door.

Security Center features supported by HID units

This section lists the standard Security Center access control features that HID units support.

Readerless door

Readerless doors (doors that use an I/O module for a REX, door state, and door lock only) are supported, both when the unit is operating online and offline.

For readerless doors to work, the following is required:

- The inputs of an HID VertX V1000 must be not used for this feature.
- All inputs and outputs must belong to the same HID controller (one V2000 or one Edge).

NOTE: A readerless door does not support the buzzer feature.

Door control

- **Card and PIN:** Card and PIN reader mode is supported if the installed reader supports it.

  For card and PIN reader mode to work, all reader interfaces/inputs/outputs for a door must be controlled by the same HID unit (HID Edge, VertX V2000, or VertX V100 interface module).
- **PIN entry timeout:** Supported as per door configuration.
- **Extended grant time:** Supported as per door configuration.
- **Entry time (standard and extended):** Supported as per door configuration.
- **Door relock:** The relock option on door closed is not supported. Only the delayed locking after the door opens is supported, and the maximum delay is 27 minutes.
- **Door held event and buzzer:** Both the *Door open too long* event and the reader buzzer are supported as per door configuration.
- **Door forced event and buzzer:** Both the *Door forced open* event and the reader buzzer are supported as per door configuration.
- **Request to exit (REX):** All REX handling behavior are supported as per door configuration.
- **Shunting:** Reader shunting is not supported. Only inputs can be shunted.

People counting

People counting is supported only when all units used for this feature are connected to the same Access Manager. The moment a unit assigned to one of the perimeter doors of an area is offline, the feature is disabled for the entire area.

Security clearance

The concept of security clearance is not supported for areas controlled by HID units.

Elevator control

For elevator control to work, the following is required:

- All interface modules used for elevator control (HID VertX V100, V200, and V300) must be assigned to the same VertX V1000. Reader, inputs and outputs must be assigned to the same V2000 (max. of 4 floors) or Edge (max. of 2 floors).
- All units used for this feature must be assigned to the same Access Manager.

- The reader interface, inputs, and outputs must be connected to the same HID controller (VertX V1000, V2000, or Edge). A maximum of 1 elevator cab reader can be assigned per HID controller (VertX V1000, V2000, or Edge).

NOTE: If you plan to offer both periods of controlled access and free access to your elevators, contact your representative of Genetec Inc. for a custom firmware to use with the units controlling elevators.

The use of HID VertX controllers (V1000 and V2000) for elevator control is subject to the following limitations:

- A VertX controller should be dedicated to the control of a single elevator cab.
- Once a VertX controller has been assigned to perform elevator control, it should only be used for that purpose. Door and zone control should not be mixed with elevator control, even when the unit has unused readers, inputs and outputs.
- When *elevator* floors are operating under controlled access mode, schedules from different *access rules* applied to different floors are merged when the rules are granted to a same cardholder.

  Example: Bob is granted access to Floor-1 from 9 am to 10 am through access rule 1, and to Floor-2 from 10 am to 11 am through access rule 2. When Bob presents his card in the elevator, the VertX controller actually grants access to Robert from 9 am to 11 am on both floors.
- Unlock schedules cannot be used on elevators controlled by HID units.

Elevator floor tracking

Floor tracking is only supported when the unit is online, and when all units used for this feature are assigned to the same Access Manager.

NOTE: Elevator floor tracking is not supported when the unit is offline because event reporting is unavailable. Events are not regenerated when the unit reconnects to Security Center.

Antipassback feature

The *antipassback* feature is supported both when the unit is operating online and offline.

For antipassback to work, the following is required:

- Use either VertX V1000 (multiple areas and multiple doors per area) or VertX V2000 (area with a single door) controllers. HID Edge products are not supported.
- All units used for antipassback must be assigned to the same Access Manager.
- The interlock feature must be disabled. Interlock (including the lockdown and override functions) and antipassback are mutually exclusive; both features cannot be enabled for an area at the same time.

Antipassback works best once the access control system has been configured and the system is operational and relatively static. It is recommended to enable antipassback once the following entities have been properly configured in Security Center and are not expected to change on a daily basis:

- Unit time zones
- Doors and associated readers
- Areas (groups of doors)
- Elevators and associated floors (including unlocking schedules)
- Cardholder groups
- Schedules (including card and PIN schedules)
- Access rules

The following section provides guidelines for configuring, enabling, and managing antipassback with HID VertX controllers (units):

- You must use either the V1000 or V2000 for antipassback.
  - V2000: Antipassback is only supported for an area with a single door having both entry and exit readers.
  - V1000: Antipassback is supported for multiple areas, with each area supporting multiple doors with entry and exit readers. Limitation in the number of doors is based on the number of V100 modules installed.
- Antipassback is not recommended with the Edge product line for the following reasons:
  - Only a single reader can be specified for either entry or exit (not both) while antipassback typically requires both entry and exit readers.
  - Peer-to-peer communication between Edge devices is not supported by Security Center.
- An area with antipassback must be configured for readers wired to, and doors managed by, the same unit (V1000 or V2000) because:
  - Antipassback functions are handled by the unit (V1000 or V2000).
  - The Security Center does not support peer-to-peer communication between either VertX V1000 or V2000 devices.
- Antipassback can be reset using the following methods:
  - A unit synchronization operation
  - An action (manually or with an event-to-action)
- The following system behavior will reset a unit’s antipassback state:
  - Initial unit synchronization when the Security Center services are started or restarted.
  - Unit synchronization following the loss and recovery of a connection with the unit (V1000 or V2000).
  - Unit synchronization following certain configuration changes (see below for more details).
  - Manual synchronization of the unit through the Config Tool page.

Antipassback options

The following antipassback options are supported:

- Soft antipassback (passback violation event generated and access is granted) is only supported when the unit is online. Soft antipassback is not supported when the unit is offline because event reporting is unavailable. Events are not regenerated when the unit reconnects to Security Center.
- Hard antipassback (passback violation event generated and access is denied) is supported both when the unit is operating online and offline.
- Strict antipassback (passback violation event is generated when a cardholder attempts to leave an area that they were never granted access to). With HID units, hard and strict antipassback are one and the same. There is no distinction between the two.
- Antipassback on schedule is supported both when the unit is operating online and offline.
- Antipassback on schedule is not supported with hard antipassback.

NOTE: The timed antipassback option is not supported.

Interlock feature

The interlock feature is supported both when the unit is operating online and offline.

For interlock to work, the following is required:

- The antipassback feature must be disabled. *Interlock* (including the lockdown and override functions) and *antipassback* are mutually exclusive; both features cannot be enabled for an area at the same time.
- The inputs of an HID VertX V1000 must be not used for this feature.

- All perimeter doors of an interlocked area must be assigned to the same HID controller (one VertX V1000 or one V2000).

NOTE: If a perimeter door of an interlock is open, when an authorized cardholder accesses a second perimeter door of the same interlock, an *Access granted* event for the second door might be generated, even through the second door does not unlock.

Interlock options

The following interlock options are supported both when the unit is operating online and offline:

- Lockdown
- Override

First-person-in rule

First-person-in rule is not supported by HID units.

Two-person-in rule

Two-person rule is not supported by HID units.

Visitor escort rule

Visitor escort rule is not supported by HID units.

Event-to-actions

Event-to-action is supported when the unit is operating online and offline, with limitations.

- **Event-to-actions with Trigger output action:** The *Trigger output* action type can be used in event-to-actions when the unit is online, and is partially supported when the unit is offline. For the *Trigger output* action type to work, all units used for this feature must be assigned to the same Access Manager.
- **Event-to-actions with Silence buzzer or Sound buzzer actions:** The *Silence buzzer* and *Sound buzzer* action types can be used in event-to-actions both when the unit is operating online and offline. For these actions to work, all inputs and outputs must belong to the same HID controller (one VertX V1000, one V2000, or one Edge).

  NOTE: The *Action* feature is not available with a readerless door.
- **Access granted events are not supported when the unit is offline:** Event-to-actions based on the *Access granted* event do not work when the unit is disconnected from the Access Manager role.

I/O Linking

The I/O linking feature is supported both when the unit is operating online and offline, with the following limitations.

- The inputs of an HID VertX V1000 must be not be used for this feature.
- All inputs and outputs must be controlled by the same HID controller.
- Only the *Trigger output* action is supported when the unit is operating offline.

Related Topics

HID features and models supported by Security Center on page 1489

Multiple-Swipe feature

This section includes the following topics:

About the multi-swipe feature

The multi-swipe feature allows cardholders to badge their credentials multiple times at a door in order to generate a custom event. This event can then be used to trigger an action through an event-to-action.

The MultiSwipe macro

The MultiSwipe macro enables a specific group of cardholders to generate two distinct custom events when they swipe their credentials a given number of times at door, within the prescribed delay. N swipes generates the first custom event, and N+1 swipes generates the second custom event. All cardholders in the designated group must be granted access to the door.

The MultiSwipe macro is provided with your Security Center software to help you implement this feature.

Implementing the multi-swipe feature

You can implement the multi-swipe feature using the macro provided with your Security Center software.

Before you begin

You need to create the following entities in order to implement the multi-swipe feature:

- A door equipped with a reader, to be used for the multi-swipe feature.
- A cardholder group authorized to use the multi-swipe feature. All members of this group must have access to the designated door.
- Two custom events: a first one to be generated when an authorized cardholder swipes N times at the door, and a second one to be generated when the cardholder swipes N+1 times.
- A schedule that defines when the multi-swipe feature is available.

What you should know

All macros provided with the Security Center software are found in the folder *Add-On\Macros* under the Security Center installation folder (default=*C:\Program Files (x86)\Genetec Security Center 5.11*).

To implement the multi-swipe feature at a door:

1. Create a macro and name it *Multi-Swipe at <Door>*, where *<Door>* is the name of the door where the multi-swipe feature is enabled.

   Instead of a door, you can also select an area. In this case, the multi-swipe feature is enabled on all doors within the area.
2. Select the **Properties** tab, click **Import from file**, select *MultiSwipe.cs*, and click **Open**.
3. Click **Check syntax**, click **Close**, and then click **Apply**.
4. Select the **Default execution context** tab, and set the following properties.
   - **CardholderGroup:** Cardholder group authorized to use the multi-swipe feature.
   - **DoorOrArea:** Door or area for which the multi-swipe feature is being enabled.
   - **DelayInSecondsBetweenEachSwipe:** The maximum delay in seconds between two consecutive swipes from the same authorized cardholder for the swipe to be considered as part of the multi-swipe action.
   - **NumberOfSwipes:** Number of swipes (N) to generate the first custom event.
   - **NSwipesCustomEventId:** Value assigned to the first custom event. Note that the first custom event is only generated *n* seconds after the last swipe, *n* being the maximum delay in seconds between two consecutive swipes.
   - **Np1SwipesCustomEventId:** Value assigned to the second custom event. Note that the second custom event is immediately generated after N+1 swipes.
   - **Schedule:** Schedule during which the multi-swipe feature is in effect.
5. Click **Apply**.
6. Create a scheduled task and name it *RunMultiSwipe-OnStartup*.
7. Select the **Properties** tab, and set its properties as follows.
   - **Status:** Set the status to ON.
   - **Recurrence:** Set the recurrence to **On startup**.
   - **Action:** Select **Run a macro**, and set **Macro** to the macro you just created.
8. Click **Apply**.

   This makes sure that the multi-swipe macro is always running, even after a system restart.

9 Create an event-to-action to link the first custom event to the desired action.
Example: Temporarily override unlock schedule, arm a zone, and so on.

10 Create an event-to-action to link the second custom event to the desired action.
Example: Cancel the unlock schedule override, disarm a zone, and so on.

Glossary

Access control

The *Access control* task is an administration task that you can use to configure access control roles, units, access rules, cardholders, credentials, and related entities and settings.

Access control health history

The *Access control health history* task is a maintenance task that reports on events related to the health of access control entities. Unlike the events in the *Health history* report, the events in the *Access control health history* report are not generated by the Health Monitor role, identified by an event number, or categorized by severity.

access control unit

An access control unit entity represents an intelligent access control device, such as a Synergis™ appliance or an HID network controller, that communicates directly with the Access Manager over an IP network. An access control unit operates autonomously when it is disconnected from the Access Manager.

Access control unit events

The *Access control unit events* task is a maintenance task that reports on events pertaining to selected access control units.

Access Manager

The Access Manager role manages and monitors access control units on the system.

access point

An access point is any entry (or exit) point to a physical area where access can be monitored and governed by access rules. An access point is typically a door side.

access right

An access right is the basic right users must have over any part of the system before they can do anything with it. Other rights, such as viewing and modifying entity configurations, are granted through privileges. In the context of a Synergis™ system, an access right is the right granted to a cardholder to pass through an access point at a given date and time.

access rule

An access rule entity defines a list of cardholders to whom access is either granted or denied based on a schedule. Access rules can be applied to secured areas and doors for entries and exits, or to intrusion detection areas for arming and disarming.

Access rule configuration

The *Access rule configuration* task is a maintenance task that reports on entities and access points affected by a given access rule.

Access troubleshooter

Access troubleshooter is a tool that helps you detect and diagnose access configuration problems. With this tool, you can find out about the following:

- Who is allowed to pass through an access point at a given date and time
- Which access points a cardholder is allowed to use at a given date and time
- Why a given cardholder can or cannot use an access point at a given date and time

action

An action is a user-programmable function that can be triggered as an automatic response to an event, such as door held open for too long or object left unattended, or that can be executed according to a specific time table.

active alarm

An active alarm is an alarm that has not yet been acknowledged.

active authentication

Active authentication is when the client application captures the user credentials and sends them through a secure channel to a trusted identity provider for authentication.

Active Directory

Active Directory is a directory service created by Microsoft, and a type of role that imports users and cardholders from an Active Directory and keeps them synchronized.

Active Directory Federation Services

Active Directory Federation Services (ADFS) is a component of the Microsoft® Windows® operating system that issues and transforms claims, and implements federated identity.

Activity trails

The *Activity trails* task is a maintenance task that reports on the user activity related to video, access control, and ALPR functionality. This task can provide information such as who played back which video recordings, who used the Hotlist and permit editor, who enabled hotlist filtering, and much more.

add-on

An add-on is a software package that adds tasks, tools, or specific configuration settings to Security Center systems.

Advanced Systems Format

The Advanced Systems Format (ASF) is a video streaming format from Microsoft. The ASF format can only be played in media players that support this format, such as Windows Media Player.

agent

An agent is a subprocess created by a Security Center role to run simultaneously on multiple servers for the purpose of sharing its load.

alarm

An alarm entity describes a particular type of trouble situation that requires immediate attention and how it can be handled in Security Center. For example, an alarm can indicate which entities (usually cameras and doors) best describe the situation, who must be notified, how it must be displayed to the user, and so on.

alarm acknowledgement

An alarm acknowledgement is the final user response to an alarm that ends its lifecycle and removes it from the active alarm list. In Security Center, we have two variants of alarm acknowledgements: default and alternative. Each variant is associated to a different *event* so that specific actions can be programmed based on the alarm response selected by the user.

Alarm monitoring

The *Alarm monitoring* task is an operation task that you can use to monitor and respond to alarms (acknowledge, forward, snooze, and so on) in real time, and to review past alarms.

Alarm report

The *Alarm report* task is an investigation task that you can use to search and view current and past alarms.

Alarms

The *Alarms* task is an administration task that you can use to configure alarms and monitor groups.

ALPR

The *ALPR* task is an administration task that you can use to configure roles, units, hotlists, permits, and overtime rules for ALPR, and related entities and settings.

ALPR camera

An Automatic License Plate Recognition (ALPR) camera is a camera connected to an ALPR unit that produces high resolution close-up images of license plates.

ALPR context

An ALPR context is an ALPR optimization that improves license plate recognition performance for license plates from a specific region (for example, New York) or from a group of regions (for example, Northeast states).

ALPR Frequency Monitor

The Stakeout - ALPR Frequency Monitor plugin tracks how often vehicles are detected by fixed Sharp cameras. The system can alert Security Desk users if vehicles without whitelisted license plates have exceed the configured threshold.

ALPR Manager

The ALPR Manager role manages and controls the patrol vehicle software (Genetec Patroller™), Sharp cameras, and parking zones. The ALPR Manager stores the ALPR data (reads, hits, timestamps, GPS coordinates, and so on) collected by the devices.

ALPR rule

ALPR rule is a method used by Security Center and AutoVu™ for processing a license plate read. An ALPR rule can be a hit rule or a parking facility.

ALPR unit

An ALPR unit is a device that captures license plate numbers. An ALPR unit typically includes a context camera and at least one ALPR camera.

analog monitor

An analog monitor entity represents a monitor that displays video from an analog source, such as a video decoder or an analog camera. This term is used in Security Center to refer to monitors that are not controlled by a computer.

antipassback

Antipassback is an access restriction placed on a secured area that prevents a cardholder from entering an area that they have not yet exited from, and vice versa.

architecture version

An architecture version is a software version that introduces significant changes to the architecture or user experience of the platform. Architecture upgrades require changes to system design and configuration settings, data migration, and retraining of users. Architecture versions are not compatible with previous versions. A license update is required to upgrade to a new architecture version. An architecture version is indicated by a version number with zeros at the second, third and fourth positions: X.0.0.0. For more information, see our Product Lifecycle page on GTAP.

Archiver

The Archiver role is responsible for the discovery, status polling, and control of video units. The Archiver also manages the video archive and performs motion detection if it is not done on the unit itself.

Archiver events

The *Archiver events* task is a maintenance task that reports on events pertaining to selected Archiver roles.

Archiver statistics

Archiver statistics is a maintenance task that reports on the operation statistics (number of archiving cameras, storage usage, bandwidth usage, and so on) of the selected archiving roles (Archiver and Auxiliary Archiver) in your system.

Archives

The *Archives* task is an investigation task that you can use to find and view video archives by camera and time range.

Archive storage details

The *Archive storage details* task is a maintenance task that reports on the video files (file name, start and end time, file size, protection status, and so on) used to store video archive. Using this task, you can also change the protection status of these video files.

archive transfer

Archive transfer is the process of transferring your video data from one location to another. The video is recorded and stored on the video unit itself or on an Archiver storage disk, and then the recordings are transferred to another location.

Archive transfer

(Obsolete as of Security Center 5.8 GA) The *Archive transfer* task is an administration task that allows you to configure settings for retrieving recordings from a video unit, duplicating archives from one Archiver to another, or backing up archives to a specific location. Starting from Security Center 5.8 GA, *Archive transfer* is a page inside the *Video* administration task.

archiving role

An archiving role is an instance of either the Archiver role or Auxiliary Archiver role.

area

In Security Center, an area entity represents a concept or a physical location (room, floor, building, site, and so on) used for grouping other entities in the system.

Area activities

The *Area activities* task is an investigation task that reports on access control events pertaining to selected areas.

Area presence

The *Area presence* is and investigation task that provides a snapshot of all cardholders and visitors currently present in a selected area.

area view

The area view is a view that organizes the commonly used entities such as doors, cameras, tile plugins, intrusion detection areas, zones, and so on, by areas. This view is primarily created for the day to day work of the security operators.

Area view

The *Area view* task is an administration task that you can use to configure areas, doors, cameras, tile plugins, intrusion detection areas, zones, and other entities found in the *area view*.

armed tile

An armed tile is a tile in Security Desk that displays new alarms that are triggered. In the *Alarm monitoring* task all tiles are armed, while in the *Monitoring* task, tiles must be armed by a user.

asset

An asset entity represents any valuable object with an RFID tag attached, thus allowing it to be tracked by an asset management software.

asymmetric encryption

See "public-key encryption".

asynchronous video

Asynchronous video is simultaneous playback video from more than one camera that are not synchronized in time.

audio decoder

An audio decoder is a device or software that decodes compressed audio streams for playback. Synonym of *speaker*.

audio encoder

An audio encoder is a device or software that encodes audio streams using a compression algorithm. Synonym of *microphone*.

Audit trails

The *Audit trails* task is a maintenance task that reports on the configuration changes of the selected entities in the system. The report also indicates the user who made the changes.

authentication

The process of verifying that an entity is what it claims to be. The entity could be a user, a server, or a client application.

Authentication Service

The Authentication Service role connects Security Center to an external identity provider for third-party authentication.

Instances of the Authentication Service role are protocol-specific. One of the following protocols is selected at role creation:

- OpenID
- SAML2
- WS-Trust or WS-Federation

Multiple Authentication Service roles can be created, but each must monitor a unique list of domains.

authorization

The process of establishing the rights an entity has over the features and resources of a system.

authorized user

An authorized user is a user who can see (has the right to access) the entities contained in a partition. Users can only exercise their privileges on entities they can see.

automatic enrollment

Automatic enrollment is when new IP units on a network are automatically discovered by and added to Security Center. The role that is responsible for the units *broadcasts* a discovery request on a specific port, and the units listening on that port respond with a message that contains the connection information about themselves. The role then uses the information to configure the connection to the unit and enable communication.

automatic license plate recognition

Automatic license plate recognition (ALPR) is an image processing technology used to read license plate numbers. ALPR converts license plate numbers cropped from camera images into a database searchable format.

AutoVu™

The AutoVu™ automatic license plate recognition (ALPR) system automates license plate reading and identification, making it easier for law enforcement and for municipal and commercial organizations to locate vehicles of interest and enforce parking restrictions. Designed for both fixed and mobile installations, the AutoVu™ system is ideal for a variety of applications and entities, including law enforcement, municipal, and commercial organizations.

AutoVu™ Managed Services

With AutoVu™ Managed Services (AMS), your automatic license plate recognition (ALPR) system is hosted in the cloud and experts from Genetec Inc. configure and maintain it. This reduces the need for on-site IT infrastructure and support.

AutoVu™ Third-party Data Exporter

The AutoVu™ Third-party Data Exporter is a feature that uses either an HTTPS or a SFTP connection protocol to securely export ALPR events, for example reads and hits, to external endpoints.

Auxiliary Archiver

The Auxiliary Archiver role supplements the video archive produced by the Archiver role. Unlike the Archiver role, the Auxiliary Archiver role is not bound to any particular *discovery port*, therefore, it can archive any camera in the system, including cameras federated from other Security Center systems. The Auxiliary Archiver role cannot operate independently; it requires the Archiver role to communicate with video units.

Axis Powered by Genetec

Axis Powered by Genetec is an all-in-one solution that combines Genetec™ access control software with Axis network door controllers. Synergis™ Softwire is preinstalled onto the Axis controllers and runs as an app on the AXIS OS platform. This simplifies their deployment, configuration, and maintenance in Security Center. Axis Powered by Genetec is sold exclusively through Genetec™ Certified channel partners.

Badge designer

The Badge designer is the tool that you can use to design and modify badge templates.

badge template

A badge template is an entity used to configure a printing template for badges.

block face (2 sides)

A block face (2 sides) is a parking regulation characterizing an overtime rule. A block face is the length of a street between two intersections. A vehicle is in violation if it is seen parked within the same block over a specified period of time. Moving the vehicle from one side of the street to the other does not make a difference.

body-worn camera

A body-worn camera (BWC), also known as a wearable camera, is a video recording system that is typically used by law enforcement to record their interactions with the public or gather video evidence at crime scenes.

bookmark

A bookmark is an indicator of an event or incident that is used to mark a specific point in time in a recorded video sequence. A bookmark also contains a short text description that can be used to search for and review the video sequences at a later time.

Bookmarks

The *Bookmarks* task is an investigation task that searches for bookmarks related to selected cameras within a specified time range.

Breakout box

The breakout box is the proprietary connector box of Genetec Inc. for AutoVu™ mobile solutions that use Sharp cameras. The breakout box provides power and network connectivity to the Sharp units and the in-vehicle computer.

broadcast

Broadcast is the communication between a single sender and all receivers on a network.

camera

A camera entity represents a single video source in the system. The video source can either be an IP camera, or an analog camera that connects to the video encoder of a video unit. Multiple video streams can be generated from the same video source.

camera blocking

Camera blocking is an Omnicast™ feature that lets you restrict the viewing of video (live or playback) from certain cameras to users with a minimum user level.

Camera configuration

The *Camera configuration* task is a maintenance task that reports on the properties and settings of local cameras in your system (manufacturer, resolution, frame rate, stream usage, and so on).

Camera events

The *Camera events* task is an investigation task that reports on events pertaining to selected cameras within a specified time range.

Camera Integrity Monitor

The Camera Integrity Monitor role samples video images from cameras at regular intervals, detects abnormal variations that indicate that cameras might have been tampered with, and generates *Camera tampering* events.

camera integrity monitoring

In Security Center, camera integrity monitoring is software that detects any form of tampering with the camera, such as moving the camera, obstructing the camera view, changing the camera focus, and so on. The software automatically generates events to alert the security team to remedy the situation.

camera sequence

A camera sequence is an entity that defines a list of cameras that are displayed one after another in a rotating fashion within a single tile in Security Desk.

canvas

Canvas is one of the panes found in the Security Desk's task workspace. The canvas is used to display multimedia information, such as videos, maps, and pictures. It is further divided into three panels: the tiles, the dashboard, and the properties.

capture rate

The capture rate measures the speed at which a license plate recognition system can take a photo of a passing vehicle and detect the license plate in the image.

Card and PIN

Card and PIN is an access point mode that requires a cardholder to present their card, and then enter a personal identification number (PIN).

cardholder

A cardholder entity represents a person who can enter and exit secured areas by virtue of their credentials (typically access cards) and whose activities can be tracked.

Cardholder access rights

The *Cardholder access rights* task is a maintenance task that reports on which cardholders and cardholder groups are granted or denied access to selected areas, doors, and elevators.

Cardholder activities

The *Cardholder activities* task is an investigation task that reports on cardholder activities, such as access denied, first person in, last person out, antipassback violation, and so on.

Cardholder configuration

The *Cardholder configuration* is a maintenance task that reports on cardholder properties, such as first name, last name, picture, status, custom properties, and so on.

cardholder group

A cardholder group is an entity that defines the common access rights of a group of cardholders.

Cardholder management

The *Cardholder management* task is an operation task. You can use this task to create, modify, and delete cardholders. With this task, you can also manage a cardholders' credentials, including temporary replacement cards.

certificate

Designates one of the following: (1) *digital certificate*; (2) *SDK certificate*.

certificate authority

A certificate authority or certification authority (CA) is an entity or organization that signs identity certificates and attests to the validity of their contents. The CA is a key component of the public-key infrastructure (PKI)

Certificate Signing

The Certificate Signing role acts as the certificate authority (CA) for all access control and video units whose certificates are managed in Security Center by the Unit Assistant role. You may have only one instance of this role in your system.

City Parking Enforcement

City Parking Enforcement is a Genetec Patroller™ software installation that is configured for the enforcement of parking permit and overtime restrictions.

City Parking Enforcement with Wheel Imaging

City Parking Enforcement with Wheel Imaging is a *City Parking Enforcement* installation of a Genetec Patroller™ application that also includes wheel imaging. The use of maps is mandatory and the mobile AutoVu™ system must include navigation hardware.

claim

A statement that a trusted third-party makes about a subject, such as a user. For example, a claim can be about a name, identity, key, group, privilege, or capability. Claims are issued by an identity provider. They are given one or more values and then packaged in a security token that is sent to relying applications during third-party authentication.

client certificate

A client certificate is an *identity certificate* used to authenticate the client's identity to the server. Unlike server certificates, client certificates are not used to encrypt data-in-transit. They only serve as a more secure authentication mechanism than passwords.

client-specific key stream

The client-specific key stream is the encrypted form of the *master key stream*. The master key stream is encrypted with the *public key* contained in an *encryption certificate*, specifically issued for one or more client machines. Only the client machines that have the encryption certificate installed have the required *private key* to decrypt the encrypted key stream.

cloud platform

A cloud platform provides remote computing and storage services through centralized data centers that are accessible via the Internet.

Cloud Playback

The Cloud Playback role is used by Cloud storage to stream video archives from the cloud to clients and federated users connected to the system. Cloud Playback supports the Real Time Streaming Protocol (RTSP) locally and uses TLS to retrieve video sequences from the cloud.

Cloud storage

Cloud storage is a service from Genetec Inc. that extends on premise storage for Security Center Omnicast™ into the cloud. Video archives in Cloud storage benefit from extended retention periods, secure and redundant storage, and seamless retrieval from Security Desk.

collaborative incident

A collaborative incident is an incident type that requires the collaboration of multiple teams to resolve. Each team has specific tasks to follow, which are represented by sub-incidents. The collaborative incident is resolved when all its sub-incidents are resolved.

Config Tool

Config Tool is the Security Center administrative application used to manage all Security Center users and to configure all Security Center entities such as areas, cameras, doors, schedules, cardholders, patrol vehicles, ALPR units, and hardware devices.

Conflict resolution utility

The Conflict resolution utility is a tool that helps you resolve conflicts caused by importing users and cardholders from an Active Directory.

context camera

A context camera is a camera connected to an ALPR unit that produces a wider angle color image of the vehicle whose license plate was read by the ALPR camera.

Continuous Delivery

The Continuous Delivery (CD) release track offers customers an upgrade path with ongoing innovations, introducing new features, bug fixes, performance enhancements, and support for the latest devices through minor versions. The frequency of changes introduced on the CD track may be impractical for some organizations, who opt for the long-term predictability of the LTS track.

contract permit parking

Contract permit parking is a parking scenario where only drivers with monthly permits can park in the parking zone. A whitelist is used to grant permit holders access to the parking zone.

controlled exit

A controlled exit is when credentials are necessary to leave a secured area.

controller module

Controller module is the processing component of Synergis™ Master Controller with IP capability. This module comes pre-loaded with the controller firmware and the web-based administration tool, Synergis™ Appliance Portal.

convenience time

The convenience time is a configurable leeway time before a vehicle starts to be charged after entering the parking zone. For example, if you need to set up a 2-hour free parking period before paid time or parking enforcement takes effect, you would set the convenience time for 2 hours. For parking lots where parking enforcement begins immediately, you would still need to set a short convenience time to allow vehicle owners time to find a parking spot and purchase parking time before parking enforcement begins.

Copy configuration tool

The Copy configuration tool helps you save configuration time by copying the settings of one entity to many others that partially share the same settings.

correlation

Correlation refers to the relationship that exists between two types of events, X and Y. A correlation exists between X and Y if whenever event X occurs, event Y is expected. For example, if whenever there is a large gathering of people (event X), the number of new cases of COVID-19 increases in the following days (event Y), we can say that there is a correlation between large gatherings and the increase of the number of new COVID-19 cases.

covert hit

A covert hit is a read (captured license plate) that is matched to a covert hotlist. Covert hits are not displayed on the Genetec Patroller™ screen, but can be displayed in Security Desk by a user with proper privileges.

covert hotlist

Covert hotlists allow you to ensure the discretion of an ongoing investigation or special operation. When a hit is identified, only the authorized officer at the Security Center station is notified, while the officer in the patrol vehicle is not alerted. This enables enforcement officials to assign multiple objectives to the vehicle and back-end systems, while not interrupting the priorities of officers on duty.

credential

A credential entity represents a proximity card, a biometrics template, or a PIN required to gain access to a secured area. A credential can only be assigned to one cardholder at a time.

Credential activities

The *Credential activities* task is an investigation task that reports on credential related activities, such as access denied due to expired, inactive, lost, or stolen credentialsl, and so on.

credential code

A credential code is a textual representation of the credential, typically indicating the Facility code and the Card number. For credentials using custom card formats, the user can choose what to include in the credential code.

Credential configuration

The *Credential configuration* task is a maintenance task that reports on credential properties, such as status, assigned cardholder, card format, credential code, custom properties, and so on.

Credential management

The *Credential management* task is an operation task. You can use this task to create, modify, and delete credentials. With this task, you can also print badges and enroll large numbers of card credentials into the system, either by scanning them at a designated card reader or by entering a range of values.

Credential request history

The *Credential request history* task is an investigation task that reports on which users requested, canceled, or printed cardholder credentials.

cumulative security rollup

A cumulative security rollup is a periodic release that contains the latest security fixes and updates for legacy Synergis™ Cloud Link units.

custom event

A custom event is an event added after the initial system installation. Events defined at system installation are called system events. Custom events can be user-defined or automatically added through plugin installations. Unlike system events, custom events can be renamed and deleted.

custom field

A custom field is a user-defined property that is associated with an entity type and is used to store additional information that is useful to your organization.

cyphertext

In cryptography, cyphertext is the encrypted data.

Daily usage per Patroller

The *Daily usage per Patroller* task is an investigation task that reports on the daily usage statistics of a selected patrol vehicle (operating time, longest stop, total number of stops, longest shutdown, and so on) for a given date range.

database server

A database server is an application that manages databases and handles data requests made by client applications. Security Center uses Microsoft SQL Server as its database server.

data ingestion

Data ingestion is the means through which you can import data from external sources into Security Center without having to develop complex code-based integrations.

debounce

A debounce is the amount of time an input can be in a changed state (for example, from active to inactive) before the state change is reported. Electrical switches often cause temporarily unstable signals when changing states, possibly confusing the logical circuitry. Debouncing is used to filter out unstable signals by ignoring all state changes that are shorter than a certain period (in milliseconds).

default expiration delay

The default expiration delay is used for permits supplied by Pay-by-Plate Sync that do not include an expiration. In this case, AutoVu™ Free-Flow checks with the parking permit provider to see if the permit is still valid. Increasing this value reduces the frequency of the permit checks. For example, if the parking lot charges for parking in increments of 15 minutes, and you also set the default expiration delay to 15 minutes, the system validates the permit with the parking provider every 15 minutes.

degraded mode

Degraded mode is an offline operation mode of the interface module when the connection to the Synergis™ unit is lost. The interface module grants access to all credentials matching a specified facility code.

dependent mode

Dependent mode is an online operation mode of the interface module where the Synergis™ unit makes all access control decisions. Not all interface modules can operate in dependent mode.

dewarping

Dewarping is the transformation used to straighten a digital image taken with a fisheye lens.

Diagnostic data collector

The *Diagnostic data collector* is a tool that you can use to collect and package system information to send to Genetec™ Technical Assistance Center for troubleshooting purposes.

digital certificate

A digital certificate, also known as *X.509 certificate*, is a digitally signed document that binds the identity of the certificate owner (a person, a computer, or an organization) to a pair of electronic encryption keys. Digital certificates are used for identity verification, asymmetric cryptography, data-in-transit security, and so on. Digital certificates are the basis for the HTTPS protocol.

digital signature

A digital signature is cryptographic metadata added to video frames by the Archiver or Auxiliary Archiver to ensure their authenticity. If a video sequence is manipulated by adding, deleting, or modifying frames, the signature of the modified content will differ from the original, indicating that the video sequence has been tampered with.

Directory

The Directory role identifies a Security Center system. It manages all entity configurations and system-wide settings. Only a single instance of this role is permitted on your system. The server hosting the Directory role is called the *main server*, and must be set up first. All other servers you add in Security Center are called *expansion servers*, and must connect to the main server to be part of the same system.

Directory authentication

Directory authentication is a Security Center option that forces all client and server applications on a given machine to validate the identity certificate of the Directory before connecting to it. This measure prevents man-in-the-middle attacks.

Directory gateway

Directory gateways allow Security Center applications located on a non-secured network to connect to the main server that is behind a firewall. A Directory gateway is a Security Center server that acts as a proxy for the main server. A server cannot be both a Directory server and a Directory gateway; the former must connect to the Directory database, while the latter must not, for security reasons.

Directory Manager

The Directory Manager role manages the Directory failover and load balancing to produce the high availability characteristics in Security Center.

Directory server

A Directory server is any one of the multiple servers simultaneously running the Directory role in a high availability configuration.

discovery port

A discovery port is a port used by certain Security Center roles (Access Manager, Archiver, ALPR Manager) to find the units they are responsible for on the LAN. No two discovery ports can be the same on one system.

district

A district is a parking regulation characterizing an overtime rule. A district is a geographical area within a city. A vehicle is in violation if it is seen within the boundaries of the district over a specified period of time.

door

A door entity represents a physical barrier. Often, this is an actual door but it could also be a gate, a turnstile, or any other controllable barrier. Each door has two sides, named *In* and *Out* by default. Each side is an access point (entrance or exit) to a secured area.

Door activities

The *Door activities* task is an investigation task that generates reports on door-related activities, such as access denied, door forced open, door open too long, hardware tamper, and so on.

door contact

A door contact monitors the state of a door, whether it is open or closed. It can also be used to detect an improper state, such as door open too long.

door side

Every door has two sides, named *In* and *Out* by default. Each side is an access point to an area. For example, passing through one side leads into an area, and passing through the other side leads out of that area. For the purposes of access management, the credentials that are required to pass through a door in one direction are not necessarily the same that are required to pass through in the opposite direction.

Door troubleshooter

The *Door troubleshooter* task is a maintenance task that lists all the cardholders who have access to a particular door side or elevator floor at a specific date and time.

Driver Development Kit

Driver Development Kit is a SDK for creating device drivers.

duress

A duress is a special code used to disarm an alarm system. This code quietly alerts the monitoring station that the alarm system was disarmed under threat.

dynamic permit

In a system that uses the Pay-by-Plate Sync plugin, a dynamic permit holds a list of vehicles that is updated by a third-party permit provider. For example, in a system where vehicle owners pay for parking at a kiosk or using a mobile phone app, the list of vehicles are dynamically managed by a third-party permit provider.

edge recording

Edge recording is the process of recording and storing recorded videos on the peripheral device, thus removing the need for a centralized recording server or unit. With edge recording, you can store video directly on the camera’s internal storage device (SD card) or on a network attached storage volume (NAS volume).

electric door strike

An electric door strike is an electric device that releases the door latch when current is applied.

elevator

An elevator is an entity that provides access control properties to elevators. For an elevator, each floor is considered an access point.

Elevator activities

The *Elevator activities* task is an investigation task that reports on elevator related activities, such as access denied, floor accessed, unit is offline, hardware tamper, and so on.

encryption certificate

An encryption certificate, also known as a *digital certificate* or *public-key certificate*, is an electronic document that contains a public and private key pair used in Security Center for *fusion stream encryption*. Information encrypted with the *public key* can only be decrypted with the matching *private key*.

enforce

To enforce is to take action following a confirmed hit. For example, a parking officer can enforce a scofflaw violation (unpaid parking tickets) by placing a wheel boot on the vehicle.

entity

Entities are the basic building blocks of Security Center. Everything that requires configuration is represented by an entity. An entity can represent a physical device, such as a camera or a door, or an abstract concept, such as an alarm, a schedule, a user, a role, a plugin, or an add-on.

entity tree

An entity tree is the graphical representation of Security Center entities in a tree structure, illustrating the hierarchical nature of their relationships.

event

In the context of Security Center, an event indicates the occurrence of an activity or incident, such as access denied to a cardholder or motion detected on a camera. Events are automatically logged in Security Center. Every event has an entity as its main focus, called the event source.

event-to-action

An event-to-action links an action to an event. For example, you can configure Security Center to trigger an alarm when a door is forced open.

expansion server

An expansion server is any server machine in a Security Center system that does not host the Directory role. The purpose of the expansion server is to add to the processing power of the system.

extension

An extension refers to a group of manufacturer-specific settings found in the *Extensions* configuration page of a role, such as Archiver, Access Manager, or Intrusion Manager. Most extensions are built-in to Security Center, but some require the installation of an add-on; in those situations, the extension also refers to this add-on.

failover

Failover is a backup operational mode in which a role (system function) is automatically transferred from its primary server to a secondary server that is on standby. This transfer between servers occurs only if the primary server becomes unavailable, either through failure or through scheduled downtime.

false positive read

False positive plate reads can occur when a license plate recognition system mistakes other objects in an image for license plates. For example, lettering on a vehicle or street signs can sometimes create false positive plate reads.

Federal Agency Smart Credential Number

A Federal Agency Smart Credential Number (FASC-N) is an identifier used in the Personal Identity Verification (PIV) credentials issued by US Federal Agencies. FASC-N credential bit lengths vary based on reader configuration; Security Center natively recognizes 75-bit and 200-bit formats.

Federal Information Processing Standard

Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors.

federated entity

A federated entity is any entity that is imported from an independent system through one of the Federation™ roles.

federated identity

A federated identity is a security token that is generated outside of your own realm that you accept. Federated identity enables single sign-on, allowing users to sign on to applications in different realms without needing to enter realm-specific credentials.

federated system

A federated system is a independent system (Omnicast™ or Security Center) that is unified under your local Security Center through a Federation™ role, so that the local users can view and control its entities as if they belong to their local system.

Federation™

The Federation™ feature joins multiple, independent Genetec™ IP security systems into a single virtual system. With this feature, users on the central Security Center system can view and control entities that belong to remote systems.

Federation™ host

The Federation™ host is the Security Center system that runs Federation™ roles. Users on the Federation™ host can view and control entities that belong to federated systems directly from their local system.

Federation™ user

The Federation™ user is the local user account on the remote system that the Federation™ host uses to connect to the remote system. The Federation™ user must have the *Federation*™ privilege. It is used to control what the Federation™ host can access on the remote system.

first-person-in rule

The first-person-in rule is the additional access restriction placed on a secured area that prevents anyone from entering the area until a supervisor is on site. The restriction can be enforced when there is free access (on door unlock schedules) and when there is controlled access (on access rules).

Forensic search

The *Forensic search* task is an investigation task that searches for video sequences based on video analytics events.

four-port RS-485 module

A four-port RS-485 module is a RS-485 communication component of Synergis™ Master Controller with four ports (or channels) named A, B, C, and D. The number of interface modules you can connect to each channel depends on the type of hardware you have.

free access

A free access is an access point state where no credentials are necessary to enter a secured area. The door is unlocked. This is typically used during normal business hours, as a temporary measure during maintenance, or when the access control system is first powered up and is yet to be configured.

free exit

A free exit is an access point state where no credentials are necessary to leave a secured area. The person releases the door by turning the doorknob, or by pressing the REX button, and walks out. An automatic door closer shuts the door so it can be locked after being opened.

fusion stream

Fusion stream is a proprietary data structure of Genetec Inc. for streaming multimedia. Each fusion stream is a bundle of data (video, audio, and metadata) streams and key streams related to a single camera. Fusion streams are generated on specific client requests. The key streams are included only if the data streams are encrypted.

fusion stream encryption

Fusion stream encryption is a proprietary technology of Genetec Inc. used to protect the privacy of your video archives. The Archiver uses a two-level encryption strategy to ensure that only authorized client machines or users with the proper certificates on smart cards can access your private data.

G64

G64 is a Security Center format used by archiving roles (Archiver and Auxiliary Archiver) to store video sequences issued from a single camera. This data format supports audio, bookmarks, metadata overlays, timestamps, motion and event markers, and variable frame rate and resolution.

G64x

G64x is a Security Center format used to store video sequences from multiple cameras that are exported or backed up simultaneously. This data format supports audio, bookmarks, metadata overlays, timestamps, motion and event markers, variable frame rate and resolution, and watermarking.

Genetec Clearance™ Uploader

Genetec Clearance™ Uploader is an application used to automatically upload media from body-worn cameras, sync folders, or other devices to Genetec Clearance™, or a Security Center video archive, depending on which *.json* config file is used.

Genetec Mission Control™

Genetec Mission Control™ is a collaborative decision management system that provides organizations with new levels of situational intelligence, visualization, and complete incident management capabilities. It allows security personnel to make the right decision when faced with routine tasks or unanticipated situations by ensuring a timely flow of information. To learn more about Genetec Mission Control™, refer to the Genetec™ resource center.

Genetec Patroller™

Genetec Patroller™ is the software application installed on an in-vehicle computer that analyzes license plate reads from AutoVu™ Sharp camera units. The application can be installed to operate in different modes to suit your specific enforcement needs and can be configured to notify the vehicle operator if immediate action is required.

Genetec™ Mobile

Official name of the map-based Security Center mobile application for Android and iOS devices.

Genetec™ Protocol

Genetec™ Protocol is a standard protocol developed by Genetec Inc. that third-party video encoder and IP camera manufacturers can use to integrate their products to Security Center Omnicast™.

Genetec™ Server

Genetec™ Server is the Windows service that is at the core of Security Center architecture, and that must be installed on every computer that is part of the Security Center's pool of servers. Every such server is a generic computing resource capable of taking on any role (set of functions) you assign to it.

Genetec™ Update Service

The Genetec™ Update Service (GUS) is automatically installed with most Genetec™ products and enables you to update products when a new release becomes available.

Genetec™ Video Player

Genetec™ Video Player is a standalone media player you can use to view G64 and G64x video files exported from Security Desk. You can also use it to view video on a computer that does not have Security Center installed.

Genetec™ Web App

Genetec™ Web App is the web application that gives users remote access to Security Center so that they can monitor videos, investigate events related to various system entities, search for and investigate alarms, respond to incidents, and generate reports. Users can log on from any computer that has a supported web browser installed.

geocoding

Geocoding, sometimes called forward geocoding, is the process of converting a street address into geographic location, such as a latitude and longitude pair.

Geographic Information System

Geographic Information System (GIS) is a system that captures spatial geographical data. Map Manager can connect to third-party vendors that provide GIS services in order to bring maps and all types of geographically referenced data to Security Center.

georeferencing

Georeferencing is the process of using an object's geographic coordinates (latitude and longitude) to determine its position on a map.

ghost camera

A ghost camera is an entity used as a substitute camera. This entity is automatically created by the Archiver when video archives are detected for a camera whose definition has been deleted from the Directory, either accidentally or because the physical device no longer exists. Ghost cameras cannot be configured, and only exist so users can reference the video archive that would otherwise not be associated to any camera.

ghost patroller

A ghost patroller entity is automatically created by the ALPR Manager when the AutoVu™ license includes the XML Import module. In Security Center, all ALPR data must be associated to a Genetec Patroller™ entity or an ALPR unit corresponding to a fixed Sharp camera. When you import ALPR data from an external source through a specific ALPR Manager using the XML Import module, the system uses the ghost entity to represent the ALPR data source. You can formulate queries using the ghost entity as you would with a normal entity.

global antipassback

Global antipassback is a feature that extends the antipassback restrictions to areas controlled by multiple Synergis™ units.

Global cardholder management

Global cardholder management (GCM) is used to synchronize cardholders between independent Security Center installations. With GCM, you can have a central repository of cardholder information for your entire organization, whether this information is managed from a central office or by individual regional offices.

Global Cardholder Synchronizer

The Global Cardholder Synchronizer role ensures the two-way synchronization of shared cardholders and their related entities between the local system (sharing guest) where it resides and the central system (sharing host).

global entity

A global entity is an entity that is shared across multiple independent Security Center systems by virtue of its membership to a global partition. Only cardholders, cardholder groups, credentials, and badge templates are eligible for sharing.

global partition

Global partition is a partition that is shared across multiple independent Security Center systems by the partition owner, called the sharing host.

grace period

You can add a grace period to a parking session for purposes of lenient enforcement. Following the expiration of the vehicle's paid time or convenience time, the grace period gives extra time before a parking session is flagged as a *Violation*.

hard antipassback

Hard antipassback logs the passback event in the database and prevents the door from being unlocked due to the passback event.

hardening

Hardening is the process of enhancing hardware and software security. When hardening a system, basic and advanced security measures are put in place to achieve a more secure operating environment.

hardware integration package

A hardware integration package, or HIP, is an update that can be applied to Security Center. It enables the management of new functionalities (for example, new video unit types), without requiring an upgrade to the next Security Center release.

Hardware inventory

The *Hardware inventory* task is a maintenance task that reports on the characteristics (unit model, firmware version, IP address, time zone, and so on) of access control, video, intrusion detection, and ALPR units in your system.

hardware zone

A hardware zone is a zone entity in which the I/O linking is executed by a single access control unit. A hardware zone works independently of the Access Manager, and consequently, cannot be armed or disarmed from Security Desk.

hash function

In cryptography, a hash function uses a mathematical algorithm to take input data and return a fixed-size alphanumeric string. A hash function is designed to be a one-way function, that is, a function which is infeasible to revert.

Health history

The *Health history* task is a maintenance task that reports on health issues.

Health Monitor

The Health Monitor role monitors system entities such as servers, roles, units, and client applications for health issues.

Health statistics

The *Health statistics* task is a maintenance task that gives you an overall view of the health of your system by reporting on the availability of selected system entities such as roles, video units, and access control units.

high availability

High availability is a design approach that enables a system to perform at a higher than normal operational level. This often involves failover and load balancing.

hit

A hit is a license plate read that matches a hit rule, such as a hotlist, overtime rule, permit, or permit restriction. A Genetec Patroller™ user can choose to reject or accept a hit. An accepted hit can subsequently be enforced.

hit rule

A hit rule is an ALPR rule used to identify vehicles of interest (called "hits") using license plate reads. The hit rules include the following types: hotlist, overtime rule, permit, and permit restriction.

Hits

The *Hits* task is an investigation task that reports on hits reported within a selected time range and geographic area.

hot action

A hot action is an action mapped to a PC keyboard function key (Ctrl+F1 through Ctrl+F12) in Security Desk for quick access.

hotlist

A hotlist is a list of wanted vehicles, where each vehicle is identified by a license plate number, the issuing state, and the reason why the vehicle is wanted (stolen, wanted felon, Amber alert, VIP, and so on). Optional vehicle information might include the model, the color, and the vehicle identification number (VIN).

Hotlist and permit editor

The *Hotlist and permit editor* task is an operation task. You can use it to edit an existing hotlist or permit list. A new list cannot be created with this task, but after an existing list has been added to Security Center, you can edit, add, or delete items from the list, and the original text file is updated with the changes.

hotspot

A hotspot is a map object that represents an area on the map which requires special attention. Clicking on a hotspot displays associated fixed and PTZ cameras.

I/O configuration

The *I/O configuration* task is a maintenance task that reports on the I/O configurations (controlled access points, doors, and elevators) of access control units.

I/O linking

I/O (input/output) linking is controlling an output relay based on the combined state (normal, active, or trouble) of a group of monitored inputs. A standard application is to sound a buzzer (through an output relay) when any window on the ground floor of a building is shattered (assuming that each window is monitored by a "glass break" sensor connected to an input).

I/O zone

An I/O zone is a zone entity in which the I/O linking can be spread across multiple Synergis™ units, while one unit acts as the master unit. All Synergis™ units involved in an I/O zone must be managed by the same Access Manager. The I/O zone works independently of the Access Manager, but ceases to function if the master unit is down. An I/O zone can be armed and disarmed from Security Desk as long as the master unit is online.

identity certificate

An identity certificate is a *digital certificate* used to authenticate one party to another in a secure communication over a public network. Identity certificates are generally issued by an authority that is trusted by both parties, called a *certificate authority (CA)*.

identity provider

An identity provider is a trusted, external system that administers user accounts, and is responsible for providing user authentication and identity information to relying applications over a distributed network.

illuminator

An illuminator is a light in the Sharp unit that illuminates the plate, thereby improving the accuracy of the images produced by the ALPR camera.

Import tool

The Import tool is the tool that you can use to import cardholders, cardholder groups, and credentials from a comma-separated values (CSV) file.

inactive entity

An inactive entity is an entity that is shaded in red in the entity browser. It signals that the real world entity it represents is either not working, offline, or incorrectly configured.

incident

An incident is an unexpected event reported by a Security Desk user. Incident reports can use formatted text and include events and entities as support material.

incident (Genetec Mission Control™)

A Genetec Mission Control™ incident is an undesirable or unusual situation that needs investigation and resolution, or a routine, scheduled task that requires monitoring.

incident category

An incident category is an entity that represents a grouping of incident types that have similar characteristics.

Incident configuration

The *Incident configuration* task is an administration task that you can use to configure the incident types, the incident categories, and the support documents for Genetec Mission Control™. You can also use this task to generate reports on the changes made to incident types.

Incident Manager

The Incident Manager is the central role that recognizes situational patterns, and triggers incidents in a Genetec Mission Control™ system. This role manages the automation workflows and keeps track of all user activities that are related to incidents.

Incident monitoring

The *Incident monitoring* task is an operation task that you can use to monitor and respond to incidents. From this task, you can see the incidents displayed on a map, thus improving your situational awareness.

incident owner

The incident owner is the incident recipient who took ownership of the incident. Only the incident owner can take actions to resolve the incident. An incident can only have one owner at a time.

incident recipient

An incident recipient is a user or user group that the incident has been dispatched to. Incident recipients can see the incident in the *Incident monitoring* task.

Incident report

The *Incident report* task is an investigation task that you can use to search, review, and analyze Genetec Mission Control™ incidents.

Incidents

The *Incidents* task is an investigation task that you can use to search, review, and modify incident reports created by Security Desk users.

incident supervisor

An incident supervisor is a user who sees an incident in the *Incident monitoring* task because they supervise the incident recipients. Incident supervisors are not incident recipients themselves. A user cannot be both supervisor and recipient of the same incident.

incident trigger

An incident trigger is an event or a sequence of events that can trigger an incident. The Genetec Mission Control™ Rules Engine looks for specific combinations of events (type, time, correlation, and frequency) to determine whether to trigger an incident.

incident type

An incident type entity represents a situation that requires specific actions to resolve it. The incident type entity can also be used to automate the incident detection in Genetec Mission Control™ and to enforce the standard operating procedures that your security team must follow.

interface module

An interface module is a third-party security device that communicates with an access control unit over IP or RS-485, and provides additional input, output, and reader connections to the unit.

interlock

An interlock (also known as sally port or airlock) is an access restriction placed on a secured area that permits only one perimeter door to be open at any given time.

Intrusion detection

The *Intrusion detection* task is an administration task that you can use to configure intrusion detection roles and units.

intrusion detection area

An intrusion detection area entity represents a zone (sometimes called an area) or a partition (group of sensors) on an intrusion panel.

Intrusion detection area activities

The *Intrusion detection area activities* task is an investigation task that reports on activities (master arm, perimeter arm, duress, input trouble, and so on) in selected intrusion detection areas.

intrusion detection unit

An intrusion detection unit entity represents an intrusion device (intrusion panel, control panel, receiver, and so on) that is monitored and controlled by the Intrusion Manager role.

Intrusion detection unit events

The *Intrusion detection unit events* task is an investigation task that reports on events (AC fail, battery fail, unit lost, input trouble, and so on) related to selected intrusion detection units.

Intrusion Manager

The Intrusion Manager role monitors and controls intrusion detection units. It listens to the events reported by the units, provides live reports to Security Center, and logs the events in a database for future reporting.

intrusion panel

An *intrusion panel* (also known as *alarm panel* or *control panel*) is a wall-mounted unit where the alarm sensors (motion sensors, smoke detectors, door sensors, and so on) and wiring of the intrusion alarms are connected and managed.

Inventory management

The *Inventory management* task is an operation task that you can use to add and reconcile license plate reads to a parking facility inventory.

Inventory report

The *Inventory report* task is an investigation task that you can use to view a specific inventory (vehicle location, vehicle length of stay, and so on) or compare two inventories of a selected parking facility (vehicles added, vehicles removed, and so on).

IP camera

An IP camera is a video encoder unit incorporating a camera.

IPv4

IPv4 is the first generation Internet protocol using a 32-bit address space.

IPv6

IPv6 is a 128-bit Internet protocol that uses eight groups of four hexadecimal digits for address space.

Keyhole Markup Language

Keyhole Markup Language (KML) is a file format used to display geographic data in an Earth browser such as Google Earth and Google Maps.

KiwiVision™ Camera Integrity Monitor

KiwiVision™ Camera Integrity Monitor is a Security Center module that ensures cameras are operational at all times by performing regular checks of their video to detect whether the cameras have been tampered with.

KiwiVision™ Privacy Protector™

KiwiVision™ Privacy Protector™ is a Security Center module that ensures the privacy of individuals recorded by video surveillance cameras while safeguarding potential evidence.

Law Enforcement

Law Enforcement is a Genetec Patroller™ software installation that is configured for law enforcement: the matching of license plate reads against lists of wanted license plates (hotlists). The use of maps is optional.

layout

In Security Desk, a layout entity represents a snapshot of what is displayed in a *Monitoring* task. Only the tile pattern and the tile contents are saved, not the tile state.

license key

A license key is the software key used to unlock the Security Center software. The license key is specifically generated for each computer where the Directory role is installed. To obtain your license key, you need the *System ID* (which identifies your system) and the *Validation key* (which identifies your computer).

license plate inventory

A license plate inventory is a list of license plate numbers of vehicles found in a parking facility within a given time period, showing where each vehicle is parked (sector and row).

license plate read

A license plate read is a license plate number captured from a video image using ALPR technology.

live event

A live event is an event that Security Center receives when the event occurs. Security Center processes live events in real-time. Live events are displayed in the event list in Security Desk and can be used to trigger event-to-actions.

live hit

A live hit is a hit matched by the Genetec Patroller™ and immediately sent to the Security Center over a wireless network.

live read

A live read is a license plate captured by the patrol vehicle and immediately sent to Security Center over a wireless network.

load balancing

Load balancing is the distribution of workload across multiple computers.

logical ID

Logical ID is a unique ID assigned to each entity in the system for ease of reference. Logical IDs are only unique within a particular entity type.

Logons per Patroller

The *Logons per Patroller* task is an investigation task that reports on the logon records of a selected patrol vehicle.

long-term overtime

If you need to monitor long-term parking violations for vehicles that are parked for more than a certain number of days, you can configure long-term overtime settings in Genetec Patroller™ and Security Center.

Long-Term Support

The Long-Term Support (LTS) release track offers customers an upgrade path that minimizes changes to software and extends access to critical bug and security fixes. The LTS track includes major and patch versions. Minor versions are excluded. Choosing the LTS track limits your access to new capabilities, but increases stability due to less frequent code change and extends the maintenance period by two years.

LPM protocol

The License Plate Management (LPM) protocol provides a Sharp camera with a secure and reliable connection to Security Center. When The LPM protocol is enabled on a Sharp camera, the protocol manages the camera's connection to the ALPR Manager role.

macro

A macro is an entity that encapsulates a C# program that adds custom functionalities to Security Center.

main server

The main server is the only server in a Security Center system hosting the Directory role. All other servers on the system must connect to the main server to be part of the same system. In a high availability configuration where multiple servers host the Directory role, it is the only server that can write to the Directory database.

major version

A major version is a software version that adds new features, behavioral changes, SDK capabilities, support for new devices, and performance improvements. Using backward compatibility mode, major versions are compatible with up to three previous major versions. A license update is required to upgrade to a new major version. A major version is indicated by a version number with zeros at the third and fourth positions: X.Y.0.0. For more information, see our Product Lifecycle page on GTAP.

man-in-the-middle

In computer security, man-in-the-middle (MITM) is a form of attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

manual capture

Manual capture is when license plate information is entered into the system by the user and not by the ALPR.

map

A map in Security Center is a two-dimensional diagram that helps you visualize the physical locations of your security equipment in a geographical area or a building space.

Map designer

The *Map designer* task is an administration task that you can use to create and edit maps that represent the physical locations of your equipment to Security Desk users.

map link

A map link is a map object that brings you to another map with a single click.

Map Manager

The Map Manager is the central role that manages all mapping resources in Security Center, including imported map files, external map providers, and KML objects. It acts as the map server for all client applications that require maps and as the *record provider* for all Security Center entities placed on georeferenced maps. The Map Manager role replaced the Plan Manager role in Security Center 5.4 GA.

map mode

Map mode is a Security Desk canvas operating mode that replaces tiles and controls with a geographical map showing all active, georeferenced events in your system. Switching to Map mode is a feature that comes with AutoVu™, Correlation, or Genetec Mission Control™, and requires a license for one of these major features.

map object

Map objects are graphical representations on your maps of Security Center entities or geographical features, such as cities, highways, rivers, and so on. With map objects, you can interact with your system without leaving your map.

map preset

A map preset is a saved map view. Every map has at least one preset, called the *default view*, that is displayed when a user opens the map.

Maps

The *Maps* task is an operation task that heightens your situational awareness by providing the context of a map to your security monitoring and control activities.

map view

A map view is a defined section of a map.

master arm

Master arm is arming an intrusion detection area in such a way that all sensors attributed to the area would set the alarm off if one of them is triggered.

master key stream

In *fusion stream encryption*, the master key stream is the sequence of symmetric keys generated by the Archiver to encrypt one data stream. The symmetric keys are randomly generated and change every minute. For security reasons, the master key stream is never transmitted or stored anywhere as plaintext.

maximum session time

Setting a maximum session time helps to improve parking lot occupancy statistics. When a vehicle exceeds the maximum session time, it is assumed that the vehicle's plate was not read at the exit and the vehicle is no longer in the parking zone. The parking session appears in reports generated from the *Parking sessions* task with the *State reason: Maximum session time exceeded*.

max occupancy

The *max occupancy* feature monitors the number of people in an area, up to a configured limit. Once the limit is reached, the rule will either deny access to additional cardholders (if set to *Hard*) or trigger events while allowing further access (*Soft*).

Media Gateway

The Media Gateway role is used by Genetec™ Mobile, Web Client, and the Genetec™ Web App to get transcoded video from Security Center. The Media Gateway role supports the Real Time Streaming Protocol (RTSP), which external applications can use to request raw video streams from Security Center.

Media Router

The Media Router role is the central role that handles all stream requests (audio and video) in Security Center. It establishes streaming sessions between the stream source, such as a camera or an Archiver, and its requesters (client applications). Routing decisions are based on the location (IP address) and the transmission capabilities of all parties involved (source, destinations, networks, and servers).

minor version

A minor version is a software version that adds new features, SDK capabilities, support for new devices, bug fixes, and security fixes. Different system components can run at different minor versions, provided they share the same major version. No license update is required to upgrade to a new minor version. A minor version is indicated by a version number with a zero at the fourth position: X.Y.Z.0. For more information, see our Product Lifecycle page on GTAP.

missing file

A missing file is a video file that is still referenced by an archive database, but cannot be accessed anymore. This situation occurs when video files are deleted manually without using the *Archive storage details* task, creating a mismatch between the number of video files referenced in the database and the actual number of video files stored on disk.

Mobile Admin

(Obsolete as of SC 5.8 GA) Mobile Admin is a web-based administration tool used to configure the Mobile Server.

mobile credential

A mobile credential is a credential on a smartphone that uses Bluetooth or Near Field Communication (NFC) technology to access secured areas.

Mobile Credential Manager

The Mobile Credential Manager role links Security Center to your third-party mobile credential provider so that you can view your subscription status, and manage your mobile credentials and profiles in Config Tool.

mobile credential profile

A mobile credential profile links a part number from your mobile credential provider to your subscription so that you can create mobile credentials in Security Center.

Mobile Data Computer

Mobile Data Computer is a tablet computer or ruggedized laptop used in patrol vehicles to run the Genetec Patroller™ application. The MDC is typically equipped with a touch-screen with a minimum resolution of 800 x 600 pixels and wireless networking capability.

Mobile License Plate Inventory

Mobile License Plate Inventory (MLPI) is the Genetec Patroller™ software installation that is configured for collecting license plates and other vehicle information for creating and maintaining a license plate inventory for a large parking area or parking garage.

Mobile Server

The Mobile Server role provides Security Center access on mobile devices.

monitor group

A monitor group is an entity used to designate analog monitors for alarm display. Besides the monitor groups, the only other way to display alarms in real time is to use the *Alarm monitoring* task in Security Desk.

monitor ID

Monitor ID is an ID used to uniquely identify a workstation screen controlled by Security Desk.

Monitoring

The *Monitoring* task is an operation task that you can use to monitor and respond to real-time events that relate to selected entities. Using the *Monitoring* task, you can also monitor and respond to alarms.

motion detection

Motion detection is the feature that watches for changes in a series of video images. The definition of what constitutes motion in a video can be based on highly sophisticated criteria.

Motion search

The *Motion search* task is an investigation task that searches for motion detected in specific areas of a camera's field of view.

motion zone

A motion zone is a user defined areas within a video image where motion should be detected.

Move unit

Move unit tool is used to move units from one manager role to another. The move preserves all unit configurations and data. After the move, the new manager immediately takes on the command and control function of the unit, while the old manager continues to manage the unit data collected before the move.

multi-factor authentication

Multi-factor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user’s identity for a login or other transaction.

multi-tenant parking

If you use AutoVu™ Free-Flow to manage transient parking and contract permit parking in parking zones, you can install the AutoVu™ Free-Flow plugin to manage parking lots where parking spots are leased to tenants.

network

The network entity is used to capture the characteristics of the networks used by your system so that proper stream routing decisions can be made.

network address translation

Network address translation is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device, for the purpose of remapping one IP address space into another.

network view

The network view is a browser view that illustrates your network environment by showing each server under the network they belong to.

Network view

The *Network view* task is an administration task that you can use to configure your networks and servers.

new wanted

A new wanted is a manually entered hotlist item in Genetec Patroller™. When you are looking for a plate that does not appear in the hotlists loaded in the Genetec Patroller™, you can enter the plate in order to raise a hit if the plate is captured.

notification tray

The notification tray contains icons that allow quick access to certain system features, and also displays indicators for system events and status information. The notification tray display settings are saved as part of your user profile and apply to both Security Desk and Config Tool.

OCR equivalence

OCR equivalence is the interpretation of OCR (Optical Character Recognition) equivalent characters performed during license plate recognition. OCR equivalent characters are visually similar, depending on the plate's font. For example, the letter "O" and the number "0", or the number "5" and the letter "S". There are several pre-defined OCR equivalent characters for different languages.

officer

An officer, or wearable camera user, is an entity that identifies a person who holds a body-worn camera license and uploads video evidence to Genetec Clearance™ or a Security Center video archive. Officers are automatically added when a camera is connected to the Genetec Clearance™ Uploader, but can also be added and modified manually.

offline event

An offline event is an event that occurs while the event source is offline. Security Center only receives the offline events when the event source is back online.

Omnicast™

Security Center Omnicast™ is the IP video management system (VMS) that provides organizations of all sizes the ability to deploy a surveillance system adapted to their needs. Supporting a wide range of IP cameras, it addresses the growing demand for HD video and analytics, all the while protecting individual privacy.

Omnicast™ compatibility pack

Omnicast™ compatibility pack is the software component that you need to install to make Security Center compatible with an Omnicast™ 4.x system. Please note Omnicast™ 4.8 has reached End of Life. For more information, see the Genetec™ Product Lifecyle page.

Omnicast™ Federation™

The Omnicast™ Federation™ role connects an Omnicast™ 4.x system to Security Center. That way, the Omnicast™ entities and events can be used in your Security Center system. Please note Omnicast™ 4.8 has reached End of Life. For more information, see the Genetec™ Product Lifecyle page.

orphan file

An orphan file is a video file that is no longer referenced by any archive database. Orphan files remain on the disk until they are manually deleted. This situation occurs when the archive database is changed inadvertently, creating a mismatch between the number of video files referenced in the database and the actual number of video files stored on disk.

output behavior

An output behavior is an entity that defines a custom output signal format, such as a pulse with a delay and duration.

overtime rule

An overtime rule is an entity that defines a parking time limit and the maximum number of violations enforceable within a single day. Overtime rules are used in city and university parking enforcement. For university parking, an overtime rule also defines the parking area where these restrictions apply.

paid time

The paid time stage of a parking session begins when the *convenience time* expires. Vehicle owners can purchase parking time through a pay station or mobile app, and the payment system can be provided by integrated third-party parking permit providers.

parking facility

A parking facility entity defines a large parking area as a number of sectors and rows for the purpose of inventory tracking.

parking lot

A parking lot is a polygon that defines the location and shape of a parking area on a map. By defining the number of parking spaces inside the parking lot, Security Center can calculate its percentage of occupancy during a given time period.

parking rule

A parking rule defines how and when a parking session is either considered to be valid or in violation.

parking session

The AutoVu™ Free-Flow feature in Security Center uses parking sessions to track each vehicle's stay in a parking zone. A parking session is divided into four states: *Valid* (including convenience time, paid time, and grace period), *Violation*, *Enforced*, and *Completed*.

Parking sessions

The *Parking sessions* task is an investigation task that you can use to generate a list of vehicles that are currently in violation. You can create a vehicle inventory report for the current parking zone occupancy or for a specific time in the past based on the selected time filter.

parking session states

A vehicle's parking session is divided into four states: *Valid* (including convenience time, paid time, and grace period), *Violation*, *Enforced*, and *Completed*. When a vehicle parks in a parking zone, its parking session progresses through the parking session states based on the timing that is configured for the parking rule, the validity of the paid time, and whether the vehicle's parking session incurs a violation.

parking zone

The parking zones that you define in Security Center represent off-street parking lots where the entrances and exits are monitored by Sharp cameras.

Parking zone activities

The *Parking zone activities* task is an investigation task that you can use to track the parking zone-related events that occur between the time the vehicle's plate is read at the entrance and at the exit of the parking zone.

parking zone capacity

The parking zone capacity is the maximum number of vehicles that can be parked in a parking zone.

parking zone capacity threshold

The parking zone capacity threshold setting determines at what point a *capacity threshold reached* event is generated. For example, if you lower the threshold to 90%, the system generates an event when the parking zone reaches 90% capacity.

partition

A partition is an entity in Security Center that defines a set of entities that are only visible to a specific group of users. For example, a partition could include all areas, doors, cameras, and zones in one building.

patch version

A patch version is a software version that adds support for new devices, bug fixes, and security fixes. Patch versions do not affect system compatibility, as long as all your system components are at the same major version. If you are on the Long-Term Support (LTS) track, patch versions only include critical bug and security fixes. A patch version is indicated by a version number where the fourth position is not a zero. For more information, see our Product Lifecycle page on GTAP.

Patroller Config Tool

Genetec Patroller™ Config Tool is the Genetec Patroller™ administrative application used to configure Patroller-specific settings, such as adding Sharp cameras to the in-vehicle LAN, enabling features such as Manual Capture or New Wanted, and specifying that a username and password are needed to log on to Genetec Patroller™.

patroller entity

A patroller entity in Security Center represents a patrol vehicle equipped with an in-vehicle computer running Genetec Patroller™ software.

Patroller tracking

The *Patroller tracking* task is an investigation task that you can use to replay the route followed by a patrol vehicle on a given date on a map, or view the current location of patrol vehicles on a map.

patrol vehicle

A patrol vehicle monitors parking lots and city streets for parking violations or wanted vehicles. A patrol vehicle includes one or more Sharp automatic license plate recognition (ALPR) cameras and an in-vehicle computer running Genetec Patroller™ software.

People counting

The *People counting* task is an operation task that keeps count in real-time of the number of cardholders in all secured areas of your system.

perimeter arm

Perimeter arm is arming an intrusion detection area in such a way that only sensors attributed to the area perimeter set the alarm off if triggered. Other sensors, such as motion sensors inside the area, are ignored.

permit

A permit is an entity that defines a single parking permit holder. Each permit holder is characterized by a category (permit zone), a license plate number, a license issuing state, and optionally, a permit validity range (effective date and expiry date). Permits are used in both city and university parking enforcement.

permit hit

A permit hit is a hit that is generated when a read (license plate number) does not match any entry in a permit or when it matches an invalid permit.

permit restriction

A permit restriction is an entity that applies time restrictions to a series of parking permits for a given parking area. Permit restrictions can be used by patrol vehicles configured for University Parking Enforcement and for systems that use the AutoVu™ Free-Flow feature.

plaintext

In cryptography, plaintext is the data that is not encrypted.

Plate Reader

Plate Reader is the software component of the Sharp unit that processes the images captured by the ALPR camera to produce license plate reads, and associates each license plate read with a context image captured by the context camera. The Plate Reader also handles the communications with the Genetec Patroller™ and the ALPR Manager. If an external wheel imaging camera is connected to the Sharp unit, the Plate Reader also captures wheel images from this camera.

plugin

A plugin (in lowercase) is a software component that adds a specific feature to an existing program. Depending on the context, plugin can refer either to the software component itself or to the software package used to install the software component.

Plugin

Plugin (with an uppercase, in singular) is the role template that serves to create specific plugin roles.

plugin role

A plugin role adds optional features to Security Center. A plugin role is created by using the *Plugin* role template. By default, it is represented by an orange puzzle piece in the *Roles* view of the *System* task. Before you can create a plugin role, the software package specific to that role must be installed on your system.

Plugins

The *Plugins* task is an administration task that you can use to configure plugin-specific roles and related entities.

Powered by Genetec

Powered by Genetec is a Genetec™ program where Genetec Inc. works with its partners to deploy Genetec™ software directly on their devices or firmware. *Axis Powered by Genetec* is the first application of this program.

primary server

The primary server is the default server chosen to perform a specific function (or role) in the system. To increase the system's fault-tolerance, the primary server can be protected by a secondary server on standby. When the primary server becomes unavailable, the secondary server automatically takes over.

privacy protection

In Security Center, privacy protection is software that anonymizes or masks parts of a video stream where movement is detected. The identity of individuals or moving objects is protected, without obscuring movements and actions or preventing monitoring.

Privacy Protector™

The Privacy Protector™ role requests original video streams from Archiver roles and applies data anonymization to the original video streams. The privacy-protected (anonymized) video stream is then sent back to the Archiver role for recording.

private IP address

A private IP address is an IP address chosen from a range of addresses that are only valid for use on a LAN. The ranges for a private IP address are: 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.16.255.255, and 192.168.0.0 to 192.168.255.255. Routers on the Internet are normally configured to discard any traffic using private IP addresses.

private key

In cryptography, a private or secret key is either an encryption or decryption key known only to one of the parties that exchange secret messages.

private task

A private task is a saved task that is only visible to the user who created it.

privilege

Privileges define what users can do, such as arming zones, blocking cameras, and unlocking doors, over the part of the system they have access rights to.

Privilege troubleshooter

The Privilege troubleshooter is a tool that helps you investigate the allocation of user privileges in your Security Center system. With this tool, you can discover:

- Who has permission to work with a selected entity
- What privileges are granted to selected users or groups
- Who has been granted a privilege, has access to a specific entity, or both

public key

In cryptography, a public key is a value provided by a designated authority as an encryption key that, combined with a private key that is generated at the same time, can be used to effectively encrypt messages and verify digital signatures.

public-key encryption

Public-key encryption, also known as asymmetric encryption, is a type of encryption where two different keys are used to encrypt and decrypt information. The private key is a key that is known only to its owner, while the public key can be shared with other entities on the network. What is encrypted with one key can only be decrypted with the other key.

public-key infrastructure

A public-key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to support the distribution and identification of public encryption keys. This enables users and computers to securely exchange data over networks such as the Internet and verify the identity of the other party.

public task

A public task is a saved task that can be shared and reused among multiple Security Center users.

reader

A reader is a sensor that reads the credential for an access control system. For example, this can be a card reader, or a biometrics scanner.

read rate

The read rate measures the speed at which a license plate recognition system can correctly detect and read all of the characters in an image of a license plate.

Reads

The *Reads* task is an investigation task that reports on license plate reads performed within a selected time range and geographic area.

Reads/hits per day

The *Reads/hits per day* task is an investigation task that reports on license plate reads performed within a selected time range and geographic area.

Reads/hits per zone

The *Reads/hits per zone* task is an investigation task that reports on the number of reads and hits per parking area for a selected date range.

realm

In identity terms, a realm is the set of applications, URLs, domains, or sites for which a token is valid. Typically a realm is defined using an Internet domain such as genetec.com, or a path within that domain, such as genetec.com/support/GTAC. A realm is sometimes described as a security domain because it encompasses all applications within a specified security boundary.

record cache

The record cache is the database where the Record Caching Service role keeps copies of records ingested from external data sources in Security Center. You can generate reports on the cached records using the *Records* investigation task.

Record Caching Service

The Record Caching Service role is used for *data ingestion*. Using this role, you can import records from external data sources into Security Center. You can share the ingested data across the entire unified platform to enhance awareness and response, to provide contextual information on dynamic maps, or to visualize in operational dashboards.

Record Fusion Service

The Record Fusion Service is the central role that provides a unified querying mechanism for data records that come from a wide variety of sources, such as Security Center modules or third-party applications. All record requests go through this role, which then queries their respective record providers.

recording mode

Recording mode is the criteria by which the system schedules the recording of video streams. There are four possible recording modes:

- **Continuous**. Records continuously.
- **On motion/Manual**. Records according to motion detection settings, and when a user or system action requests it.
- **Manual**. Records only when a user or system action requests it.
- **Off**. No recording is permitted.

recording state

Recording state is the current recording status of a given camera. There are four possible recording states: *Enabled*, *Disabled*, *Currently recording (unlocked)*, and *Currently recording (locked)*.

record provider

A record provider is either a Security Center role or an SDK application that connects a data source to the Record Fusion Service role.

Records

Renamed to *Unified report* in Security Center 5.11.2.0.

record type

In Security Center, a record type defines the data format and display properties of a set of records that you can share across the entire system through the Record Fusion Service role.

redirector

A redirector is a server assigned to host a redirector agent created by the Media Router role.

redirector agent

A redirector agent is an agent created by the Media Router role to redirect data streams from one IP endpoint to another.

redundant archiving

Redundant archiving is an option to enhance the availability of video and audio archives during failover and to protect against data loss. If you enable this option, all servers assigned to an Archiver role archive video, and audio, at the same time.

Remote

The *Remote* task is an operation task that you can use to remotely monitor and control other Security Desk applications in your system that are running the *Monitoring* task or the *Alarm monitoring* task.

Remote configuration

The *Remote configuration* task is an administration task that you can use to configure federated Security Center entities without logging off from your local Config Tool.

rendering rate

Rendering rate is the comparison of how fast the workstation renders a video with the speed the workstation receives that video from the network.

Report Manager

The Report Manager role automates report emailing and printing based on schedules.

report pane

The report pane is one of the panes found in the Security Desk workspace. It displays query results or real-time events in a tabular form.

request to exit

Request to exit (REX) is a door release button normally located on the inside of a secured area that when pressed, allows a person to exit the secured area without having to show any credential. This can also be the signal from a motion detector. It is also the signal received by the controller for a request to exit.

restricted camera

Restricted cameras are cameras that Genetec Inc. has identified as cybersecurity risks.

reverse geocoding

Reverse geocoding is the process of converting a geographic location, such as a latitude and longitude pair, into a human-readable address.

reverse tunnel

A reverse tunnel is a private communication channel open between a server inside a secured LAN and a client outside. In the Security Center implementation, certificate authentication is used to protect against man-in-the-middle attacks.

reverse tunneling

Reverse tunneling is a technique used on servers protected behind a firewall to avoid having to open inbound ports to receive requests from clients found on the other side of the firewall. Instead of having the client contact the server, the communication is reversed. The client generates a keyfile that includes an identity certificate about itself that the server uses to contact the client, hence, eliminating the need to open any inbound port on the server. For more information, see "What is Reverse Tunneling?" in the Cloud-Hosted Security Center SaaS Edition Deployment Guide.

role

A role is a software component that performs a specific job within Security Center. To execute a role, you must assign one or more servers to host it.

roles and units view

The roles and units view is a browser view that lists the roles on your system with the units they control as child entities.

route

A route is a setting that configures the transmission capabilities between two end points in a network for the purpose of routing media streams.

Rules Engine

The Rules Engine is the component of the Genetec Mission Control™ system that analyzes and correlates the events collected by Security Center, based on predefined rules. The Rules Engine uses these events to detect and trigger incidents in the Genetec Mission Control™ system.

same position

The *same position* regulation is a type of parking regulation characterizing an overtime rule. A vehicle is in violation if it is seen parked at the exact same spot over a specified period of time. Genetec Patroller™ must be equipped with GPS capability to enforce this type of regulation.

schedule

A schedule is an entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).

scheduled task

A scheduled task is an entity that defines an action that executes automatically on a specific date and time, or according to a recurring schedule.

SDK certificate

An SDK certificate is what an SDK application (or plugin) needs to connect to Security Center. The certificate must be included in the Security Center license key for the SDK application to work.

secondary server

A secondary server is an alternative server on standby intended to replace the primary server in case the latter becomes unavailable.

secured area

A secured area is an area entity that represents a physical location where access is controlled. A secured area consists of perimeter doors (doors used to enter and exit the area) and access restrictions (rules governing the access to the area).

Secure Socket Layer

The Secure Sockets Layer (SSL) is a computer networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients.

Security Center

Security Center is a truly unified platform that blends IP video surveillance, access control, automatic license plate recognition, intrusion detection, and communications within one intuitive and modular solution. By taking advantage of a unified approach to security, your organization becomes more efficient, makes better decisions, and responds to situations and threats with greater confidence.

Security Center Federation™

The Security Center Federation™ role connects a remote independent Security Center system to your local Security Center system. That way, the remote system's entities and events can be used in your local system.

Security Center Mobile

(Obsolete) See Mobile Server and Genetec™ Mobile.

Security Center Mobile application

(Obsolete) See Genetec™ Mobile.

Security Center SaaS edition

The Security Center SaaS edition is Security Center offered by subscription. Subscription-based ownership simplifies the transition to cloud services and provides an alternative way to purchase, deploy, and maintain the Genetec™ Security Center unified platform.

security clearance

A security clearance is a numerical value used to further restrict the access to an area when a threat level is in effect. Cardholders can only enter an area if their security clearance is equal or higher than the minimum security clearance set on the area.

Security Desk

Security Desk is the unified user interface of Security Center. It provides consistent operator flow across all of the Security Center main systems, Omnicast™, Synergis™, and AutoVu™. The unique task-based design of Security Desk lets operators efficiently control and monitor multiple security and public safety applications.

security token

An on-the-wire representation of claims that is cryptographically signed by the issuer of the claims, providing strong proof to any relying party as to the integrity of the claims and the identity of the issuer.

Security video analytics

The *Security video analytics* task is an investigation task that reports on video analytics events that are triggered based on analytics scenarios.

self-signed certificate

A self-signed certificate is an *identity certificate* that is signed by the same entity whose identity it certifies, as opposed to a *certificate authority (CA)*. Self-signed certificates are easy to make and do not cost money. However, they do not provide all of the security properties that certificates signed by a CA aim to provide.

server

In Security Center, a server entity represents a computer on which the Genetec™ Server service is installed.

Server Admin

Server Admin is the web application running on every server machine in Security Center that you use to configure the Genetec™ Server settings. You use this same application to configure the Directory role on the main server.

server certificate

A server certificate is an *identity certificate* used to authenticate the server's identity to the client. Server certificates are also used to encrypt data-in-transit to ensure data confidentiality.

server mode

The server mode is a special online operation mode restricted to Synergis™ units, in which the unit allows the Access Manager (the server) to make all access control decisions. The unit must stay connected to the Access Manager at all times to operate in this mode.

sharing guest

A sharing guest is a Security Center system that has been given the rights to view and modify entities owned by another Security Center system, called the sharing host. Sharing is done by placing the entities in a global partition.

sharing host

A sharing host is a Security Center system that gives the right to other Security Center systems to view and modify its entities by putting them up for sharing in a global partition.

SharpOS

SharpOS is the software component of a Sharp unit. SharpOS is responsible for everything related to plate capture, collection, processing, and analytics. For example, a SharpOS update can include new ALPR contexts, new firmware, Sharp Portal updates, and updates to the Sharp's Windows services (Plate Reader, HAL, and so on).

Sharp Portal

Sharp Portal is a web-based administration tool used to configure Sharp cameras for AutoVu™ systems. From a web browser, you log on to a specific IP address (or the Sharp name in certain cases) that corresponds to the Sharp you want to configure. When you log on, you can configure options such as selecting the ALPR context (for example, Alabama, Oregon, Quebec), selecting the read strategy (for example, fast moving or slow moving vehicles), viewing the Sharp’s live video feed, and more.

Sharp unit

The Sharp unit is a proprietary ALPR unit of Genetec Inc. that integrates license plate capturing and processing components, as well as digital video processing functions, inside a ruggedized casing.

SharpV

SharpV is a Sharp unit that is specialized for fixed installations. It is ideally suited for a range of applications, from managing off-street parking lots and facilities to covering major city access points to detect wanted vehicles. SharpV combines two high-definition cameras with onboard processing and illumination in a ruggedized, environmentally sealed unit. Both lenses are varifocal for ease of installation and the camera is powered via PoE+.

SharpX

SharpX is the camera component of the SharpX system. The SharpX camera unit integrates a pulsed LED illuminator that works in total darkness (0 lux), a monochrome ALPR camera (1024 x 946 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The ALPR data captured by the SharpX camera unit is processed by a separate hardware component called the AutoVu™ ALPR Processing Unit.

SharpZ3

SharpZ3 is a proprietary mobile ALPR system designed by Genetec Inc. that integrates license plate cameras and a trunk unit that is responsible for ALPR processing as well as communication with the Genetec Patroller™ software running on the in-vehicle computer.

SharpZ3 base unit

The SharpZ3 base unit is the processing component of the SharpZ3 system. The base unit includes the ALPR module and up to three expansion modules that are used to add features to the system such as precise navigation, PoE ports for wheel imaging cameras, and so on.

single sign-on

Single sign-on (SSO) is the use of a single user authentication for multiple IT systems or even organizations.

soft antipassback

Soft antipassback only logs the passback events in the database. It does not restrict the door from being unlocked due to the passback event.

Software Development Kit

The Software Development Kit (SDK) is what end-users use to develop custom applications or custom application extensions for Security Center.

standalone mode

Standalone mode is an operation mode where the interface module makes autonomous decisions based on the access control settings previously downloaded from the Synergis™ unit. When the module is online, activity reporting occurs live. When the module is offline, activity reporting occurs on schedule, or when the connection to the unit is available. Not all interface modules can operate in standalone mode.

standard schedule

A standard schedule is a schedule entity that can be used in all situations. Its only limitation is that it does not support daytime or nighttime coverage.

static permit

In a system that uses the Pay-by-Plate Sync plugin, a static permit holds a list of vehicle license plates that is not updated by a third-party permit provider. For example, a list of employee vehicles that are authorized to park in the lot are manually maintained as a static list.

strict antipassback

A strict antipassback is an antipassback option. When enabled, a passback event is generated when a cardholder attempts to leave an area that they were never granted access to. When disabled, Security Center only generates passback events for cardholders entering an area that they never exited.

supervised mode

Supervised mode is an online operation mode of the interface module where the interface module makes decisions based on the access control settings previously downloaded from the Synergis™ unit. The interface module reports its activities in real time to the unit, and allows the unit to override a decision if it contradicts the current settings in the unit. Not all interface modules can operate in supervised mode.

SV appliance

A Streamvault™ is a turnkey appliance that comes with an embedded operating system and Security Center pre-installed. You can use Streamvault™ appliances to quickly deploy a unified or standalone video surveillance and access control system.

SV Control Panel

SV Control Panel is a user interface application that you can use to configure your Streamvault™ appliance to work with Security Center access control and video surveillance.

symmetric encryption

Symmetric encryption is a type of encryption where the same key is used for both encryption and decryption.

synchronous video

A synchronous video is a simultaneous live video or playback video from more than one camera that are synchronized in time.

Synergis™

Security Center Synergis™ is the IP access control system (ACS) that heightens your organization's physical security and increases your readiness to respond to threats. Synergis™ supports an ever-growing portfolio of third-party door control hardware and electronic locks. Using Synergis™, you can leverage your existing investment in network and security equipment.

Synergis™ appliance

A Synergis™ appliance is an IP-ready security appliance manufactured by Genetec Inc. that is dedicated to access control functions. All Synergis™ appliances come pre-installed with Synergis™ Softwire and are enrolled as access control units in Security Center.

Synergis™ Appliance Portal

The Synergis™ Appliance Portal is the web-based administration tool used to configure and administer the Synergis™ appliance and upgrade its firmware.

Synergis™ Cloud Link

Synergis™ Cloud Link is an intelligent PoE-enabled IoT gateway designed to address the demand for a non-proprietary access control solution. Synergis™ Cloud Link provides native support for a wide variety of intelligent controllers and electronic locks.

Synergis™ IX

Synergis™ IX (pronounced "eye-ex") is a family of hybrid controllers and downstream modules used to manage both access control points and intrusion points. The Synergis™ IX product line is only available to the Australian and New Zealand markets.

Synergis™ Master Controller

Synergis™ Master Controller (SMC) is an access control appliance of Genetec Inc. that supports various third-party interface modules over IP and RS-485. SMC is seamlessly integrated with Security Center and can make access control decisions independently of the Access Manager.

Synergis™ Softwire

Synergis™ Softwire is the access control software developed by Genetec Inc. to run on various IP-ready security appliances. Synergis™ Softwire lets these appliances communicate with third-party interface modules. A security appliance running Synergis™ Softwire is enrolled as an access control unit in Security Center.

Synergis™ unit

A Synergis™ unit is a Synergis™ appliance that is enrolled as an access control unit in Security Center.

System

The *System* task is an administration task that you can use to configure roles, macros, schedules, and other system entities and settings.

System Availability Monitor

With System Availability Monitor (SAM) running, you can collect health information and view the health status of your Security Center systems to prevent and proactively resolve technical issues.

System Availability Monitor Agent

The System Availability Monitor Agent (SAMA) is the component of SAM that is installed on every Security Center main server. SAMA collects health information from Security Center and sends health information to the Health Monitoring Services in the cloud.

system event

A system event is a predefined event that indicates the occurrence of an activity or incident. System events are defined by the system and cannot be renamed or deleted.

System status

The *System status* task is a maintenance task that you can use to monitor the status of all entities of a given type in real time and to interact with them.

task

A task is the central concept on which the entire Security Center user interface is built. Each task corresponds to one aspect of your work as a security professional. For example, use a monitoring task to monitor system events in real-time, use an investigation task to discover suspicious activity patterns, or use an administration task to configure your system. All tasks can be customized and multiple tasks can be carried out simultaneously.

taskbar

A taskbar is a user interface element of the Security Center client application window, composed of the *Home* tab and the active task list. The taskbar can be configured to be displayed on any edge of the application window.

task cycling

A task cycling is a Security Desk feature that automatically cycles through all tasks in the active task list following a fixed dwell time.

task workspace

A task workspace is an area in the Security Center client application window reserved for the current task. The workspace is typically divided into the following panes: canvas, report pane, controls, and area view.

temporary access rule

A temporary access rule is an access rule that has an activation and an expiration time. Temporary access rules are suited for situations where permanent cardholders need to have temporary or seasonal access to restricted areas. These access rules are automatically deleted seven days after they expire to avoid cluttering the system.

third-party authentication

Third-party authentication uses a trusted, external identity provider to validate user credentials before granting access to one or more IT systems. The authentication process returns identifying information, such as a username and group membership, that is used to authorize or deny the requested access.

threat level

Threat level is an emergency handling procedure that a Security Desk operator can enact on one area or the entire system to deal promptly with a potentially dangerous situation, such as a fire or a shooting.

tile

A tile is an individual window within the canvas, used to display a single entity. The entity displayed is typically the video from a camera, a map, or anything of a graphical nature. The look and feel of the tile depends on the displayed entity.

tile ID

The tile ID is the number displayed at the upper left corner of the tile. This number uniquely identifies each tile within the canvas.

tile mode

Tile mode is the main Security Desk canvas operating mode that presents information in separate tiles.

tile pattern

The tile pattern is the arrangement of tiles within the canvas.

tile plugin

A tile plugin is a software component that runs inside a Security Desk tile. By default, it is represented by a green puzzle piece in the area view.

Time and attendance

The *Time and attendance* task is an investigation task that reports on who has been inside a selected area and the total duration of their stay within a given time range.

timed antipassback

Timed antipassback is an antipassback option. When Security Center considers a cardholder to be already in an area, a passback event is generated when the cardholder attempts to access the same area again during the time delay defined by *Presence timeout*. When the time delay has expired, the cardholder can once again pass into the area without generating a passback event.

timeline

A timeline is a graphic illustration of a video sequence, showing where in time, motion and bookmarks are found. Thumbnails can also be added to the timeline to help the user select the segment of interest.

transfer group

A transfer group is a persistent archive transfer scenario that lets you run a video transfer without redefining the transfer settings. These transfers can be scheduled or executed on demand. Transfer groups define which cameras or archiving roles are included in the transfer, when the archives are transferred, what data is transferred, and so on.

transient parking

Transient parking is a parking scenario where the driver must purchase parking time as soon as the vehicle enters the parking lot.

Transmission Control Protocol

A connection-oriented set of rules (protocol) that, along with the IP (Internet Protocol), is used to send data over an IP network. The TCP/IP protocol defines how data can be transmitted in a secure manner between networks. TCP/IP is the most widely used communications standard and is the basis for the Internet.

Transport Layer Security

Transport Layer Security (TLS) is a protocol that provides communications privacy and data integrity between two applications communicating over a network. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

twilight schedule

A twilight schedule is a schedule entity that supports both daytime and nighttime coverages. A twilight schedule cannot be used in all situations. Its primary function is to control video related behaviors.

two-person rule

The two-person rule is the access restriction placed on a door that requires two cardholders (including visitors) to present their credentials within a certain delay of each other in order to gain access.

Unified report

The *Unified report* is an investigation task that you can use to query the *record types* available to you.

unit

A unit is a hardware device that communicates over an IP network that can be directly controlled by a Security Center role. We distinguish four types of units in Security Center:

- Access control units, managed by the Access Manager role
- Video units, managed by the Archiver role
- ALPR units, managed by the ALPR Manager role
- Intrusion detection units, managed by the Intrusion Manager role

Unit Assistant

The Unit Assistant is the central role that manages system-wide security operations, such as updating unit passwords and renewing unit certificates, on supported access control and video units.

Unit discovery tool

Starting with Security Center 5.4 GA the Unit discovery tool has been replaced by the Unit enrollment tool.

Unit enrollment

Unit enrollment is a tool that you can use to discover IP units (video and access control) connected to your network, based on their manufacturer and network properties (discovery port, IP address range, password, and so on). After you discovered a unit, you can add it to your system.

Unit replacement

Unit replacement is a tool that you can use to replace a failed hardware device with a compatible one, while ensuring that the data associated to the old unit gets transferred to the new one. For an access control unit, the configuration of the old unit is copied to the new unit. For a video unit, the video archive associated to the old unit is now associated to the new unit, but the unit configuration is not copied.

unit synchronization

Unit synchronization is the process of downloading the latest Security Center settings to an access control unit. These settings, such as access rules, cardholders, credentials, unlock schedules, and so on, are required so that the unit can make accurate and autonomous decisions in the absence of the Access Manager.

University Parking Enforcement

University Parking Enforcement is a Genetec Patroller™ software installation that is configured for university parking enforcement: the enforcement of scheduled parking permits or overtime restrictions. The use of maps is mandatory. Hotlist functionality is also included.

unlock schedule

An unlock schedule defines the periods of time when free access is granted through an access point (door side or elevator floor).

unreconciled read

An unreconciled read is an MLPI license plate read that has not been committed to an inventory.

user

A user is an entity that identifies a person who uses Security Center applications and defines the rights and privileges that person has on the system. Users can be created manually or imported from an Active Directory.

user group

A user group is an entity that defines a group of users who share common properties and privileges. By becoming member of a group, a user automatically inherits all the properties of the group. A user can be a member of multiple user groups. User groups can also be nested.

user level

A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera PTZ, viewing the video feed from a camera, or staying logged on when a threat level is set. Level 1 is the highest user level, with the most privileges.

User management

The *User management* task is an administration task that you can use to configure users, user groups, and partitions.

validation key

A validation key is a serial number uniquely identifying a computer that must be provided to obtain the license key.

Vault

The Vault is a tool that displays your saved snapshots and exported G64, G64x, and GEK (encrypted) video files. From the Vault, you can view the video files, encrypt and decrypt files, convert files to ASF, or package files with the Genetec™ Video Player.

vehicle identification number

A vehicle identification number (VIN) is an identification number that a manufacturer assigns to vehicles. This is usually visible from outside the vehicle as a small plate on the dashboard. A VIN can be included as additional information with license plate entries in a hotlist or permit list, to further validate a hit and ensure that it is the correct vehicle.

Video

The *Video* task is an administration task that you can use to configure video management roles, units, analog monitors, and cameras.

video analytics

Video analytics is the software technology that is used to analyze video for specific information about its content. Examples of video analytics include counting the number of people crossing a line, detection of unattended objects, or the direction of people walking or running.

video archive

A video archive is a collection of video, audio, and metadata streams managed by an Archiver or Auxilliary Archiver role. These collections are catalogued in the archive database that includes camera events linked to the recordings.

video decoder

A video decoder is a device that converts a digital video stream into analog signals (NTSC or PAL) for display on an analog monitor. The video decoder is one of the many devices found on a video decoding unit.

video encoder

A video encoder is a device that converts an analog video source to a digital format by using a standard compression algorithm, such as H.264, MPEG-4, MPEG-2, or M-JPEG. The video encoder is one of the many devices found on a video encoding unit.

video file

A video file is a file created by an archiving role (Archiver or Auxiliary Archiver) to store archived video. The file extension is G64 or G64x. You need Security Desk or the Genetec™ Video Player to view video files.

Video file explorer

The *Video file explorer* is an investigation task that you can use to browse through your file system for video files (G64 and G64x), and to play, convert to ASF, and verify the authenticity of these files.

video protection

Video can be protected against deletion. Protection is applied on all video files needed to store the protected video sequence. Because no video file can be partially protected, the actual length of the protected video sequence depends on the granularity of the video files.

video sequence

A video sequence is any recorded video stream of a certain duration.

video stream

A video stream is an entity representing a specific video quality configuration (data format, image resolution, bit rate, frame rate, and so on) on a camera.

video unit

A video unit is a video encoding or decoding device that is capable of communicating over an IP network and that can incorporate one or more video encoders. The high-end encoding models also include their own recording and video analytics capabilities. Cameras (IP or analog), video encoders, and video decoders are all examples of video units. In Security Center, a video unit refers to an entity that represents a video encoding or decoding device.

video watermarking

Video watermarking adds visible text to live, playback, and exported video processed by Security Center. This text includes identifying information that is intended to deter unauthorized users from leaking video recordings.

(Obsolete) Beginning in Security Center 5.9.0.0, video watermarking no longer refers to the use of digital signatures for tampering protection. Tampering protection is now called *digital signature*.

virtual alarm

We call *virtual alarm*, an alarm on an intrusion detection area that is activated through a virtual input.

virtual input

A virtual input is an input on an intrusion detection unit that is physically connected to an output so that Security Center can trigger it through the *Trigger output* action.

virtual zone

A virtual zone is a zone entity where the I/O linking is done by software. The input and output devices can belong to different units of different types. A virtual zone is controlled by the Zone Manager and only works when all the units are online. It can be armed and disarmed from Security Desk.

Visit details

The *Visit details* task is an investigation task that reports on the stay (check-in and check-out time) of current and past visitors.

Visitor activities

The *Visitor activities* task is an investigation task that reports on visitor activities (access denied, first person in, last person out, antipassback violation, and so on).

visitor escort rule

The visitor escort rule is the additional access restriction placed on a secured area that requires visitors to be escorted by a cardholder during their stay. Visitors who have a host are not granted access through access points until both they and their assigned host (cardholder) present their credentials within a certain delay.

Visitor management

The *Visitor management* task is the operation task that you can use to check in, check out, and modify visitors, as well as manage their credentials, including temporary replacement cards.

visual reporting

Visual reporting is dynamic charts or graphs in Security Desk that deliver insights that you act on. You can perform searches and investigate situations using these visual and user-friendly reports. The visual report data can be analyzed to help identify activity patterns and enhance your understanding.

visual tracking

Visual tracking is a Security Center feature that lets you follow an individual in live or playback mode through areas of your facility that are monitored by cameras.

VSIP port

The VSIP port is the name given to the discovery port of Verint units. A given Archiver can be configured to listen to multiple VSIP ports.

Watchdog

Genetec™ Watchdog is a Security Center service installed alongside the Genetec™ Server service on every server computer. Genetec™ Watchdog monitors the Genetec™ Server service, and restarts it if abnormal conditions are detected.

Wearable Camera Manager

The Wearable Camera Manager role is used to configure and manage body-worn camera (BWC) devices in Security Center, including configuring camera stations, adding officers (wearable camera users), uploading content to an Archiver, and setting the retention period for uploaded evidence.

web-based authentication

Web-based authentication (also known as passive authentication) is when the client application redirects the user to a web form managed by a trusted identity provider. The identity provider can request any number of credentials (passwords, security tokens, biometric verifications, and so on) to create a multi-layer defense against unauthorized access. This is also known as multi-factor authentication.

Web-based SDK

The Web-based SDK role exposes the Security Center SDK methods and objects as web services to support cross-platform development.

Web Client

Security Center Web Client is the web application that gives users remote access to Security Center so that they can monitor videos, investigate events related to various system entities, search for and investigate alarms, and manage cardholders, visitors, and credentials. Users can log on to Web Client from any computer that has a supported web browser installed.

Web Map Service

Web Map Service (WMS) is a standard protocol for serving georeferenced map images over the Internet that are generated by a map server using data from a GIS database.

Web Server

The Web Server role is used to configure the Genetec™ Web App and the Web Client, two web applications that give users remote access to Security Center. Each role created defines a unique web address (URL) that users enter in their web browser to log on to the Genetec™ Web App or Web Client and access information from Security Center.

wheel imaging

Wheel imaging is a virtual tire-chalking technology that takes images of the wheels of vehicles to prove whether they have moved between two license plate reads.

whitelist

A whitelist is a hotlist that is created to grant a group of license plates access to a parking lot. A whitelist can be compared to an access rule where the secured area is the parking lot. Instead of listing the cardholders, the whitelist applies to license plate credentials.

widget

A widget is a component of the graphical user interface (GUI) with which the user interacts.

Windows Communication Foundation

Windows Communication Foundation (WCF) is a communication architecture used to enable applications, in one machine or for multiple machines connected by a network, to communicate. Genetec Patroller™ uses WCF to communicate wirelessly with Security Center.

workstation

A workstation entity represents a Security Desk workstation in the system that grants additional access rights and privileges to selected users when they log on to the system through it.

X.509 certificate

X.509 certificate and *digital certificate* are synonyms. In Security Center, these two terms are used interchangeably.

zone

A zone is an entity that monitors a set of inputs and triggers events based on their combined states. These events can be used to control output relays.

Zone activities

The *Zone activities* task is an investigation task that reports on zone related activities (zone armed, zone disarmed, lock released, lock secured, and so on).

Zone Manager

The Zone Manager role manages virtual zones and triggers events or output relays based on the inputs configured for each zone. It also logs the zone events in a database for zone activity reports.

Zone occupancy

The *Zone occupancy* task is an investigation task that reports on the number of vehicles parked in a selected parking area, and the percentage of occupancy.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ TechDoc Hub:** The latest documentation is available on the TechDoc Hub. To access the TechDoc Hub, log on to Genetec Portal and click TechDoc Hub. Can't find what you're looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explains how the product works and provide instructions on how to use the product features. To access the help, click **Help**, press F1, or tap the **?** (question mark) in the different client applications.

Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to TechDoc Hub, where you can find information and search for answers to your product questions.

- **Genetec TechDoc Hub:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

  Before contacting GTAC or opening a support case, it is recommended to search TechDoc Hub for potential fixes, workarounds, or known issues.

  To access the TechDoc Hub, log on to Genetec Portal and click TechDoc Hub. Can't find what you're looking for? Contact documentation@genetec.com.
- **Genetec Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec Lifecycle Management (GLM) documents: Genetec Assurance Description and Genetec Advantage Description.

Technical training

In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to http://www.genetec.com/support/training/training-calendar.

Licensing

- For license activations or resets, please contact GTAC at https://portal.genetec.com/support.
- For issues with license content or part numbers, or concerns about an order, please contact Genetec Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, please contact Genetec Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Please contact GTAC at https://portal.genetec.com/support to address any issue regarding Genetec appliances or any hardware purchased through Genetec Inc.