Security Center User Guide 5.10

Document last updated: October 7, 2021

Genetec™

Legal notices

Document information

Document title: Security Center User Guide 5.10

Original document number: EN.500.004-V5.10.2.0(1)

Document number: EN.500.004-V5.10.2.0(1)

Document update date: October 7, 2021

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

About this guide

This guide describes Security Desk features and commands, and provides instruction on how to perform tasks, such as live monitoring of events, video playback and instant replay, report generation, LPR route playback, alarm management, and visitor management.

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

Chapter 4: Tasks

Chapter 5: Reports

Chapter 6: Basic tasks

Chapter 7: Advanced tasks

Chapter 13: Video archives

Chapter 14: Video export

Chapter 15: Video options

Part III: Introduction to access control in Security Desk

Chapter 16: Access control at a glance

Chapter 17: Cardholders and visitors

Chapter 18: Credentials

Chapter 19: Areas, doors, and elevators

Chapter 24: AutoVu™ Free-Flow

Chapter 25: Genetec Patroller™

Chapter 26: Mobile License Plate Inventory

Part V: Alarms and critical events in Security Desk

Chapter 27: Alarms

Chapter 28: Incidents and threat levels

Chapter 29: Zones and intrusion detection

Part VI: Overview of troubleshooting topics in Security Desk

Chapter 30: General troubleshooting

Chapter 31: Troubleshooting video

Chapter 32: Troubleshooting access control

Security Desk reference

Part I

Introduction to Security Desk

This part includes the following chapters:

1

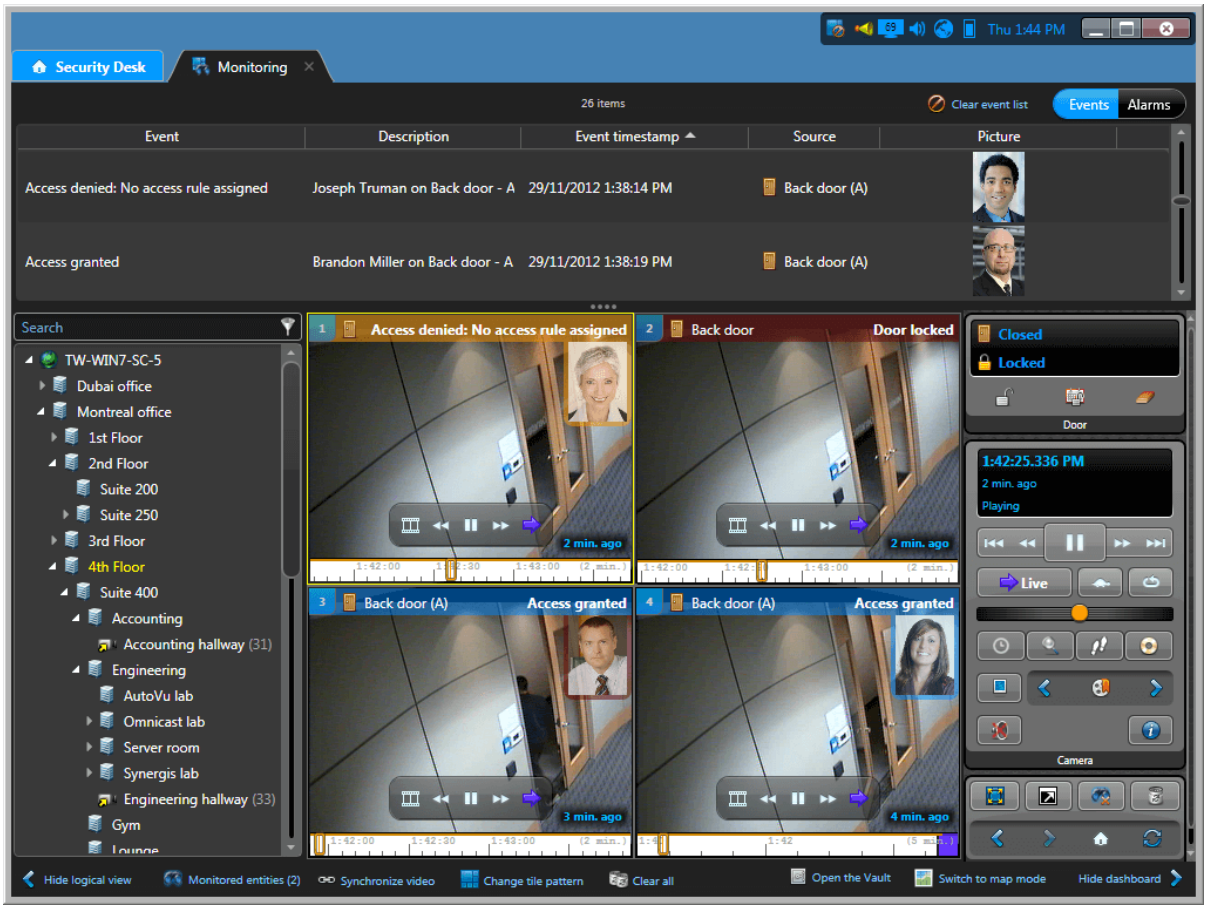
Security Desk at a glance

This section includes the following topics:

About 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.

In a single interface, you can monitor real-time events and alarms, generate reports, track door and cardholder activity, and view live and recorded video. When connected to a *Federation* of multiple systems, Security Desk allows you to monitor, report on, and manage hundreds of sites.



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 home page 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.

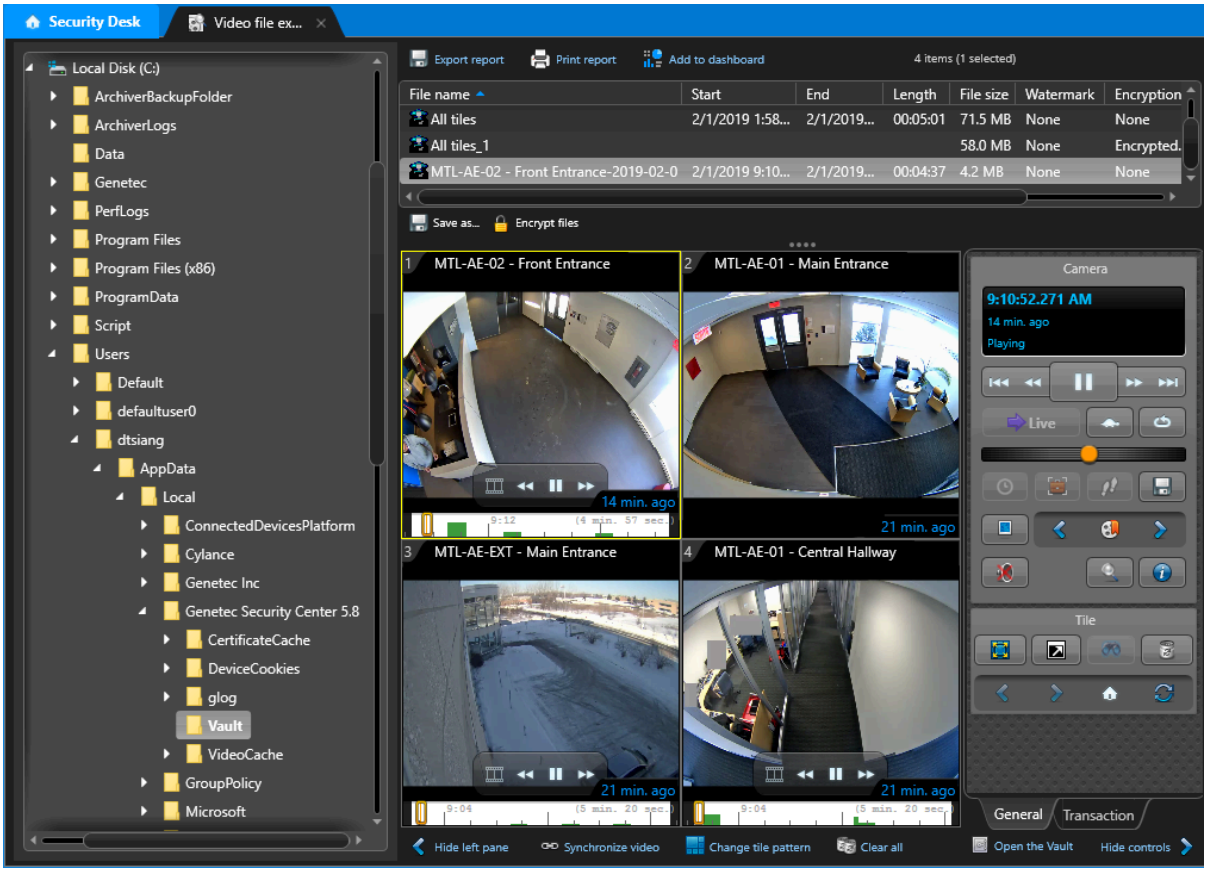
Under each major category, the tasks are further divided as follows:

- **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.

About Security Desk offline mode

You can use Security Desk offline mode to search for and view videos with the *Video file explorer* task instead of the Genetec™ Video Player.

When offline mode is activated, Security Desk launches without needing to log on. The *Video file explorer* task opens automatically upon startup and it is the only task available in this mode. Use the **Selector** list to browse for your desired files.



Activating Security Desk offline mode

You can activate Security Desk offline mode using a command line argument or the Security Desk configuration file.

What you should know

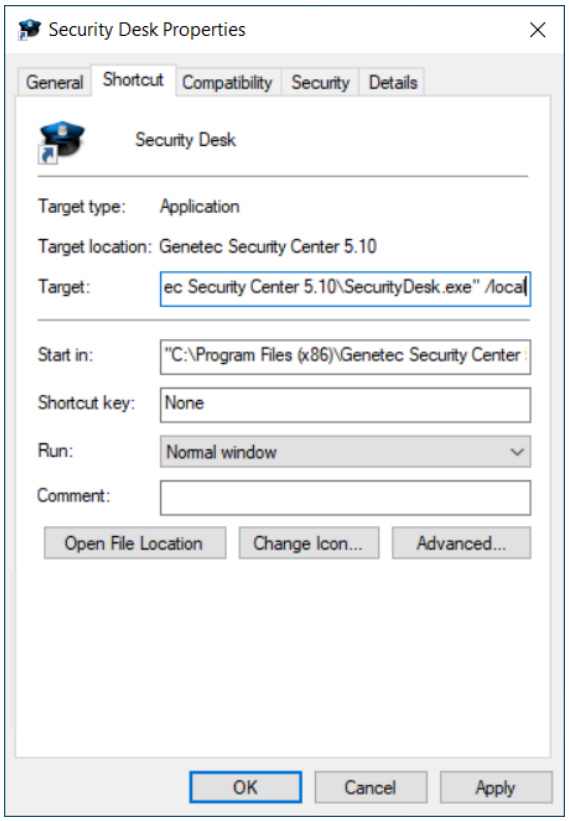
You can use Security Desk offline mode to search for and view videos with the *Video file explorer* task without being connected to the internet.

To activate Security Desk offline mode using a command line argument:

1 In Windows, right-click the Config Tool or Security Desk shortcut, and click **Properties**.

2 Click the **Shortcut** tab.

3 At the end of the **Target** field, add the command line argument /local.
Example: "C:\Program Files (x86)\Genetec Security Center 5.x\SecurityDesk.exe" **/local**



4 Click **Apply** > **OK**.

To activate Security Desk offline mode using the configuration file:

1 In Windows File Explorer, navigate to *C:\Program Files (x86)\Genetec Security Center 5.10\ConfigurationFiles*.
2 Open the *App.SecurityDesk.Config* file with a text editor.
3 Edit the Workspace line in the <configuration> section as follows:
Example: <Workspace FastLayoutSwitching="False" **Local="True"**/>
4 Save your changes and open Security Desk in offline mode.

Logging on to Security Center through Security Desk

To log on to Security Center, you must open the Security Desk application and connect to the Security Center Directory.

Before you begin

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

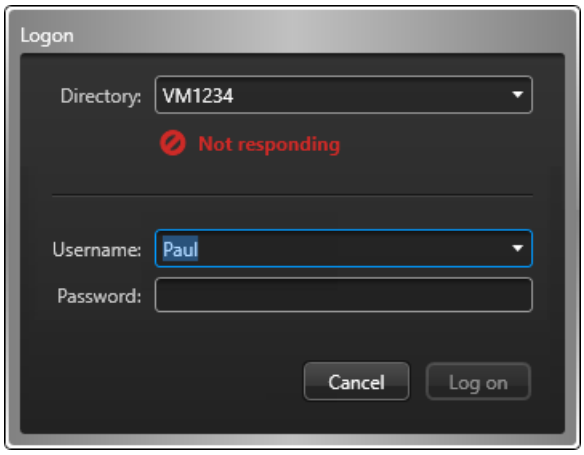
What you should know

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

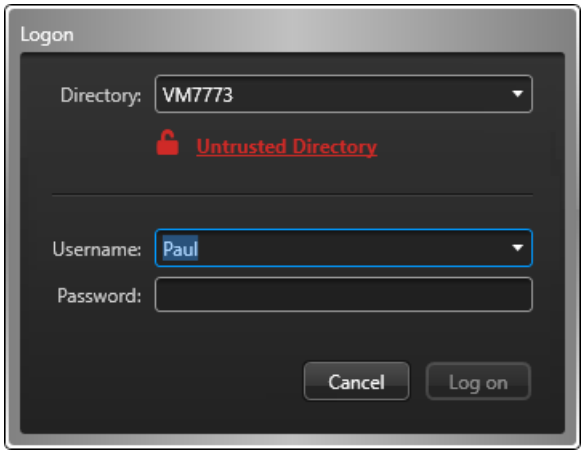
To log on to Security Center:

1 Open Security Desk.
   a) Up to Windows 8, click **Start** > **All programs** > **Genetec Security Center 5.10** > **Security Desk**
   b) In Windows 10, click **Start** > **Genetec Security Center 5.10** > **Security Desk**

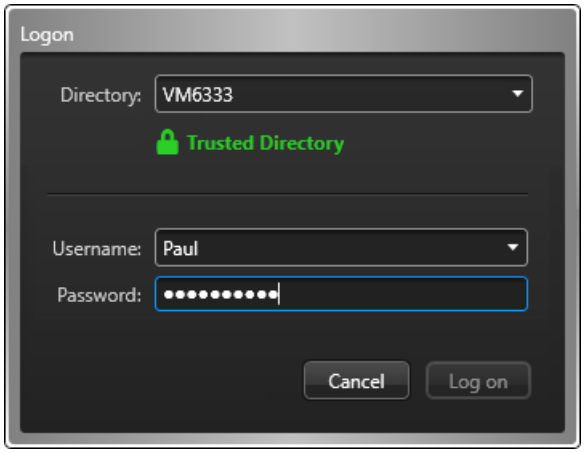
2 In the *Logon* dialog box, enter the name of the **Directory**.
If the Directory is not responding, check the spelling or contact your administrator.



If the Directory is not trusted, it could be the sign of a man-in-the-middle attack. Do not proceed unless your administrator confirms that it is safe to do so.



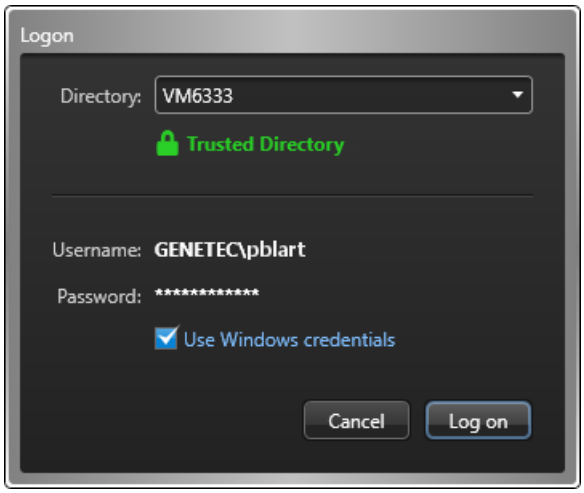
3 Enter your Security Center username and password.



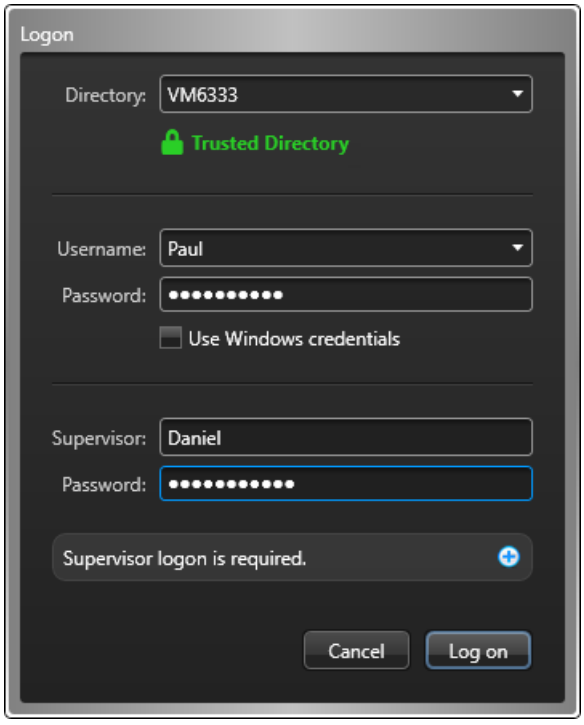
If single sign-on is deployed, you must click the **Sign in** button for your *identity provider*, or append your domain name to the end of your username, such as `Username@DomainName`. You will then be redirected

to your identity provider for authentication. Skip to Logging on using web-based authentication on page 10.

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.



5 Click **Log on**.
6 If you are required to log on with supervision, your supervisor must provide a username and password.



7 Click **Log on**.
Security Desk opens.

NOTE: After a period of inactivity you might be locked out of Security Desk. You will have to re-enter your credentials to use the application again.

8 To log off, click the home ( ) tab, and then click **Log off**.
By default, you are asked to save your workspace when you log off Security Desk. You can change this behavior in the User Interaction section of the *Options* dialog box.

Example

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

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 Security Desk and enter the name of the **Directory** in the *Logon* dialog box.

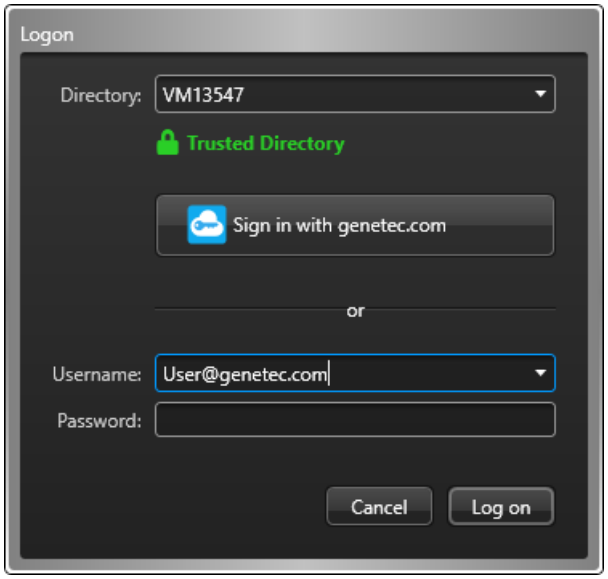
What you should know

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: Security Desk remembers all valid logon parameters used and automatically calls up the parameters used for the last logon attempt.

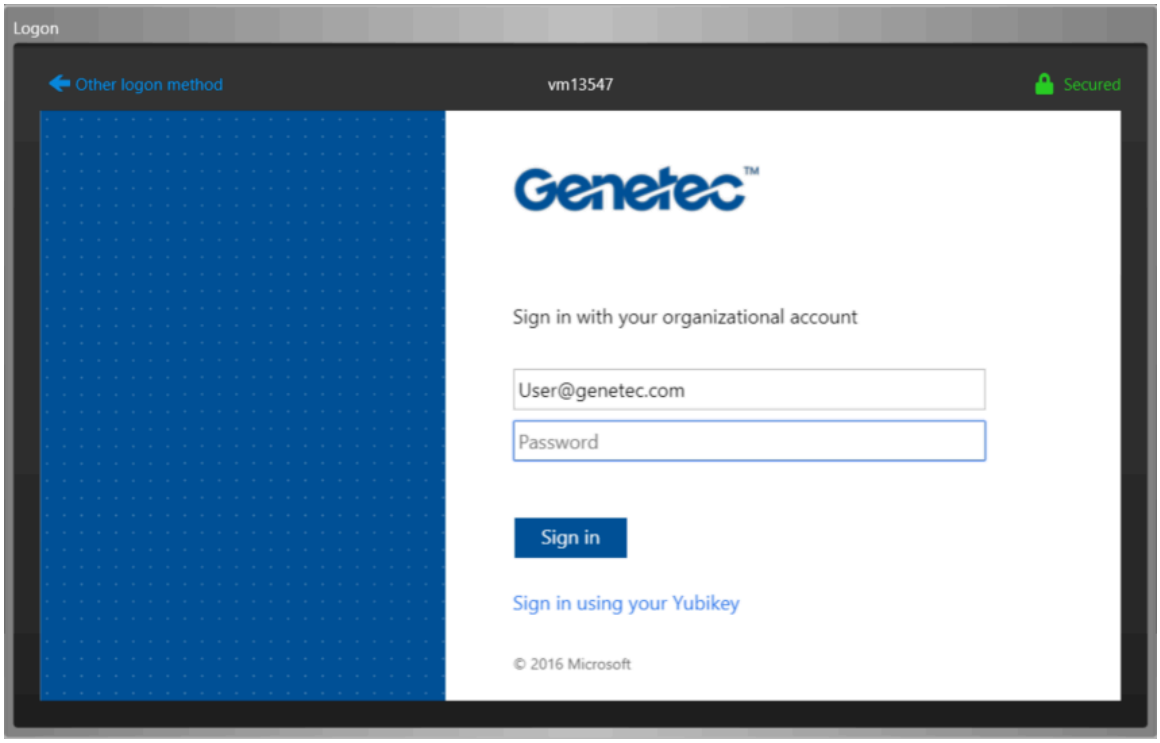
To log on using web-based authentication:

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.



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**.

Closing Security Desk

You can close Security Desk and save your workspace for the next time you log on.

What you should know

By default, you are asked to save your workspace when you close Security Desk. You can change this behavior in the User Interaction section of the *Options* dialog box.

To close Security Desk:

1. In the upper-right corner of the Security Desk window, click the exit button ().
   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 Security Desk, click **Save**.

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

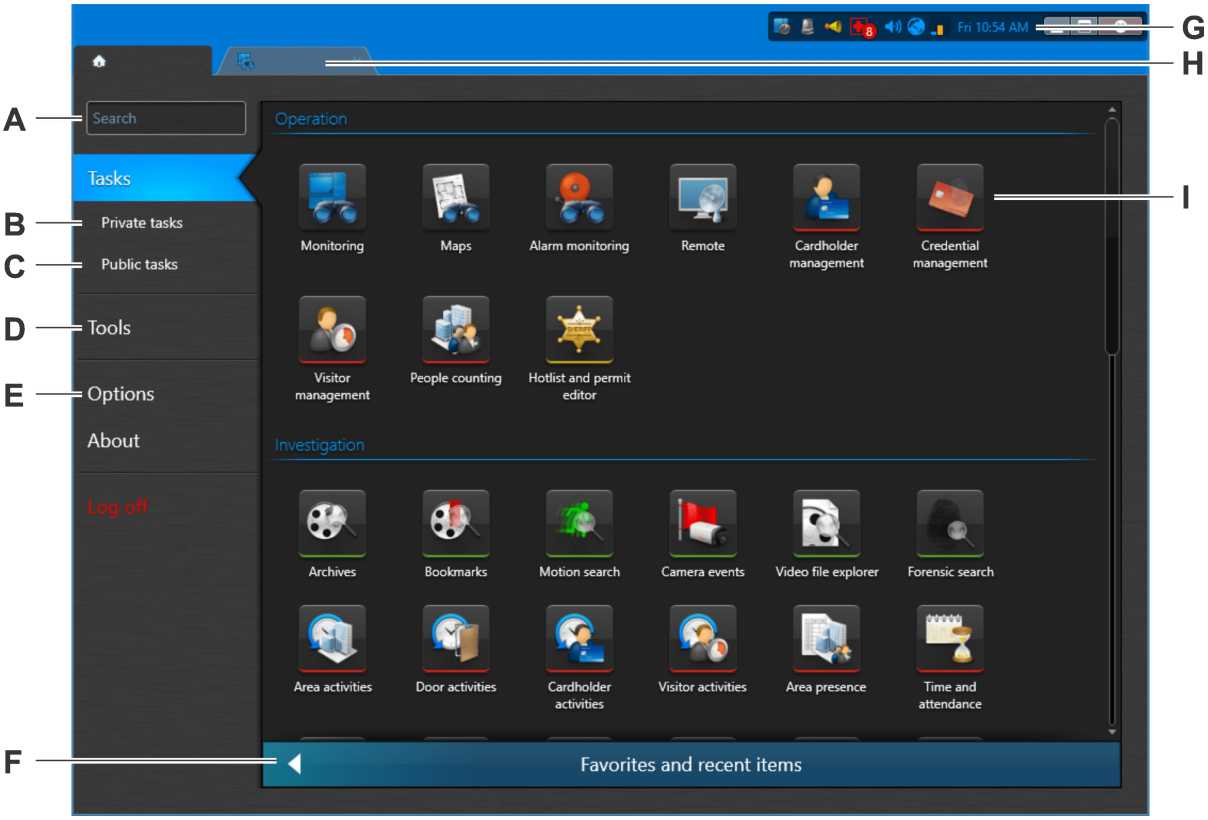
This setting is saved with your user profile and applies to both Security Desk and Config Tool.

To save your workspace automatically when closing the client:

1. From the home page, 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**.

Home page overview

The home page is the main page in Security Center. Open the home page by clicking the home tab ( ).



A	**Search box**	Type the name of the task 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 home page.
E	**Options**	Click to configure the options for your application.
F	**Favorites** and **Recent items**	Lists the tasks and tools 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 you have 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

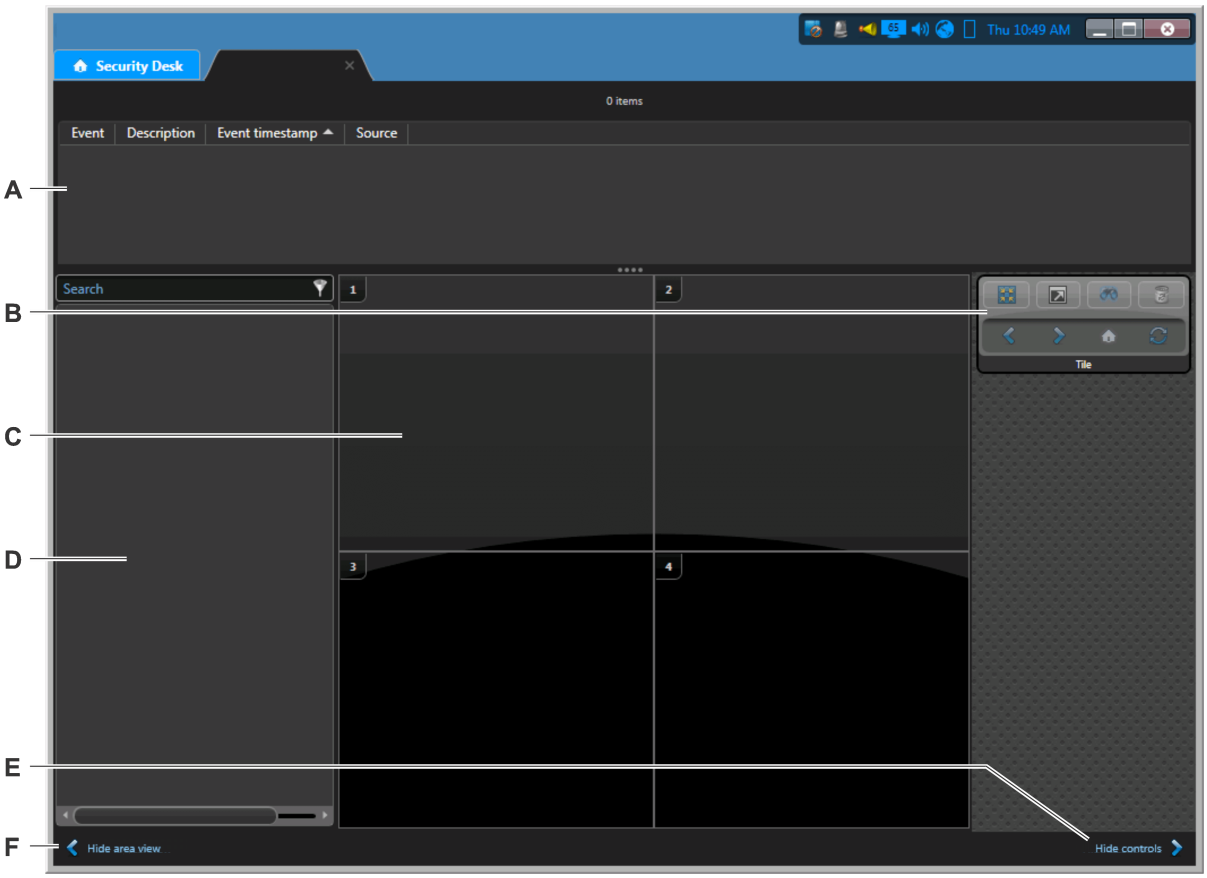
Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

Related Topics

Configuring the notification tray on page 94
Saving tasks on page 54
Opening tasks on page 53
Shortcuts to external tools on page 133

UI component overview

Security Desk has a standard user interface in the *Monitoring* task and most reporting tasks, which has four main parts: the *Area view*, *Report pane*, *Canvas*, and *Controls*.



A	**Report pane**	Displays information in the form of a table listing events, active alarms, or query results, depending on the task you are using. The information can appear as text or graphics (cardholder picture, timeline, thumbnails, and so on).
B	**Controls**	Contains widget commands related to the entity type displayed in the selected tile in the canvas.
C	**Canvas**	Allows you to view and control entities in *tile mode* or *map mode*.
D	**Area view**	Lists all the entities that are part of your system, which you can drag into the canvas.
E	**Hide controls**	Click to hide or show the controls.
F	**Hide area view**	Click to hide or show the area view.

Watch this video to learn more.

Related Topics

Monitoring ALPR events in map mode on page 389

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, Security Desk shows the current use vs. the maximum allowed.

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.

Related Topics

Changing passwords on page 20
Sending feedback on page 21

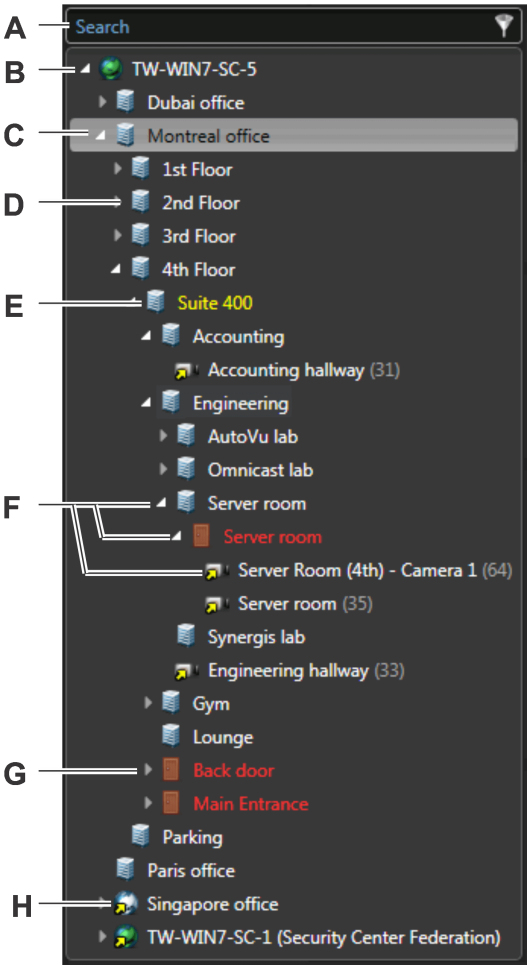
About the area view

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	**Configure entity**	Right-click an entity in the area view, and then click **Configure entity** ( ) to jump to that entity's configuration page in Config Tool. You need the user privilege to modify entity properties to use this command.

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.

Related Topics

Viewing entities in the canvas on page 27
Searching for entities on page 90
Entity states on page 513

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 home page, 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**.

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 home page, 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**.

2

Canvas

This section includes the following topics:

About tiles

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.

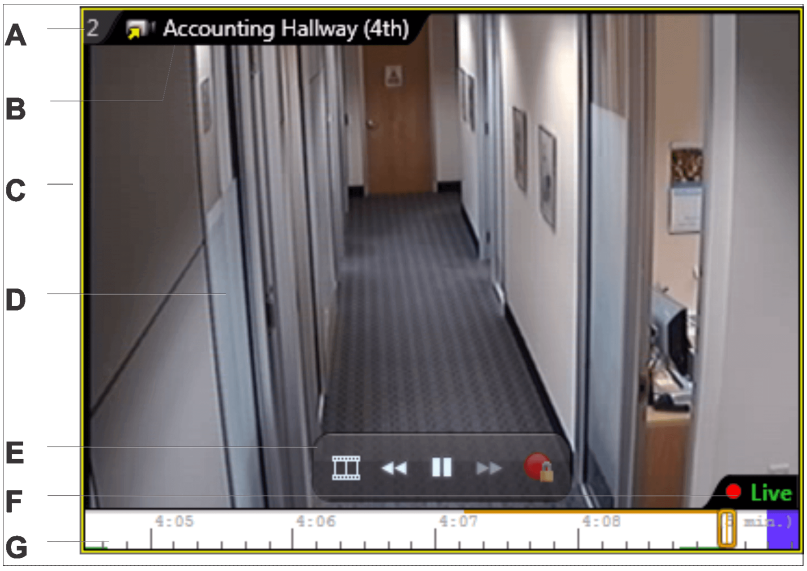
Tiles can display the following:

- Entities
- Event information
- Live and playback video
- Video images
- Cardholder and visitor pictures and information
- ALPR reads
- Web pages
- Tile plugins
- maps

Content is automatically displayed in tiles when events occur related to the entities you are monitoring. You can also display entities by dragging them to a tile. Security Desk tiles have a *tile-memory*, meaning that Security Desk remembers the last 8 entities displayed in each tile. Using the commands in tile widget, you can switch to the previous, next, and initial tile content.

You can right-click inside the tile to view tile menu commands.

The following figure shows a tile displaying a camera.



A	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. If the tile ID is blue, it means event monitoring is enabled for the tile. If it is black, monitoring is disabled. If it is red with a narrow band of blue, event and alarm monitoring are enabled for the tile.
B	Tile toolbar	Displays the entity name. When an event occurs, information corresponding to the event is also shown in the tile toolbar.

C	Yellow frame	Indicates that the tile is selected.
D	Video stream	The streaming video is displayed inside the tile. Double-click to expand the tile to the whole canvas.
E	On-tile video controls	Use the on-tile video controls while viewing video in a tile.
F	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)*. Green indicates that it is not recording. Red indicates that it is recording.
G	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. Use the timeline to control playback video.

Related Topics

Customizing how tiles are displayed on page 33

Tile menu commands

You can control your tiles and the entities displayed in tiles using commands in the tile menu.

Some commands always appear, and other contextual commands change depending on the entity type displayed in the tile. The following table lists the commands available from the tile menu:

Command		Description
Camera		Commands related to video surveillance. The other camera commands are listed in the camera widget.
	Auxiliary recording	If the camera is controlled by an Auxiliary Archiver, manually start recording on the Auxiliary Archiver by clicking the record button (⚫) next to the Auxiliary Archiver role name.
	Protect video from deletion	Prevent the current video recording from being deleted due to the Archiver role's disk space constraints. This command is only available when video content is displayed in the tile.
	Remove privacy protection	Displays the confidential (Private) video stream that contains the original video from the video unit and the video content is not blurred or masked.
	Reinstate privacy protection	Displays the public video stream that contains privacy-protected blurred content with video anonymization applied. This ensures that all regular access to video will always access the blurred video.
	Block	Prevent users from viewing the selected video stream. This command is only available when video content is displayed in the tile.
	Unblock	Allow users to view the selected video stream. This command is only available when video content is displayed in the tile.
	Select live stream	Select the camera's video stream to be displayed in the current tile. By default, the Live stream is displayed. This commands is only available when live video is displayed in the tile and the video unit supports multiple streams.
	Select video playback source	Select which archiving source (Archiver, Auxiliary Archivers, Cloud storage) to view the playback video from. For example, if you want to view a specific resolution, frame rate, or video stream, you can select the Archiver that is configured to record with those settings. By default, All sources is displayed. This command is only available when playback video is displayed in the tile.
	Commands	Select additional camera-specific commands, such as play audio clip, turn on white light, auto focus, and so on. These contextual camera command are currently supported on some Axis, Panasonic, and Bosch cameras.

Command		Description
Monitoring	**Monitor alarms**	Select to turn alarm monitoring on and off for the tile. A blue check mark indicates that alarm monitoring is turned on.
	Monitor events	Select to turn event monitoring on and off for the tile. A blue check mark indicates that event monitoring is turned on.
Investigate		Click to open an *Investigation* task based on the selected entity. That entity will already be selected in the report query filters.
Report an incident		Create an incident report for something you see happening in the tile.
Start incident recording		Start recording the video related to every entity that is placed in the tile (cameras, areas, doors, cardholders, and so on), to create a incident report package.
Maximize tile		Expand the current tile to fill the canvas. Hides all other tiles.
Maximize tile fullscreen		Hide the area view and controls, and make the current tile fill the canvas. Forces the tile to be displayed in full screen mode.
Navigate	**Back**	Show previous tile content.
	Forward	Show next tile content.
	Home	Show initial tile content.
	Refresh	Refresh tile content.
Add to dashboard		For Security Center entities only. Adds the entity to a dashboard as a **Tile** widget.
Clear all		Empty all content from tiles.

Viewing entities in the canvas

You can view an entity in a canvas tile from the area view or the report pane.

What you should know

All entities listed in the area view and some entities and events in the report pane can be viewed in a canvas tile, with the exception of the System entity ( ). Entities can also appear automatically in a tile when an event occurs.

If it is helpful for you, you can show more information next to the entities in the area view by customizing how entities are displayed.

To view an entity in the canvas:

1 From the area view or the report pane, do one of the following:
- To view a single entity, double-click or drag the entity into a tile.
- To view multiple entities, hold Ctrl or Shift, select the entities, and drag them to a tile. This method only works if there enough free tiles.

2 To control the entities, right-click inside the tile and use the tile menu commands, or use the widgets in the *Controls* pane.

3 To clear entities from the canvas, do one of the following:
- Right-click on a tile, and then click **Clear** ( ).
- Select a tile, and then press the Backspace key.
- (Empties all tiles) At the bottom of the canvas, click **Clear all** ( ).
- (Empties all tiles) Press Ctrl+Backspace.

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

Entity states on page 513

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 home page, 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**.

Unpacking content in tiles

When an entity is displayed in a tile that has other entities associated with it, you can unpack the entity and view all the attached entities in separate tiles.

What you should know

Entities that have two or more entities attached to them are called *composite entities* (for example, a door that has multiple cameras associated to it). If you are monitoring the door and an event occurs at the door, only the first camera is displayed because the multiple cameras are *packed*. If you unpack the door, you can view all the cameras in separate tiles.

Limitation: Limited to a maximum of 16 unpacked elements.

To unpack content in a tile:

1 Select a tile that is displaying a composite entity.

2 Beside the entity name in the tile toolbar, click .

3 From the drop-down menu, click one of the following:

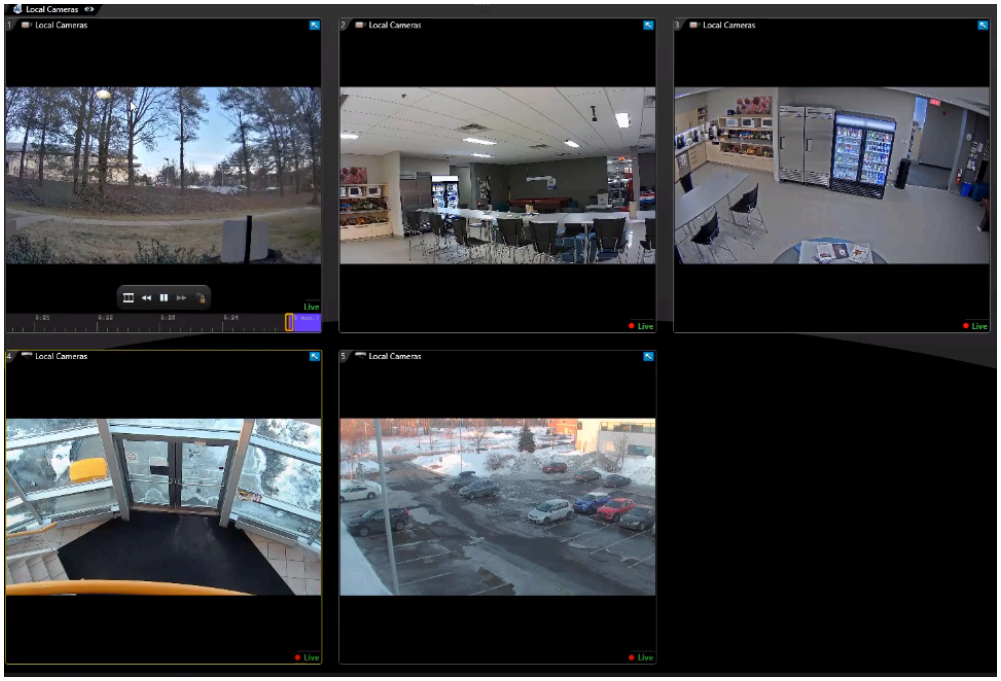
- An attached camera (in the example, *Main Entrance* or *Front Hallway*).
- **Unpack:** View all entities attached to the selected entity in separate tiles.
- **Start cycling:** Rotate through the entities that are attached to the composite entity within the tile. The amount of time each entity is displayed can be configured from the *Options* dialog box.

  NOTE: If there is a PTZ camera attached to the composite entity and you start controlling the PTZ, the cycling stops. You can click **Start cycling** again once you are done controlling the PTZ.

4 To repack the tiles when you have finished viewing what you need to see, click **Pack** ( ) in the upper-left corner of the tile.

Example

The *Main Entrance* door has two cameras associated to it: the *Main Entrance* camera and the *Front Hallway* camera. An *Access denied* event occurs at the main door, and the event is displayed in a tile. Because the tile is packed, only the first camera is displayed (Main Entrance), until you unpack the tile content.



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

Customizing entity cycling options

You can select how many seconds Security Desk dwells on each entity when rotating through composite entities (such as an alarm, area, or a camera sequence) in a tile.

What you should know

This setting is saved as part of your user profile.

To customize entity cycling options:

1. From the home page, click **Options** > **General**.
2. In the *Dwell time* section, set the **Entity cycling** value.
3. Click **Save**.

Maximizing the canvas to full screen

When Security Desk is in full screen mode, you can hide the area view, taskbar, and controls so only the canvas and the video streams you are monitoring are shown, or you can maximize one tile to focus on a particular video image.

What you should know

The full screen video mode looks similar to an analog monitor. If Security Desk is connected to multiple monitors and you switch the canvas to full screen mode, each monitor displays a separate canvas. You can select which monitors switch to full screen mode from the *Options* dialog box.

To maximize the canvas to full screen mode:

1 Do one of the following:

- To maximize the canvas, press **F11** > **F10**.

  Everything is hidden except for the canvas tiles.
- To maximize one tile, press **Alt+ENTER**.

2 Use your keyboard shortcuts to control the video streams.

3 To show the taskbar, hover your mouse at the top of the Security Desk window.

4 To exit full screen mode, do one of the following:

- If your canvas is maximized, press **F11** > **F10**.
- If one tile is maximized, press **Alt+ENTER**.

Related Topics

Default keyboard shortcuts on page 174

Selecting which monitors can switch to full screen

If Security Desk is connected to multiple monitors, you can choose which monitors are able to switch to full screen mode, from the *Options* dialog box.

What you should know

These settings apply to the local Security Desk workstation, and affect Security Desk and Config Tool for all users.

To select which monitors can switch to full screen:

1 On your default monitor, select the home page and click **Options** > **General**.

2 In the *Full screen monitors* section, select which monitors can switch to full screen.

This section is only displayed when Security Desk is connected to more than one monitor.

3 Click **Save**.

Changing tile patterns

You can change the tile pattern of the canvas.

What you should know

The default tile pattern in the canvas displays four viewing tiles in a 2x2 formation.

To change the tile pattern:

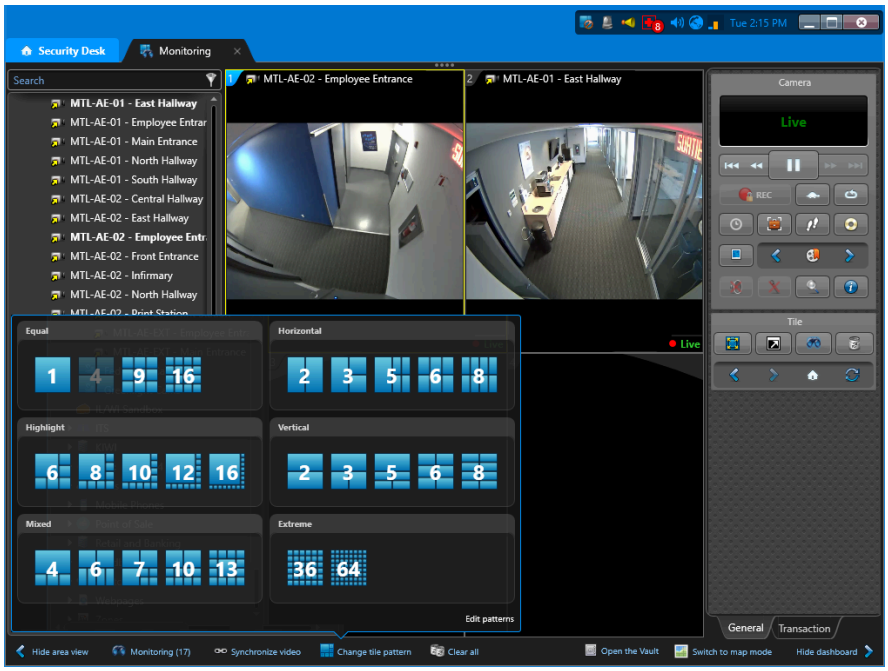
1 At the bottom of the canvas, click **Change tile pattern** ( ).

2 Do one of the following:

- Select one of the displayed tile patterns.

  These patterns are either the default ones, or patterns that you have set as favorites.
- Click **More**, and select one of the additional tile patterns.

  They range between 1 large tile to 64 small tiles.



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

Editing and creating tile patterns on page 32

Editing and creating tile patterns

To customize your workspace, you can modify the 26 tile patterns that are available in the canvas, delete default patterns, and create new tile patterns.

What you should know

The tile pattern editor in Security Desk only allows you to create patterns that are a maximum of 8x8 files.

Tile pattern settings are saved as part of the workstation. You require the *Edit tile patterns* user privilege to edit and create tile patterns.

To edit or create a tile pattern:

1. At the bottom of the canvas, click **Change tile pattern** ( ).
2. Click **More** > **Edit patterns**.
3. Do one of the following:
   - Select an existing pattern.
   - To create a new tile pattern, click .
4. In the **Name** field, type a name for the pattern.
5. In the **Category** field, select which group to place the pattern in.
6. To display the pattern in the main dialog box when you click **Change tile pattern** ( ), select **Display as favorite** ( ).
7. To change the number of rows and columns, use the **Rows** and **Columns** selector, or click the lines in the graph.
8. To delete a pattern, select the pattern, and click .
9. To revert all the tile patterns to their default configuration, click **Revert to default**.

   IMPORTANT: All patterns that are not default patterns are deleted.

10. Click **Save and close**.

Example

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

Customizing how tiles are displayed

You can customize what to show in the canvas tiles from the *Options* dialog box.

What you should know

The parts of a tile that can be hidden are the timeline, on-tile video controls, tile toolbar, and *tile ID*. The tile settings are saved as part of your user profile.

To customize how tiles are displayed:

1 From the home page, click **Options** > **Visual**.

2 From the **Display timeline** drop-down list, select when to show the timeline in tiles, in live, and in playback:

- **Auto-hide:** Only show the timeline when the mouse cursor hovers inside the tile boundaries.
- **Always:** Always show the timeline.
- **Never:** Never show the timeline.

3 To show the on-tile video controls when you hover your mouse cursor inside a tile (play, pause, and so on), select the **Display overlay video controls** option.

4 To show an entity's full path with the entity name in the tile toolbar, select the **Display entity names with their full path** option.

An entity's path is the hierarchy of *areas* above that entity in the area view. When the path is too long, an "*" is displayed instead.

Example: "Montreal office/Main entrance", or "*/*/Back entrance".

NOTE: This option also applies to alarms. When this option is selected, the full path of the entity that triggered the alarm is displayed in the **Source** column in the Monitoring task and Alarm monitoring task.

5 To show the tile toolbar only when you hover your mouse cursor over a tile, select the **Auto-hide tile toolbar** option.

When this option is cleared, the tile toolbar is always displayed.

6 To show the tile ID number only when you hover your mouse cursor over the tile, select the **Auto-hide tile number** option.

When this option is cleared, the tile ID is always displayed.

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.

Related Topics

On-tile video controls on page 189
About tiles on page 23

3

Widgets

This section includes the following topics:

Alarm widget

The *Alarm* widget appears whenever an alarm entity is displayed in the current tile. It offers you different ways to respond to an alarm.

If a triggered alarm requires an acknowledgment condition (for example, *Door closed*), the *Investigate* button appears in the alarm widget when that alarm entity is displayed in the current tile and the acknowledgment condition is not yet cleared.

The commands in the alarm widget are available in the *Monitoring*, *Alarm monitoring*, and *Alarm report* tasks.

The alarm widget commands are described below:

Button	Command	Description
	Acknowledge (Default)[1]	Acknowledge the alarm. The alarm is no longer active, and is removed from the canvas and the alarm list.
	Acknowledge (Alternate)[1]	Set the alarm to the *alternate* acknowledged state. The reasons for using this acknowledgment type are defined by your company. For example, if a false alarm is triggered, you can acknowledge the alarm this way. This state can be used as a filter in alarm queries.
	Forcibly acknowledge[1]	Force the alarm to be acknowledged. This is helpful for clearing alarms that are currently under investigation and their acknowledgment condition is not yet cleared.
	Investigate	Investigate the alarm. This action lets other users in the system know that you have seen the alarm without acknowledging it, so the alarm is not removed from the active alarm list.
	Snooze alarm[1]	Put the alarm to sleep for 30 seconds. When the alarm is snoozing, it is temporarily removed from the canvas. You can change the default snooze time from the *Options* dialog box.
	Forward alarm[1]	Forward the alarm to another user in the system. Before forwarding the alarm, you must select a user, and you can also type a message.
	Show alarm procedure	Show the alarm's specific procedure (if one is defined by the administrator). Alarm procedures are simple to create and can take the form of HTML pages or a web application developed by the end user.

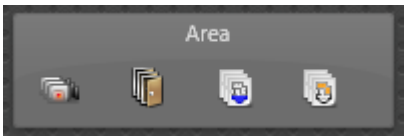
[1] If you hold Ctrl+Shift when clicking the command, that command applies to all alarms displayed in the canvas.

Related Topics

Forwarding alarms to other users automatically on page 472
Customizing alarm behavior on page 478
Overview of the Alarm report task on page 608

Area widget

The *Area* widget opens when the current tile is showing an area.



The commands included in the area widget are *recursive*, meaning that they apply to all the entities that are members of the selected area. Click on one of the commands to view a menu of commands you can pick from.

The area widget commands are described below:

Button	Command	Description
	Cameras	Apply commands to all cameras that are members of the area: • **Start recording :** Start recording on the cameras. • **Stop recording:** Stop recording on the cameras. • **Add bookmark:** Add a bookmark to the cameras. • **Block:** Prevent users from viewing the video streams. • **Unblock (recursive):** Allow users to view the video streams.
	Doors	Apply commands to all doors that are members of the area: • **Override unlock schedules :** Lockdown the doors that might be on an unlock schedule. • **Cancel override:** Put the doors back on their unlock schedules. • **Unlock area perimeter doors:** Unlock the perimeter doors of the area for the *Standard grant time* configured for those doors.

Button	Command	Description
	**Zones**	Apply commands to all zones that are members of the area: • **Arm:** Arm the zones. • **Disarm:** Disarm the zones.

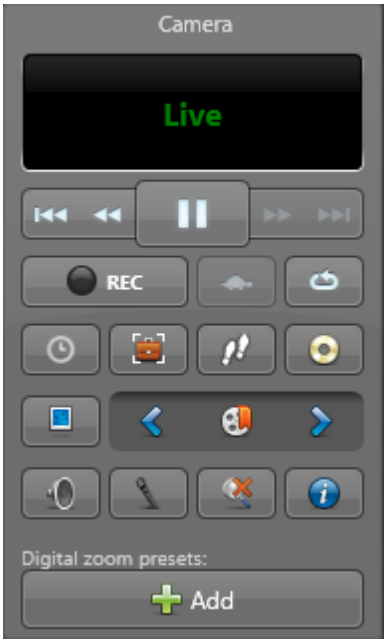
	**Intrusion detection areas**	Apply commands to all intrusion detection areas that are members of the area:
		NOTE: Some commands might be unavailable if you lack a necessary privilege, or if the command is not supported by your intrusion panel.
		• **Arm:** Arm the selected intrusion detection areas. The following options are available:
		  • **Master:** Arm all sensors in the intrusion detection areas. Any sensor can trigger the alarm when activated.
		  • **Perimeter:** Arm only the sensors designated to be on the perimeter. Activity on sensors inside the areas, such as motion detectors, is ignored.
		  • **Instant:** Arm the areas immediately.
		  • **Delay:** Arm the areas after a delay. If you do not specify a duration, the panel default is used.
		  • **Arming mode:**
		  • **Normal:** Arm the intrusion detection areas normally. Areas with active or troubled sensors remain disarmed.
		  • **Force:** If one or more intrusion detection areas are not ready for normal arming, this option forcefully arms the areas. 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 one or more intrusion detection areas are not ready for normal arming, this option automatically bypasses active or troubled sensors before arming the areas. Sensors remain bypassed while the areas are armed. Disarming an area removes the bypass from sensors in that area.
		• **Disarm:** Disarm the selected intrusion detection areas. Sensor activity in the areas is ignored by the intrusion panel.
		• **Trigger intrusion alarm:** Triggers an intrusion alarm in the selected intrusion detection areas.
		• **Silence alarm:** If there is an active alarm in a 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** can also acknowledge the alarm.
		• **Acknowledge alarm:** Acknowledge the active alarm in a selected intrusion detection area.

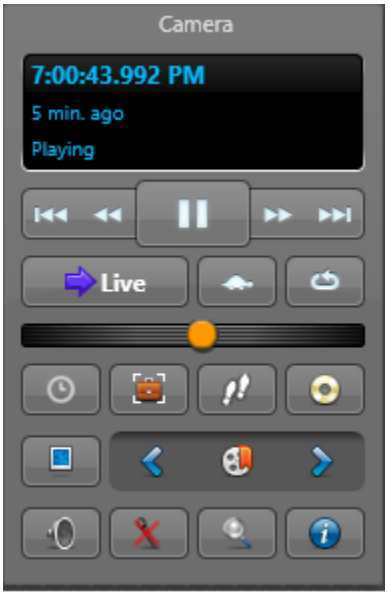
Camera widget

The *Camera* widget appears in the *Controls* pane when the currently selected tile is displaying a camera.

The buttons displayed in the camera widget change depending on the task you are performing, and the camera type. For example, if the camera displayed in the tile is streaming live video, you find one set of buttons. If the camera displayed in the tile is playing back a recording, some of the buttons change. If the camera supports audio, the audio buttons appear, otherwise, they are grayed out.

The following two images show the camera widget when live video with no audio is selected in a tile, and when playback video with audio is selected in a tile.





The camera widget commands are described below:

Button	Command	Description
	Jump backward[1]	Jump backward. Each click of this button forces the recording playback to jump backwards by 15 seconds. You can configure this value from the *Options* dialog box.
	Rewind[1]	Reverse the playback. Each click of this button adjusts the reverse playback speed from - 1x to -2x, -4x, -6x, -8x, -10x, -20x, -40x, -100x. Click the Play button to revert playback to 1x (normal speed) in the forward direction.
	Previous frame[1]	Reverse the video by one frame. You can also use the jog wheel to achieve the same result. This button is only available when the video is paused.
	Pause[1]	Pause the playback at the current frame.
	Play[1]	Play back the recording at normal speed (1x).
	Next frame[1]	Advance the video by one frame. You can also use the jog wheel to achieve the same result. This button is only available when the video is paused.

Button	Command	Description
	**Forward**[1]	Fast forward the playback. Each click of this button increases the playback speed from 1x to 2x, 4x, 6x, 8x, 10x, 20x, 40x, 100x. Click the Play button to revert playback to normal speed (1x).
	**Jump forward**[1]	Jump forward. Each click of this button forces the recording playback to jump forward by 15 seconds. You can configure this value from the *Options* dialog box.
	**Switch to live**[1]	Switch the displayed images from playback to live video.
	**Recording on**	(Solid red) The camera is currently recording. Click to stop recording.
	**Recording on**	(Blinking red) The camera is currently recording, but almost at the end of it's manual recording duration (30 seconds remaining). Click to reset timer for another five minutes.
	**Recording on (locked by system)**	The camera is currently recording, and is controlled by a system configuration. You cannot click to stop recording.
	**Recording off**	The camera is not currently recording. Click to start recording. The recording stops automatically after five minutes. You can also stop the recording manually. If the camera is also controlled by an Auxiliary Archiver, you can manually start recording on the Auxiliary Archiver by right-clicking the recording state button, selecting **Auxiliary recording**, and then clicking the record button () next to the Auxiliary Archiver role name.
	**Recording off (locked by system)**	The camera is not currently recording, and is controlled by a system configuration. You cannot click to start recording.
	**Recording problem**	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. If you see this error, contact your system Administrator to resolve the issue.
	**Slow motion**[1]	Switch between normal playback speed (1x) and slow motion (1/8x). While in slow motion mode, click the Forward or Rewind button to change the playback speed from 1/8x to 1/4x, 1/3x, 1/2x, in either direction.
	**Loop playback**	Create a looped playback. When you click this button, two timeline markers () appear at either end of the timeline. Click and drag the markers over the timeline to indicate the start and end points of the looped playback.
	**Speed slider**	Drag the slider to the right to accelerate playback to 2x, 4x, 6x, 8x, 10x, 20x, 40x, 100x. Drag the slider to the left to force reverse playback at -2x, -4x, -6x, -8x, -10x, -20x, -40x, -100x speeds.
	**Speed slider (limited)**	Same as the speed slider above except that reverse playback is limited to: -10x, -20x, -40x, -100x. The limited speed slider is used on federated Omnicast™ 4.x cameras that do not support all rewind speeds.

Button	Command	Description
	**Jog wheel**	Replaces the speed slider when the video is paused. Use it for frame by frame playback both forwards and backwards.
	**Go to specific time**[1]	Open a browser window, and jump to a precise date and time in the recording.
	**Quick search**	Opens the *Quick search* dialog box.
	**Enable visual tracking**[1]	Follow an individual or object that is moving across different cameras from the same tile.
	**Export video**[1]	Create stand-alone video files that can be played without being connected to the Security Center Directory.
	**Save a snapshot**[1]	Save the current video frame as an image file.
	**Previous bookmark**[1]	Jump to the previous bookmark.
	**Add a bookmark**[1]	Add a bookmark to the video.
	**Next bookmark**[1]	Jump to the next bookmark.
	**Listen**[1]	Enable the speaker. This button is only available when the camera supports audio.
	**Stop listening**[1]	Disable the speaker. This button is only available when the camera supports audio.
	**Talk**[1]	Enable the microphone. This button is only available when the camera supports audio.
	**Stop talking**	Disable the microphone. This button is only available when the camera supports audio.
	**Toggle digital zoom**	Apply a 2x digital zoom to the image. Further digital zoom adjustments can then be performed within the tile.
	**Show stream properties**	Display the properties of the selected video stream.
	**Digital zoom presets**	When digital zoom is applied to the selected tile, click this button to add a digital zoom preset for the current camera image position.

[1] If you hold Ctrl+Shift when clicking the command, the command applies to all cameras displayed in the canvas.

Example

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

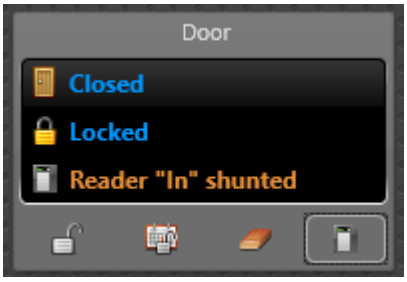
Related Topics

Video options on page 280

Switching between video modes on page 223
Performing targeted video searches on page 231
Zooming in and out of video on page 199
Adding bookmarks to video sequences on page 204
Taking snapshots of video on page 206
Exporting video in G64x format on page 250
Exporting video in G64, ASF, and MP4 formats on page 255
Monitoring parking zones on page 428

Door widget

The *Door* widget appears whenever a door entity is displayed in the current tile. It allows you to control the access through that door. The *Door* widget also displays the current door state (closed or opened), the lock state (locked, unlocked, unlocked and in maintenance mode, or unsecured), and the reader state (if it is shunted).



The door widget commands are described below:

Button	Command	Description
	Unlock[1]	Temporarily unlock the door for 5 seconds (or whatever the duration of the *Standard grant time* is, as configured by the system administrator).
	Override unlock schedules	Unlock the door indefinitely for maintenance purposes, or keep the door locked or unlocked for a predetermined period.
	Cancel	Cancel the unlock schedule override.
	Forgive antipassback violation	Forgive an antipassback violation. This button is only available when there is an antipassback violation.
	Reader (Shunt or Activate)	Select the reader to either Shunt (deactivate) or Activate. This button is only available when your access control equipment supports reader shunting.

[1] If you hold Ctrl+Shift when clicking the command, the command applies to all doors displayed in the canvas.

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

Allowing access through doors on page 361
How doors are displayed in the Security Desk canvas on page 360

Elevator widget

The *Elevator* widget appears whenever an elevator entity is displayed in the current tile. You can use the widget to override the elevator schedule and shunt the elevator reader.

The elevator widget commands are described below:

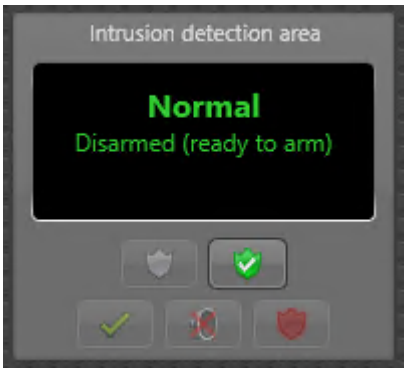
Button	Command	Description
	Override elevator schedules	Unlock the elevator indefinitely for maintenance purposes, or keep the elevator locked or unlocked for a predetermined period. **NOTE:** This button is enabled only if the elevator is controlled by an access control unit running Synergis™ Softwire 10.6 or later.
	Reader (Shunt or Activate)	Select the reader to either Shunt (deactivate) or Activate. This button is only available when your access control equipment supports reader shunting.

Related Topics

Controlling access to elevator floors on page 364

Intrusion detection area widget

When an intrusion detection area is displayed in a tile in Security Desk, you can arm or disarm the area, and interact with intrusion alarms using the *Intrusion detection area* widget.



The *Intrusion detection area* widget is described in the following table:

NOTE: Some commands might be unavailable if you lack a necessary privilege, or the command is not supported by the intrusion panel you are using.

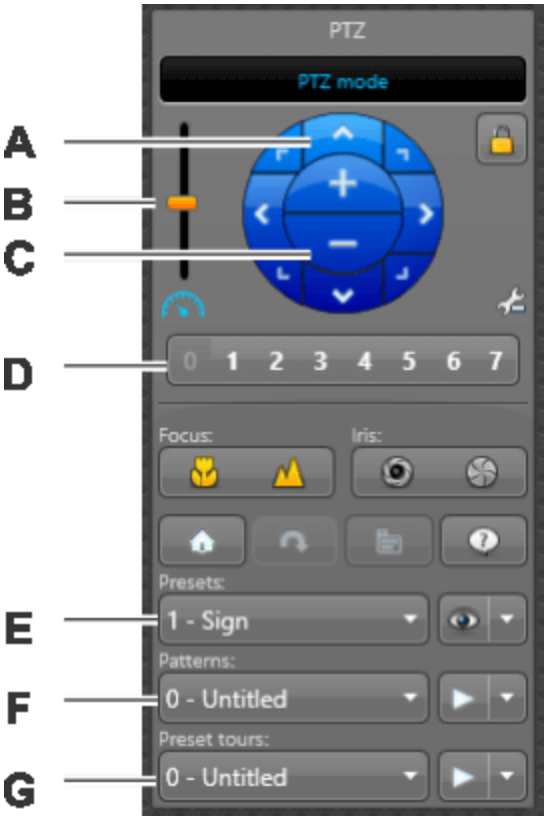
Button	Command	Description
	Disarm	Disarm the area, by causing all sensors attributed to the selected intrusion detection area to be ignored by the intrusion panel.
	Arm	Arms the intrusion detection area. The following options are available: • **Master:** Arms all sensors in the intrusion detection area. 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 specific duration, the panel default is used. • **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.
	Trigger intrusion alarm	Trigger an intrusion alarm on the selected intrusion detection area.

Button	Command	Description
	**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. For example, with Bosch intrusion panels using Mode 2, *Burglary* alarms are acknowledged from Security Desk, but *Fire* alarms must be acknowledged on the panel keypad.
	**Acknowledge alarm**	Acknowledge the intrusion alarm on the selected intrusion detection area.

PTZ widget

The *PTZ* widget is used to perform 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: Not all PTZ cameras support all PTZ commands. If one or more of the PTZ buttons are greyed out, the PTZ camera you are working with does not support that command.

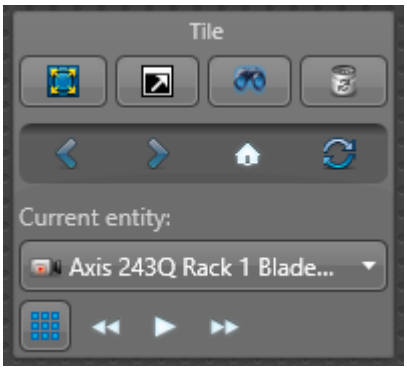


Button/Letter	Command	Description
A	**Direction arrows**	Pan the PTZ motor using the eight direction arrows.
B	**Speed slider**	Adjust the speed of the PTZ motor.
C	**Zoom in/out**	Zoom in and out using the plus (+) and minus (-) commands.
D	**Quick access buttons**	Move the PTZ motor to one of the eight 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 start a PTZ pattern (series of presets or recorded PTZ movements), record a new pattern, or 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.

Button/Letter	Command	Description
	**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).
	**Stop auxiliary command**	Stop the PTZ auxiliary command.
	Rename	Rename the selected preset, pattern, or auxiliary.

Tile widget

The *Tile* widget controls the properties of the current tile. It is always shown in the *Controls* pane.



The tile widget commands are described below. The same commands appear in the tile menu.

Button	Command	Description
	Maximize tile	Expand the current tile to fill the canvas. Hides all other tiles.
	Maximize tile fullscreen	Hide the area view and controls, and make the current tile fill the canvas. Forces the tile to be displayed in full screen mode.
	Monitoring[1]	Start alarm or event monitoring in a tile.
	Clear all[1]	Empty all content from tiles.
	Back	Show previous tile content.
	Forward	Show next tile content.
	Home	Show initial tile content.
	Refresh	Refresh tile content.
n/a	**Current entity**	Select which entity to view from the selected composite entity. For example, select a camera attached to the selected area.
	Unpack	View all entities attached to the selected entity in separate tiles.
	Pack	Pack all the attached entities.
	Go to previous content in cycle[1]	Switch to the previous entity attached to the composite entity.
	Start cycling[1]	Rotate through the entities that are attached to the composite entity within the tile. The amount of time each entity is displayed can be configured from the *Options* dialog box.
	Stop cycling[1]	Stop the entity cycling rotation.
	Go to next content in cycle[1]	Switch to the next entity attached to the composite entity.

[1] If you hold Ctrl+Shift when clicking the command, that command applies to all tiles displayed in the canvas.

Related Topics

Selecting entities to monitor on page 85
Unpacking content in tiles on page 28
Monitoring parking zones on page 428

Zone widget

The *Zone* widget only appears when the current tile is showing a zone.

The zone widget commands are described below:

Button	Command	Description
	Disarm[1]	Disarm the selected zone (inputs deactivated).
	Arm[1]	Arm the selected zone (inputs activated).

[1] If you hold Ctrl+Shift when clicking the command, the command applies to all zones displayed in the canvas.

4

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 home page, do one of the following:

- Enter the task name in the *Search* box.
- Click the **Tasks** tab, and then click **Browse all tasks**
- To open a saved task, click the **Private tasks** or **Public** tab.

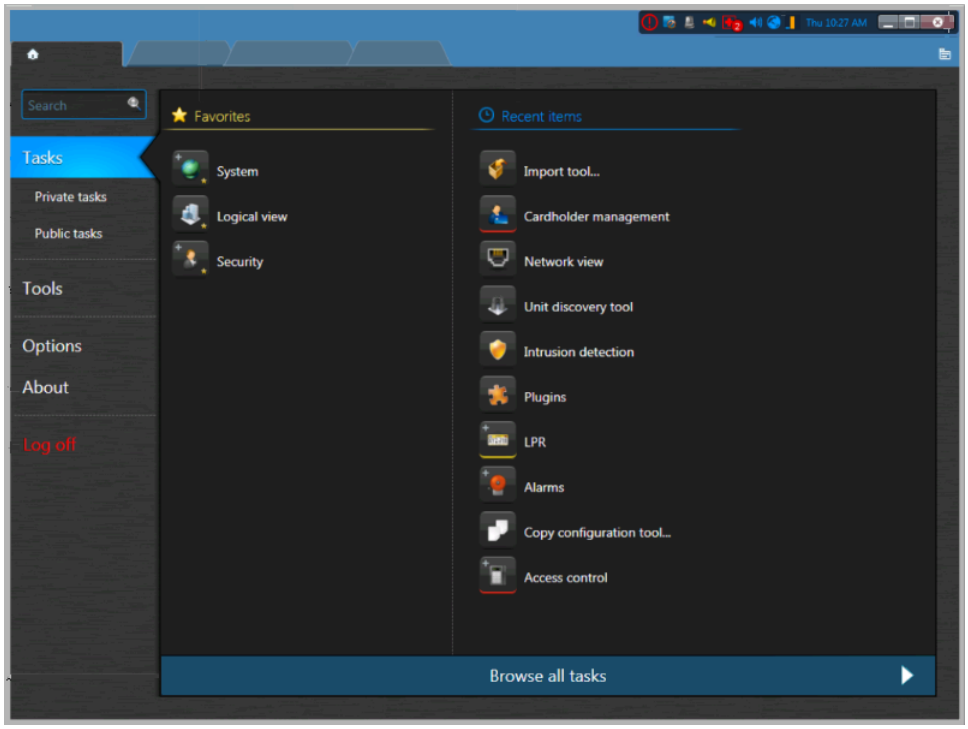
2 Click the task.

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.



Example

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

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:

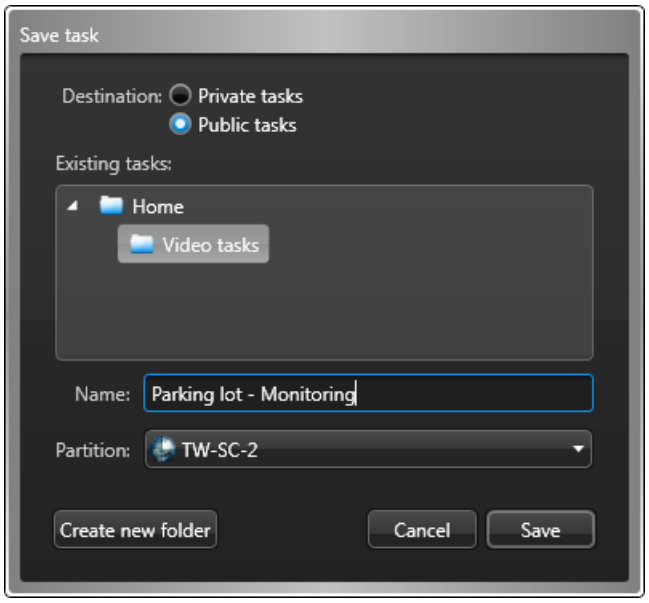
- **Private tasks:** A private task is a saved task that is only visible to the user who created it.
- **Public tasks:** A public task is a saved task that can be shared and reused among multiple Security Center users.

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*.



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**.

Saving layouts

You can save your *Monitoring* task layouts in an areas view that everyone can access.

What you should know

When you save a *Monitoring* task as a layout, the tile pattern, and the entities displayed in each tile (tile content) are saved. The monitoring state (event and alarm monitoring) of the tiles, and the video mode of the cameras (live or playback) are not saved with the layout.

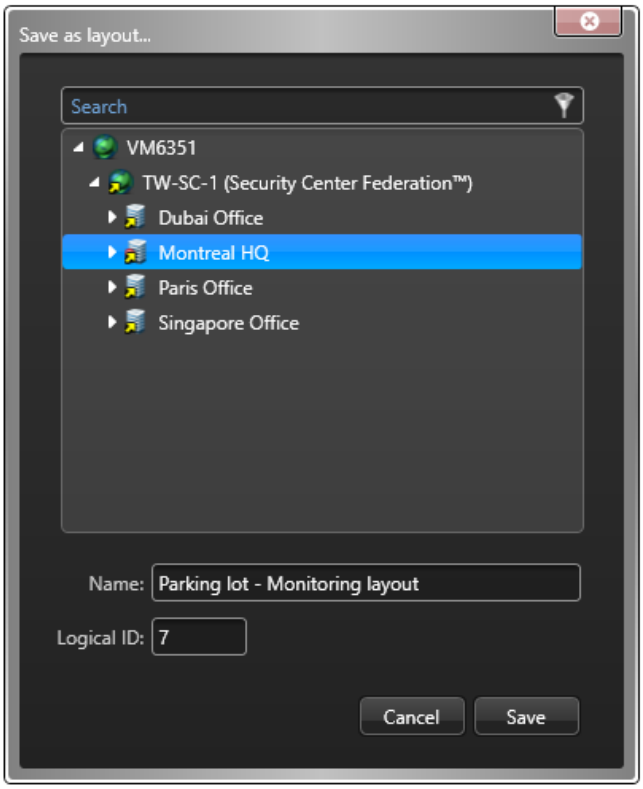
NOTE: The **Save as layout** menu item is only available in a *Monitoring* task.

The benefits of saving a *Monitoring* task layout are as follows:

- You can quickly change the monitored entities (cameras, doors, and so on) without leaving the *Monitoring* task.
- You can share layouts with other users who have access to the area view where the layout was saved.

To save a *Monitoring* task as a layout:

1 In the *Monitoring* task, right-click the task tab and click **Save as layout**.



NOTE: Only users with the required access rights to the area can view or modify this layout.

2 In the *Save as layout* dialog box, use the drop-down menu to select the area where you want to save the layout.

3 Enter a **Name** for the layout.

Example: If you are currently monitoring your parking lot cameras, you can save your *Monitoring* task as a layout with the name *Parking lot - Monitoring layout*.

4 (Optional) Enter a Logical ID.

5 Click **Save**.

After you finish

- Drag or double-click your saved layout from the area view to the *Monitoring* task to quickly change the monitored video feeds without leaving the *Monitoring* task.

  IMPORTANT: If you are monitoring an alarm, it will not be overwritten by the layout. The entity brought in by the layout only becomes visible after you acknowledge the alarm.
- To edit the layout, right-click the task tab, and click **Save as layout**, use the drop-down menu to select the layout then change the **Name** or **Logical ID** and click **Save**.
- To change the layout name, description, and logical ID, right-click the entity in the area view, and click **Configure entity** () to open the configuration page for that layout in Config Tool.
- To modify the tile pattern and entities associated with each tile, right-click the entity in the area view, and click **Overwrite with current layout** command.

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 home page

You can turn off the display of the **Remove from Favorites** and *Recent items* lists in your home page 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 home page, 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 home page, 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 home page.

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.

Sending tasks using a manual action

To immediately share a task layout with someone else or display a task on a video wall, you can send the task to another user or a Security Desk monitor using a one-time hot action.

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.

Only saved *public tasks* can be sent using a hot action.

To send a task using a manual action:

1. In the notification tray, click **Hot actions** ().
2. In the *Hot actions* dialog box, click **Manual action**.
3. In the *Configure an action* dialog box, select **Send task** from the list of actions.
4. From the **Task** drop-down list, select the saved public task that you want to send.
5. Select whether to send the task to a **User** or a Security Desk **Monitor**.
6. In the **Select destination** list, select the user or the monitor to send the task to.

   TIP: When selecting a monitor as a destination, you might see red and white entries in your monitor list. Monitors that appear red are currently disconnected. Monitors that appear white are currently connected.

7. (Optional) If you are sending the task to a user, write a message in the **Message** field.
8. Click **OK**.

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.

Closing tasks using a manual action

You can remove tasks from another workstation using a manual action.

What you should know

You cannot remove individual tasks from a remote workstation. The **Clear tasks** command removes all open tasks.

You can only close tasks for users who are currently online.

To close a task using a system action:

1 In the notification tray, click **Hot actions** ( ).
2 In the *Hot actions* dialog box, click **Manual action**.
3 From the list of actions, click **Clear tasks**.
4 From the drop-down list, select the saved public task that you want to remove.
5 Select whether to remove the task from a user (**User**) or a workstation (**Monitor**).
6 From the **Select destination** list, select the user or the monitor from which you want the tasks to be removed.
7 Click **OK**.

All open tasks are immediately removed from the remote monitor. A confirmation message is produced on the sender's workstation.

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. However, the **Task cycling** and **Ask for confirmation when opening tasks sent by other users** options are saved as local setting for your Windows user profile.

To customize task behavior:

1. From the home page, click **Options** > **General**.
2. To set the amount of time Security Desk dwells on each task when cycling through the open tasks, set the **Task cycling** value.

   NOTE: *Task cycling* can be turned on by right-clicking anywhere in the taskbar.

3. Click the **User interaction** tab.
4. 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.
5. 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.
6. Click **Save**.

5

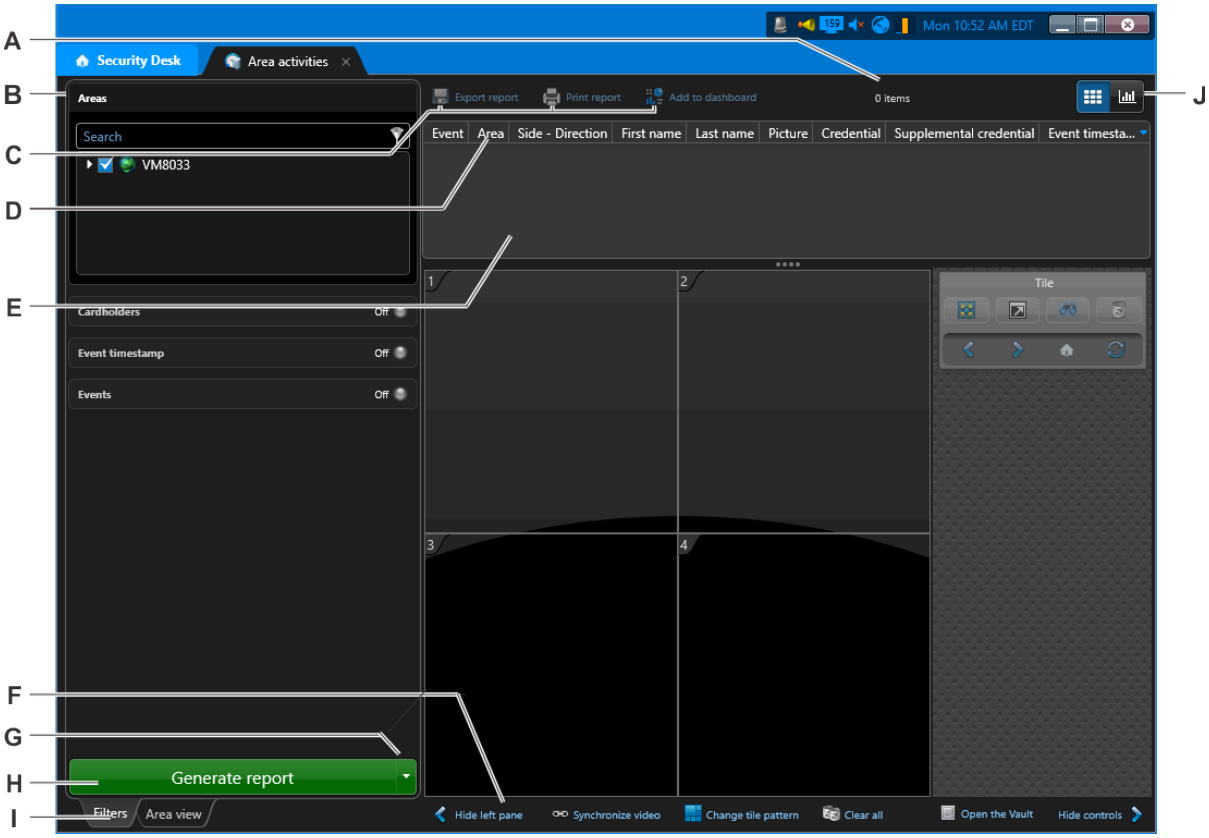
Reports

This section includes the following topics:

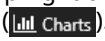
Reporting task workspace overview

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.

This section takes you on a tour of the reporting task layout, and describes the common elements of most reporting tasks. The *Area activities* task was used as an example. You can open the Area activities task by typing its name in the *Search* box on the home page.



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 *Filters* tab to set up your query. Click on 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, or add to dashboard	Click to export your generated report, print it, or add the report to a dashboard.
D	Select columns	Right-click a column heading to select which columns to display in the report pane.
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 (such as launching another report related that report result).

F	Tile commands	Commands related to canvas tiles: • **Synchronize video:** Synchronize the video displayed in the canvas. • **Clear all:** Empty all content from tiles. • **Change tile pattern:** Change the tile pattern in the canvas.
G	Generate and save report	Click to run and save the report directly to a file (PDF, CSV, or Excel format). This button is disabled if you have not selected any query filters, or when you have invalid filters.
H	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, the button changes to *Cancel*. Click on *Cancel* to interrupt the query.
I	Filters tab	Use the Filters tab to customize and filter your searches. The Filters tab is only shown in reporting tasks. **NOTE:** Click the Area view tab to show the area view, and select entities to view in the canvas.
J	Tiles or Charts	If the report supports tiles, open the chart view using the toggle button () at the top right of the task. Otherwise, open the chart view using the Charts button (). • If the report supports tiles: Click the Tiles button () to show the Tiles view below the report pane. • If the report supports charts: Click the Charts button () to show the Charts view below the report pane.

About visual reports

Security Desk's 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

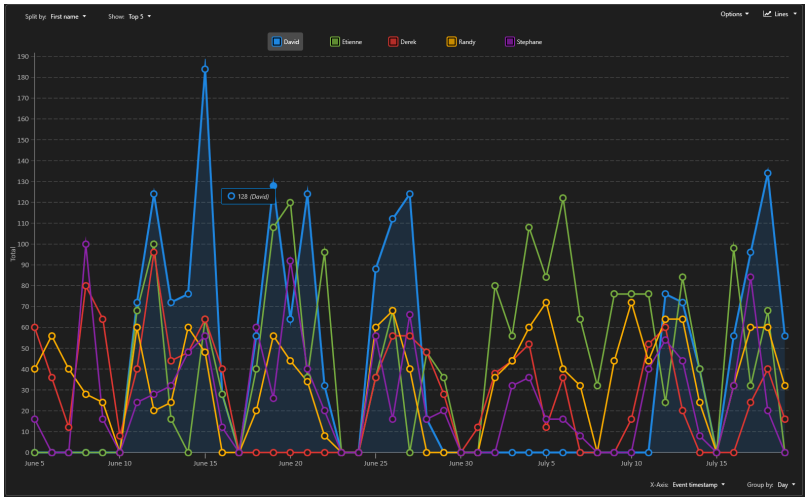
The following chart types are supported in Security Center when using the **Generate report** functions in Security Desk: **Lines**, **Columns**, **Stacked columns**, **Rows**, **Stacked rows**, **Doughnut**, and **Pie**.

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.

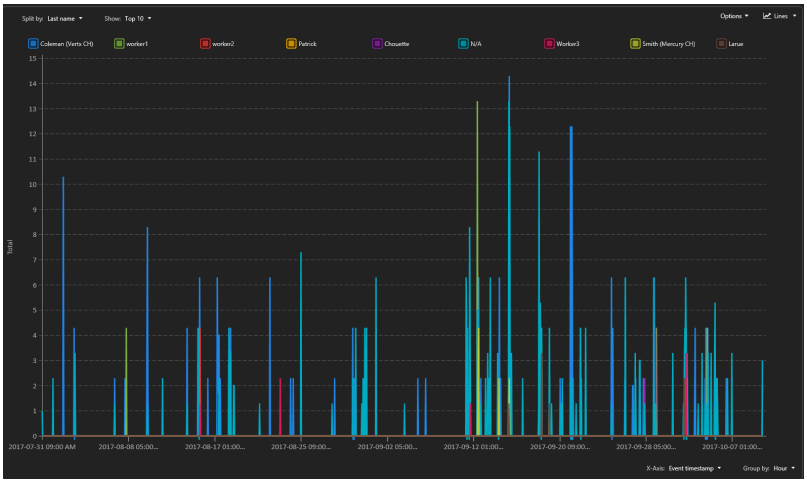
The following example shows a Cardholder events report, Split by: **First name**, Show: **Top 5** and X-Axis: **Event timestamp**, Group by: **Day** as a **Lines** chart.



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.

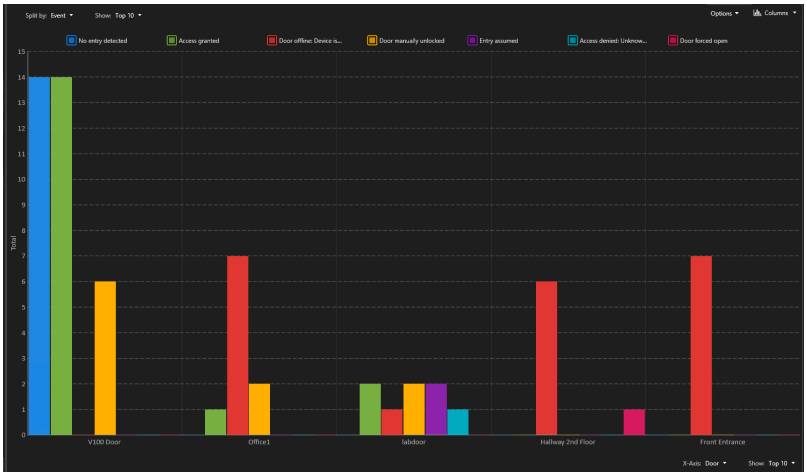


NOTE: The simplified version of a lines chart does not support interaction with the mouse or indication of Y value for a specific point.

Columns chart

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

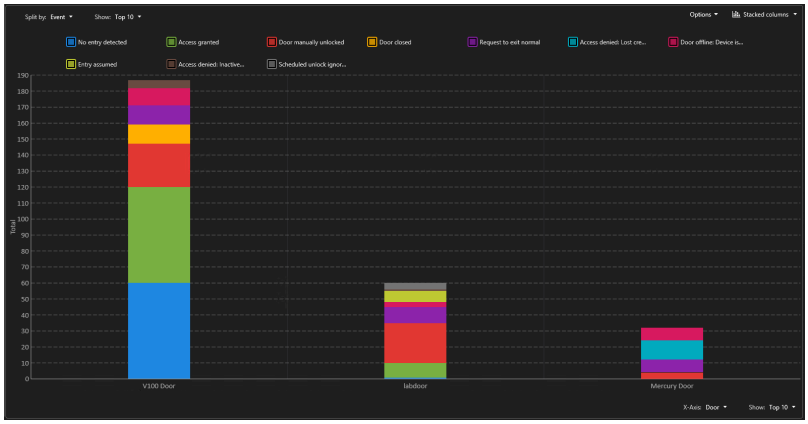
The following example shows a Door access report, Split by: **Event**, Show: **Top 10** and X-Axis: **Door**, Show: **Top 10** as a **Columns** chart.



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.

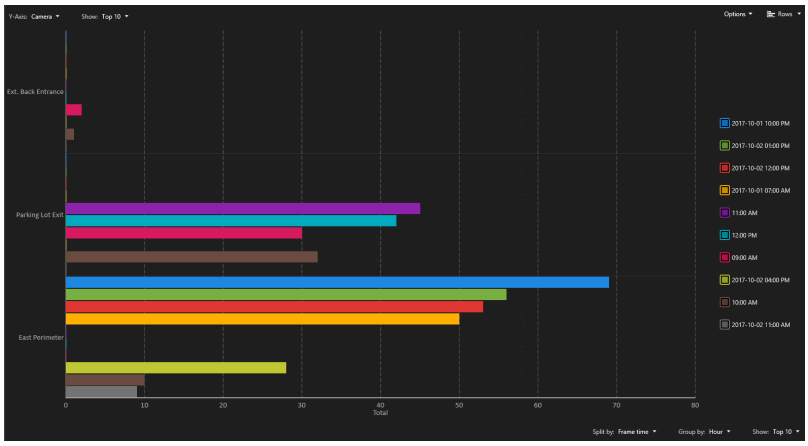
The following example shows a Door activities report, Split by: **Event**, Show: **Top 10** and X-Axis: **Door**, Show: **Top 10** as a **Stacked columns** chart.



Rows

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

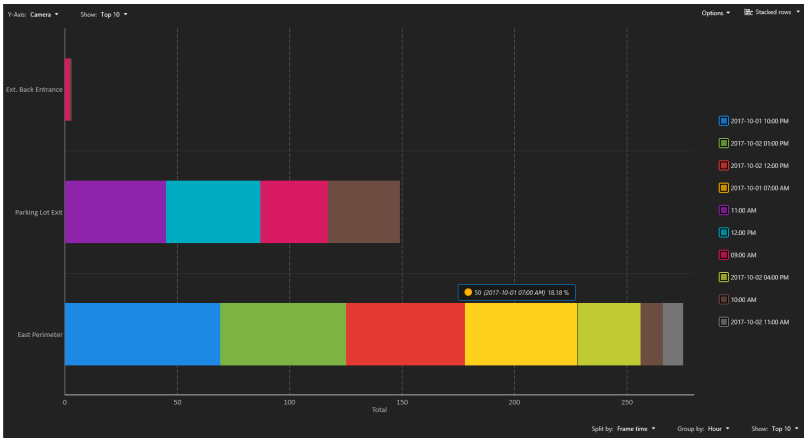
The following example shows an Intrusion detector report, Y-Axis: **Camera**, Show: **Top 10** and Split by: **Frame time**, Group by: **Hour**, Show: **Top 10** as a **Rows** chart.



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.



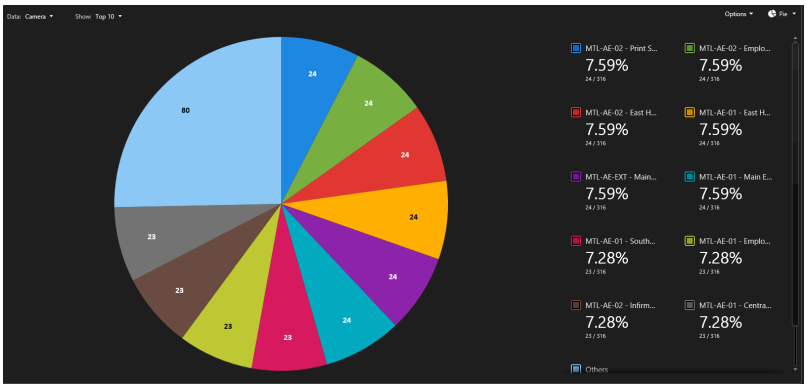
Pie and Doughnut charts

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.

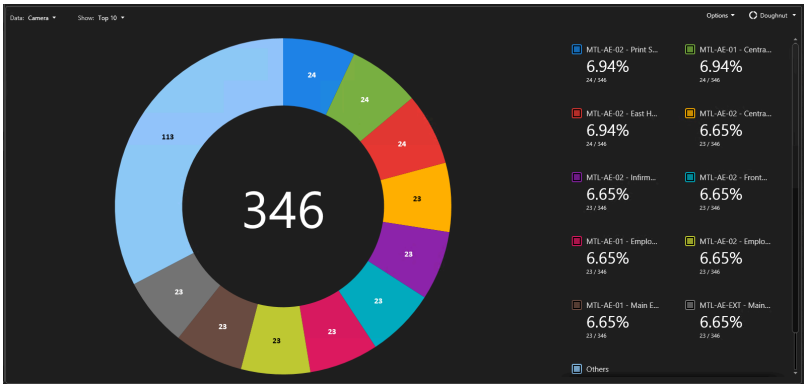
Pie chart

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



Doughnut chart

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



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 76

Generating reports

To generate a report in any reporting task, you must set the query filters, and then run the query. After you generate the 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 1000. This value can be changed in Performance section of the *Options* dialog box in Security Center.

If you want to generate a report with more than 50,000 results, then use the **Generate and save report** command.

NOTE: 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.

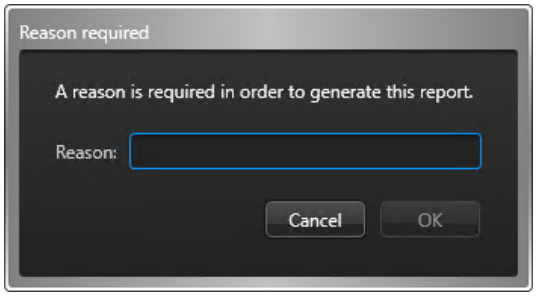
NOTE: Some of the filters have a **Select all** button. This button does not appear if there are more than 100 entities to select from (for example, if you have a list of 1500 cardholders), because if you query too many entities the report takes too long to generate.

3 Set a date and time range for the report.

4 Click **Generate report**.

If there are invalid filters, the **Generate report** button is unavailable.

IMPORTANT: The *Reason required* dialog is displayed when generating any report that contains ALPR data.



This ensures that the reason for the ALPR search is logged and included in Activity trail (Report generated) audit logs to comply with State laws.

The query results are displayed in the report pane.

TIP: You can sort the results by column. You can also right-click the titles row to select columns, then add or remove columns as required.

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 print the report, save the report as an Excel or PDF document, export the video sequences, and so on.

7 (Optional) Save the report as a template.

If you save the report layout (query filters and report columns) as a template, it can be sent to another user or workstation using 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

Generating visual reports on page 76

Selecting date and time ranges for reports

You can specify a date and time range to filter your report queries.

What you should know

If the time range is invalid, an error icon () appears, and you cannot generate the report. When the time range covers multiple days, a warning icon () appears on the filter, informing you the report might take longer to generate.

IMPORTANT: If you have a larger system that includes devices operating in different time zones, your time range filters are affected.

To select and date and time range for a report:

1 Open an existing reporting task, or create a new one.

2 In the *Time range* section, select one of the following time range modes:

NOTE: Depending on the reporting task you are using, this filter might be called **Triggered on** or **Event timestamp**.

- **During the last:** A relative time interval of seconds, minutes, hours, days, weeks, months, or years into the past. Report results can differ every time you run this query, because the time interval begins when the report is generated.
- **During the next:** A relative time range of seconds, minutes, hours, days, weeks, months, or years into the future. Report results can differ every time you run this query, because the time interval begins when the report is generated.
- **Specific range:** An absolute date and time range using *From* and *To* fields. The same report results will be produced every time you run the query.

3 If you select the **Specific range** time range mode, edit the **From** and **To** fields as follows:

a) Next to the **From** or **To** fields, click **Start** or **Now**.

b) To change the date, click the arrow, and then select a date in the calendar.

You can zoom out to view multiple years by clicking the calendar heading, or zoom in by clicking the year or month.

c) To specify a time, click the **Set time** link, and then enter the time directly in the time fields.

Related Topics

Customizing time zone settings on page 75
Opening tasks on page 53

Exporting generated reports

In every reporting task, you can export your report after it is generated. 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.

What you should know

The maximum number of report results that can be exported is 10, 000.

To export a generated report:

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

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.

NOTE: The dialog box options that are displayed can vary depending on whether the report supports Charts (Graph) or not. The Charts function is not supported for the following reports: Door Troubleshooter, Video File Explorer, and Motion Search.

3 Click **Export**.

Related Topics

Overview of the Alarm report task on page 608

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.

What you should know

NitroPdf is not currently supported.

To print a report (Print data):

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

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

TIP: You can also export ( ) the Report preview as a Microsoft Excel, Word, or Adobe PDF document.

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**.

Related Topics

Overview of the Alarm report task on page 608

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 home page, 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 A.M. and 10 A.M. 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 A.M. and 10 A.M. Pacific time.
- Fixed time zone (set to Eastern time): The report results are from events that occurred between 6 A.M. and 7 A.M. 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.

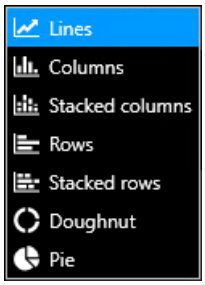
NOTE: The Charts function is not supported for the following reports: Door Troubleshooter, Video File Explorer, and Motion Search.

To generate a visual report:

1 Generate a report that supports the charts function.

2 Click **Charts** ( ).

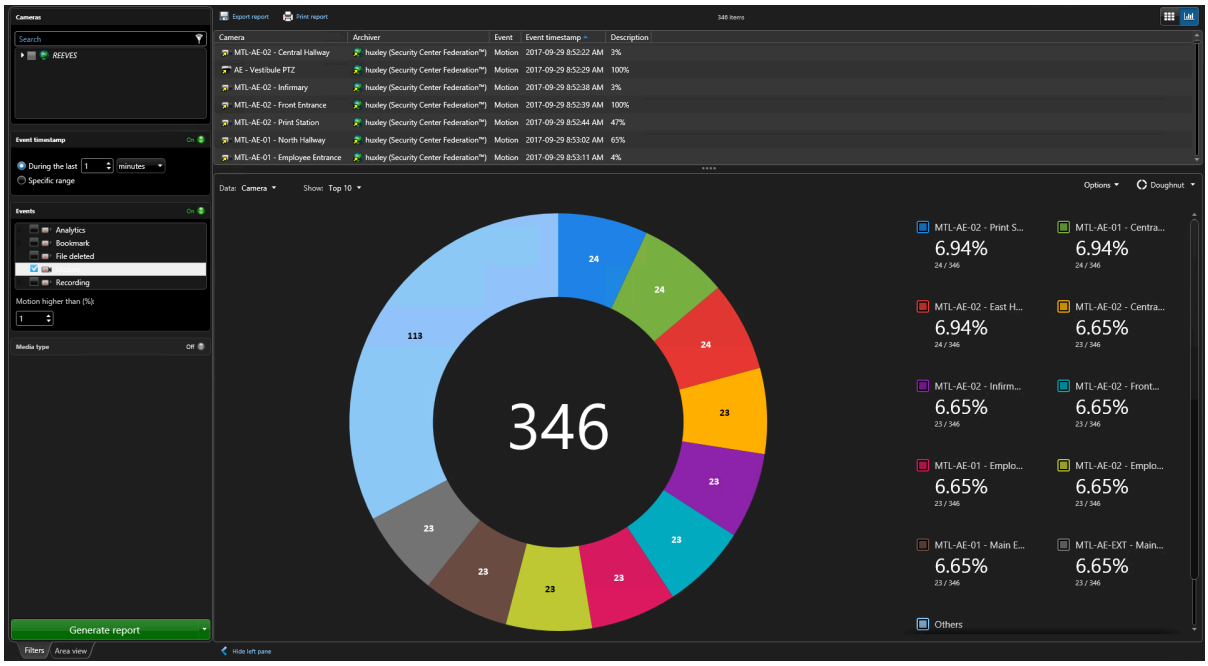
3 In the *Charts* pane, select a chart type from the drop-down menu.



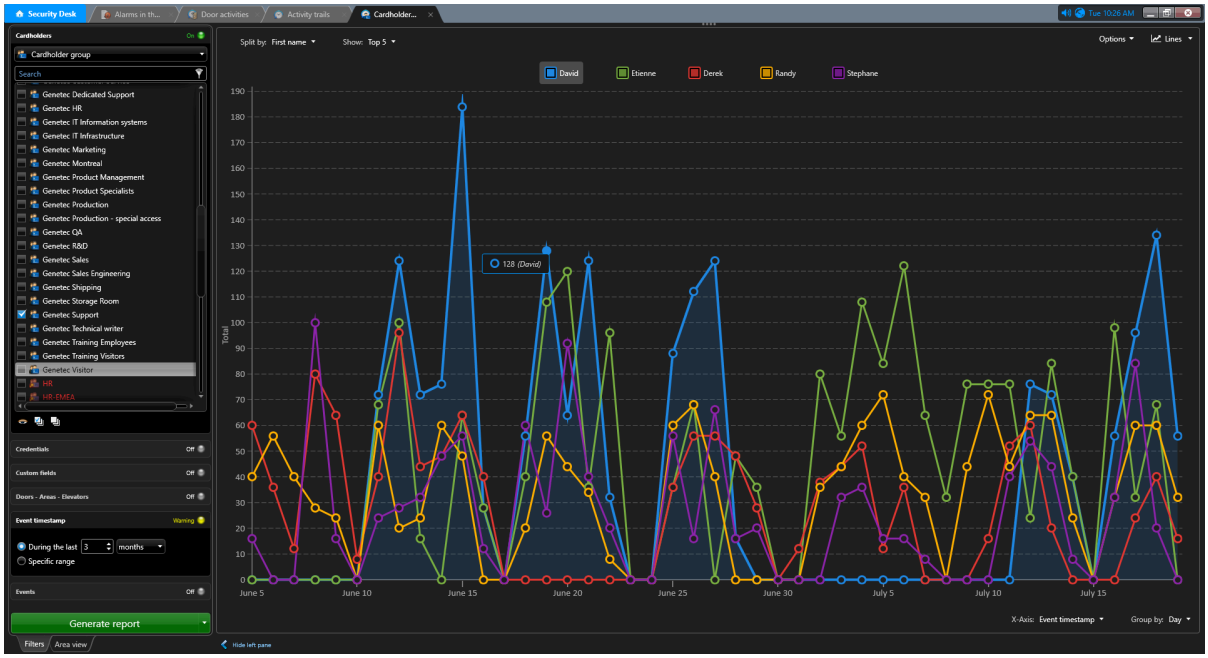
4 Select the data that you want displayed in the visual report using the drop-down menus in the *Charts* pane: **Split by**, **Show** (**Top 10**, **Top 5**, or **Top 3**), **X-Axis**, **Y-Axis**, or **Data**.

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.



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.



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 72
About visual reports on page 67
Exporting generated reports on page 74
Printing generated reports on page 74

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

Generating and saving a report is helpful, because you do not have to wait at your workstation for the report to generate. It is also helpful if your query has many results, because you are not limited to 10, 000 results like when you generate a report normally.

NOTE: The tasks that support this command are those where the results are queried from a role database, and not the directory.

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 100 entities to select from (for example, if you have a list of 1500 cardholders), because if you query too many entities the report takes too long 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 Click the drop-down arrow next to **Generate report** and click **Generate and save report**.

NOTE: To export *Audit trail* or *Activity trail* reports, you must generate and save using a manual action. See "Generating and saving reports using a system action" in the *Security Center User Guide* for more information.

6 In the dialog box, set the following options:

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

7 Click **Export**.

The report is saved in the location you specified.

Generating and saving reports using a system action

You can generate and save a report using a manual action.

Before you begin

- Save the task that you want to generate and export as a *public task*, with the query filters that you want applied, and the report columns you want to include. For more information see Saving tasks on page 54
- Set the maximum number of report results that can be saved in PDF or Excel format, and the destination folder from the Report Manager *Properties* tab. For more information, see the *Security Center Administrator Guide*.

To generate and save a report using a system action:

1 In the notification tray, click **Hot actions** ( ).

2 In the *Hot actions* dialog box, click **Manual action**.

3 In the list of actions, click **Export report**.

4 From the **Report** drop-down list, select the saved public task that you want to export.
5 From the **File format** drop-down list, select PDF, Excel, or CSV.
6 (PDF only) From the **Orientation** drop-down list, select whether the PDF file should be in portrait or landscape mode.
7 If you want to overwrite a report that was previously exported to the destination folder, then select the **Overwrite existing file** option.
8 Click **OK**.

The report is saved in the location 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 on 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 To sort the report by one of the columns, click the column heading. Click the column heading a second time to sort the report in the reverse order.

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 75
Saving tasks on page 54

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 home page, 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. If you want Security Center to display a warning message every time you are about to execute a query that might take a long time, select the **Display warning if query may take a long time to execute** option.
5. Click **Save**.

6

Basic tasks

This section includes the following topics:

Monitoring events

Using the *Monitoring* task, you can monitor events such as access control events from doors and cardholders, license plate reads and hits from fixed and mobile ALPR units, and camera related events, in real time.

What you should know

To monitoring events, you must monitor the entities that trigger those events. These entities are selected in the *Monitoring* task. You can customize how the *Monitoring* task displays information to suit the purpose of the task. For example, if you are monitoring cameras, you can hide everything else except for the canvas tiles to make the camera images bigger. You can create multiple Monitoring tasks to monitor different sets of entities, for example, only cameras or doors.

To monitor events:

1 Select the events to monitor.

2 Select the entities that are linked to the events you want to monitor.

After selecting the entities, events that occur in your system are shown chronologically in the event list and in real time. You cannot change the order of the events.

3 To show the event list, drag the divider down from the top of the *Monitoring* task window.

4 To choose what event information to display in the event list, right-click a column heading, and then click **Select columns** to choose the information you want to display in the list.

Example: In access control systems, you might only want to view cardholder and credential fields. In ALPR systems, you might only want to view plate numbers and context images.

5 To clear the event list, click **Clear event list** ( ) in the upper-right corner of the *Monitoring* task.

6 To monitor events in the canvas, choose one of the following two modes:

- **Tile mode:** Tile mode is the main Security Desk canvas operating mode that presents information in separate tiles. You can turn monitoring on or off for each tile.
- **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™, Genetec Mission Control™, or Record fusion, and requires a license for one of these major features.

  NOTE: To switch between tile mode and map mode, your account must have the *Switch to map mode* privilege.

7 From the area view, drag and drop the entities you want to view into the canvas.

8 (Optional) To protect the content in the tile from being overwritten by new events, turn off monitoring for that tile.

TIP: This is helpful if you have a tile plugin displayed in the canvas, and do not want an event to replace it.

a) Select a tile in the canvas.

b) In the tile widget, click **Monitoring** ( ), and click **Monitor events**.

The checkmark beside **Monitor events** disappears and tile ID background turns black.

Related Topics

Monitoring ALPR events in tile mode on page 387
Monitoring ALPR events in map mode on page 389

Selecting events to monitor

Before you can use the Monitoring task, you must select the event types you want to monitor.

To select events to monitor:

1 From the home page, click **Options** > **Events**.

2 In the **Event options** page, select which events to monitor.
3 In the **Display in tile** column, select the check boxes of the events you want to view in the Monitoring task canvas. If the check box is cleared, the event only appears in the event list.
4 Click **Save**.

After you finish

Select the entities you want to monitor that trigger the event types you selected.

Related Topics
Event types on page 541

Selecting entities to monitor

Before you can monitor events in the Monitoring task, you must select the entities that trigger those events.

Before you begin

Select the events to monitor.

What you should know

To monitor events, it is important to select which entities you want to monitor, because some event types can be generated by multiple entities. For example, an *Access granted* event can be generated by a cardholder, visitor, or credential. If you only monitor cardholders, you will not receive all *Access granted* events.

To select entities to monitor:

1 From the home page, click **Tasks** > **Monitoring**.
2 (Optional) To give the tab a unique name, right-click the tab, click **Rename task**; in the **Task name** box, type a name, then click **Rename**.

Example: You can rename the tab to indicate what is being monitored; for example, *Monitoring camera events*. This is helpful when you have multiple monitoring tabs open at the same time.

3 In the area view, select the entities you want to monitor (specific cameras, doors, cardholder, patrol vehicles, fixed AutoVu™ Sharp cameras, hotlists, and so on).

To select multiple entities, hold Ctrl or Shift, and then select the entities.

4 Drag the selected entities over the **Monitoring** ( ) icon at the bottom of the Monitoring task.

The entities you selected are added to the **Event monitoring** list.

NOTE: By default, all tiles are armed to monitor events. You can arm and disarm all tiles at any time by clicking . When a tile is armed to monitor events the tile ID background is blue.

5 (Optional) To add more entities from the *Event monitoring* dialog box, do the following:
   a) Click **Monitoring** ( ), and then under **Event monitoring** click **Add** ( ).
   b) Select the entity type you want to monitor (area view, cardholder, cardholder group, visitor, hotlist, permit, user, asset, and so on).

      TIP: Certain entity types, such as areas, doors, elevators, zones, and so on, only appear in the *area view* drop-down list.

   c) Select the entities you want to monitor (specific cameras, doors, cardholder, patrol vehicles, fixed AutoVu™ Sharp cameras, hotlists, and so on).
   d) To add a conditional filter, select an entity from the **For** drop-down list.

      Example: You can monitor events for a cardholder group at a specific door.

      NOTE: Only events that are related to the cardholder group *and* the door are monitored. You will not receive other events for the door unless you are also monitoring that door.
   e) Click **Add**.

6 (Optional) In the *Tile* column of the **Event monitoring** list, select a tile to display the entity in.

You can associate more than one entity to the same tile. By default, events are displayed in any tile (All).

Example: You can set Tile 1 to display events happening at the *Main Entrance* door.

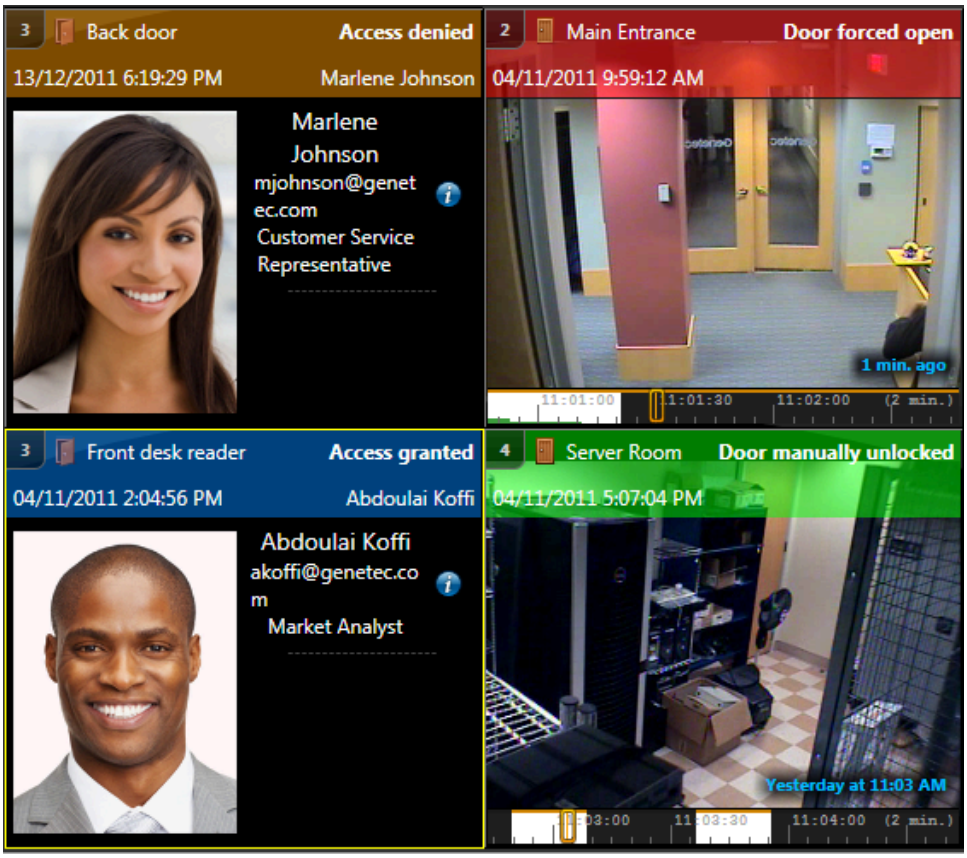
Monitoring is turned on in the canvas tiles. When a new event occurs, Security Desk displays the event in an empty tile. When there are no more empty tiles, the entity that has been displayed for the longest time is replaced by the new event.

Event colors

When you are monitoring entities, events generated by the entity are displayed in the canvas using different colors, depending on the event type. When you have a large system, this helps you focus on the events that are more important.

Event colors are configured in Config Tool. For more information about assigning colors for events, see the *Security Center Administrator Guide*.

The following figure shows four access control event that have been assigned different colors.



Customizing Monitoring task options

You can customize how many events are retrieved from the database and displayed when you load a saved Monitoring task.

What you should know

This setting is saved as part of your user profile.

To customize Monitoring task options:

1. From the home page, click **Options** > **Performance**.
2. In the **Maximum number of events to show** option, select the maximum number of events to load.
3. Click **Save**.

Event occurrence periods

Certain intrusion detection units and access control units can store events that occur while the units are disconnected from Security Center but still physically running. Occurrence periods indicate when these offline events occurred, and determine what happens with the events after the units reconnect to Security Center.

The occurrence period of an event is shown in the **Occurrence period** column in reports and in the *Monitoring* task. Events are treated differently in Security Center, based on whether its source entity is an intrusion detection unit or an access control unit.

The following table lists the different occurrence periods, and how they affect events:

Occurrence period	How the event is treated in Security Center
Online	• The event occurred while the unit was online. • The event is recorded in the database and is available for reporting. • The event appears in the *Monitoring* task. • The event can trigger actions through event-to-actions.
Grace period	• The event is recorded in the database and is available for reporting. • The event appears in the *Monitoring* task. • The event can trigger actions through event-to-actions.
	• For intrusion detection units: The event occurred during the **Grace period** configured for the unit extension in Config Tool. • For access control units: The event occurred within 15 minutes before the unit came back online.

Offline alarm	• The event is recorded in the database and is available for reporting.
	• The event does not appear in the *Monitoring* task, except for specific intrusion events.
	• The event can trigger the following actions through event-to-actions:
	  • *Trigger alarm*
	  • *Add bookmark*

	• For intrusion detection units: The event occurred between the **Grace period** and the **Alarm grace period** configured for the unit extension in Config Tool. The following events appear in the *Monitoring* task, and can trigger actions through event-to-actions:
	  • *Input alarm activated*
	  • *Intrusion detection area alarm activated*
	  • *Intrusion detection area duress*
	  • *Intrusion detection unit tamper*
	• For access control units: The event occurred within 72 hours before the unit came back online.

Occurrence period	How the event is treated in Security Center
Offline	• The event is recorded in the database and is available for reporting. • The event does not appear in the *Monitoring* task. • The event cannot trigger actions through event-to-actions.
	• For intrusion detection units: The event occurred between the **Alarm grace period** and the **Persistence grace period** configured for the unit extension in Config Tool. • For access control units: The event occurred more than 72 hours before the unit came back online.

Reasons why units can be offline

An access control or intrusion detection unit can be offline in Security Center for the following reasons:

- The unit is rebooting.
- The unit's firmware is being upgraded.
- The connection between the unit and the *Access Manager* or *Intrusion Manager* is lost.
- The connection between the Access Manager or the Intrusion Manager and the *Directory* is lost. When this happens, the role disconnects from its units until the connection with the Directory is re-established.

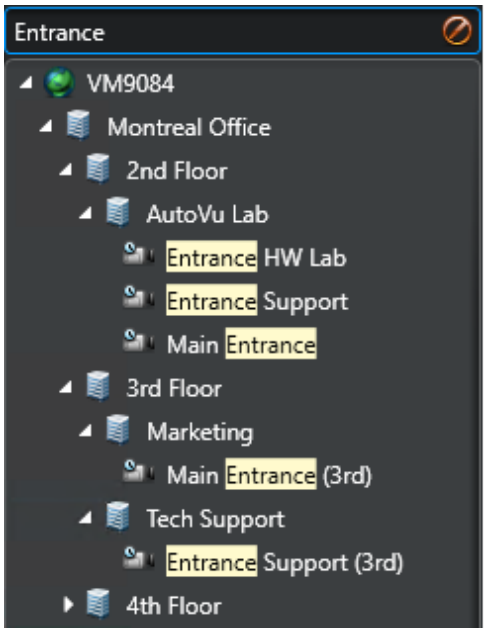
Searching for entities

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** ().



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

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

Related Topics

Entity states on page 513

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

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

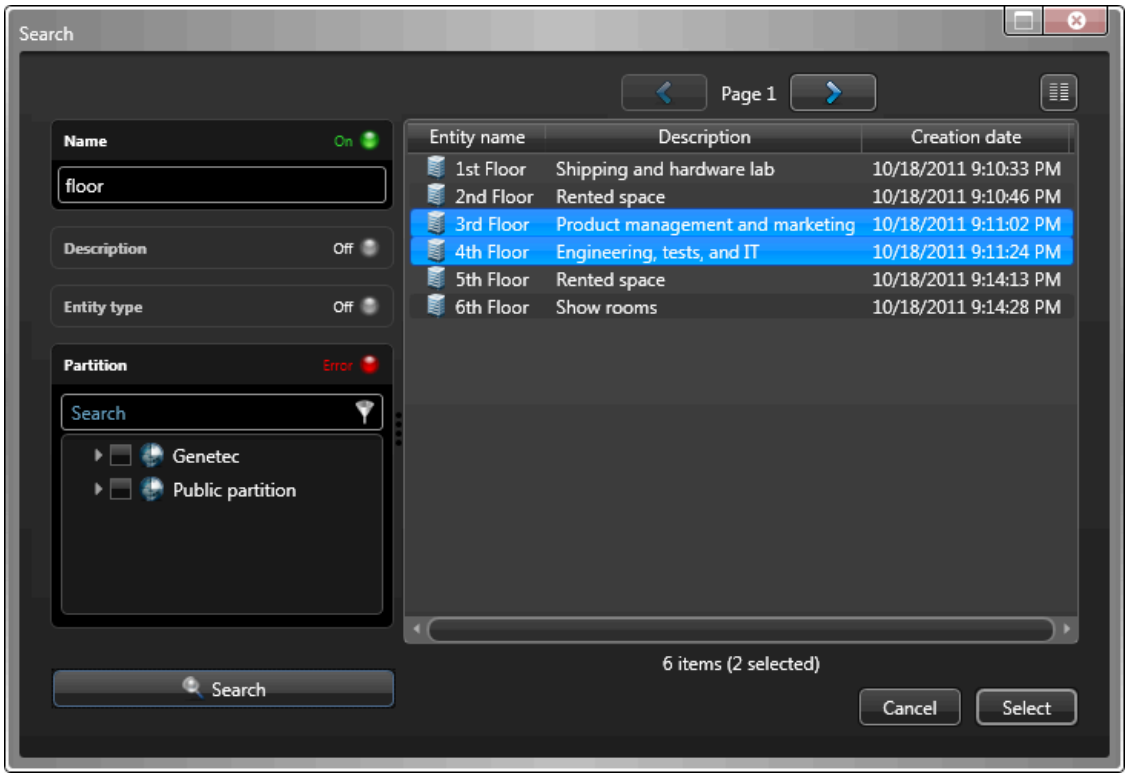
3 Click **Search** ().

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.



6 Click **Select**.

Only the entities you selected appear in the selector.

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

Triggering hot actions

You can create hot actions that can be triggered using the function keys on your keyboard, or from the notification tray.

What you should know

A hot action is an *action* that is mapped to a computer keyboard function key. You can trigger a hot action in Security Desk by pressing Ctrl+*function key* (for example, `Ctrl`+`F1` triggers the first hot action in the list), or from the notification tray.

NOTE: Mapping a hot action to a function key is specific to your user account.

To trigger a hot action:

1. In the notification tray, click **Hot actions** ( ).
2. In the *Hot actions* dialog box, click **Edit**.
3. Click **Add** ( ).
4. In the **Name** field, enter a name for the hot action.
5. In the *Configure an action* window, select an action type, and specify the additional settings required for the action.
6. Click **OK**.

   The hot action is created, and the *Hot action* dialog box closes.
7. To open the *Hot action* dialog box again, click **Hot actions** ( ) in the notification tray.
8. (Optional) Click to pin the *Hot action* dialog box to the side of your application workspace.
9. (Optional) Click **Edit**, and do one of the following:
   - To create another hot action, click **Add** ( ).
   - To delete the selected hot action, click **Remove** ( ).
   - To edit the selected hot action, click **Edit** ( ).
   - If you have more than one hot action created, click to move the selected hot action up the list. This changes the function key that the action is assigned to.
   - If you have more than one hot action created, click to move the selected hot action down the list. This changes the function key that the action is assigned to.
10. Click **Done**.

    The hot actions you created are listed with their assigned function keys (F1, F2, and so on).
11. Trigger the hot action one of the following ways:
    - Select a hot action, and then click **Execute**.
    - Press Ctrl+*Fn*.

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

Action types on page 565

Triggering one-time actions

In Security Center, you can trigger a one-time, manual action from the notification tray.

What you should know

Although actions are usually triggered through event-to-actions, you can also trigger them manually from the notification tray if needed.

For the following actions, only users who are online are available as recipients:

- Clear tasks
- Display an entity in Security Desk
- Play a sound
- Send a message
- Send task

To trigger a one-time action:

1. In the notification tray, click **Hot actions** ( ).
2. In the *Hot actions* dialog box, click **Manual action**.
3. In the *Configure an action* window, select an action type, and specify the additional settings required for the action.
4. Click **OK**.

The manual action is triggered.

Related Topics

Action types on page 565

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 home page, 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**.

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
	**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.
	**Session info**	Shows the current username and Security Center Directory name. Double-click to toggle between the long and short display.
	**Volume**	Shows the volume setting (0 - 100) of Security Desk. Click to adjust the volume using a slider, or to mute the volume.
	**Monitor ID**	Shows the logical ID number assigned to your Security Desk monitor. Every individual monitor is assigned a unique ID number for the purpose of CCTV keyboard control, macros, and remote monitoring.

Icon	Name	Description
	**Remote monitoring**	Shows how many users are remotely controlling your Security Desk workstation. Click to view information about the users controlling your Security Desk, or kick out the users if you have the privileges to do so.
	**Record types**	Shows the number of *record types* for which the *record provider* is offline (). 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 Using correlation to derive useful intelligence on page 109.
	**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 (). 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 505.
	**Hot actions**	Click to open the *Hot actions* dialog box, and trigger a manual action or a hot action. Hot actions are actions you can trigger by pressing a function key on your keyboard. For more information, see Triggering hot actions on page 92.
	**Joystick**	Shows that a USB controller, such as a joystick, is connected to your Security Desk workstation.
	**CCTV Keyboard**	Shows that a security keyboard is connected to your Security Desk workstation.
	**Threat levels**	Shows if there is a threat level set on your system. The icon turns red () when a threat level is activated. Click to open the *Threat levels* dialog box and activate or deactivate a threat level. For more information, see Responding to critical events through threat levels on page 491.
	**Alarms**	Shows the number of active alarms directed to you. The icon turns red () when you have active alarms in the system. Click to open the *Alarm monitoring* dialog box and view the active alarms. For more information, see Acknowledging alarms on page 465.
	**Inventory**	Shows the number of MLPI offload files waiting to be reconciled. Click to open the *Inventory management* task and reconcile the reads. For more information, see Creating parking facility inventories on page 455.
	**Updates**	Appears when there are critical firmware updates required. Click the icon to view the details.
	**Intrusion detection**	Shows the number of intrusion detection entities that require your attention (). Click to view the details in the **Intrusion detection overview** dialog box.
	**Task cycling**	Click to turn task cycling on or off. For more information about how to adjust the time spent on each task, see Customizing task behavior on page 63.
	**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 (). Click to open the *Card requests* dialog box and respond to the request. For more information, see Responding to credential card requests on page 349.

Icon	Name	Description
	**Video file conversion**	Shows the number of video file conversion requests that are pending and in progress (), or complete (). Click to open the *Conversion* dialog box. For more information, see Converting video files to ASF or MP4 format on page 264.
	**Retrieve cloud archives**	Shows the number of video requests from long-term Cloud storage that are in progress (), or complete (). Click to open the *Retrieve cloud archives* dialog box. For more information, see Requesting video archives from long-term Cloud storage on page 226.
	Genetec Clearance™ notifications	Shows the number of queued video export or upload requests to Genetec Clearance™ (). Genetec Clearance™ is an evidence management system that you can use to help accelerate investigations by securely collecting, managing, and sharing evidence from different sources. You only see these requests if the Genetec Clearance™ role is created in your system. For more information, see the *Genetec Clearance™ Plugin Guide*.

Moving the taskbar

You can configure the taskbar to appear on any edge of the application window, or to set it to auto-hide so it is only shown 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 home page, click **Options** > **Visual**.
2. From the **Taskbar position** drop-down 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**.

Remote monitoring

Using the *Remote* task, you can remotely monitor and control other Security Desk applications that are part of your system, using the *Monitoring* task and the *Alarm monitoring* task.

You can use the *Remote* task in the following two modes:

- **Simple mode:** Lets you control an individual Security Desk workstation.
- **Wall mode:** Lets you control a group of Security Desk monitors acting as a video wall. If you have physical video wall set up on your site, you can control all the monitors on that wall from your local Security Desk. Each monitor from the physical video wall is added as a separate remote Security Desk in the *Remote* task.

The actions you perform on the remote Security Desk are displayed locally in the *Remote* task, and on the remote Security Desk you are controlling. While remotely monitoring another Security Desk, you can still use all your local tasks.

IMPORTANT: You cannot remotely monitor Security Desk workstations with an earlier version of Security Center installed. Backward compatibility is not supported for remote monitoring.

Connecting to remote Security Desk applications

To monitor and control Security Desks remotely, you must connect to one remote Security Desk workstation (*Simple mode*), or multiple remote Security Desk monitors (*Wall mode*).

Before you begin

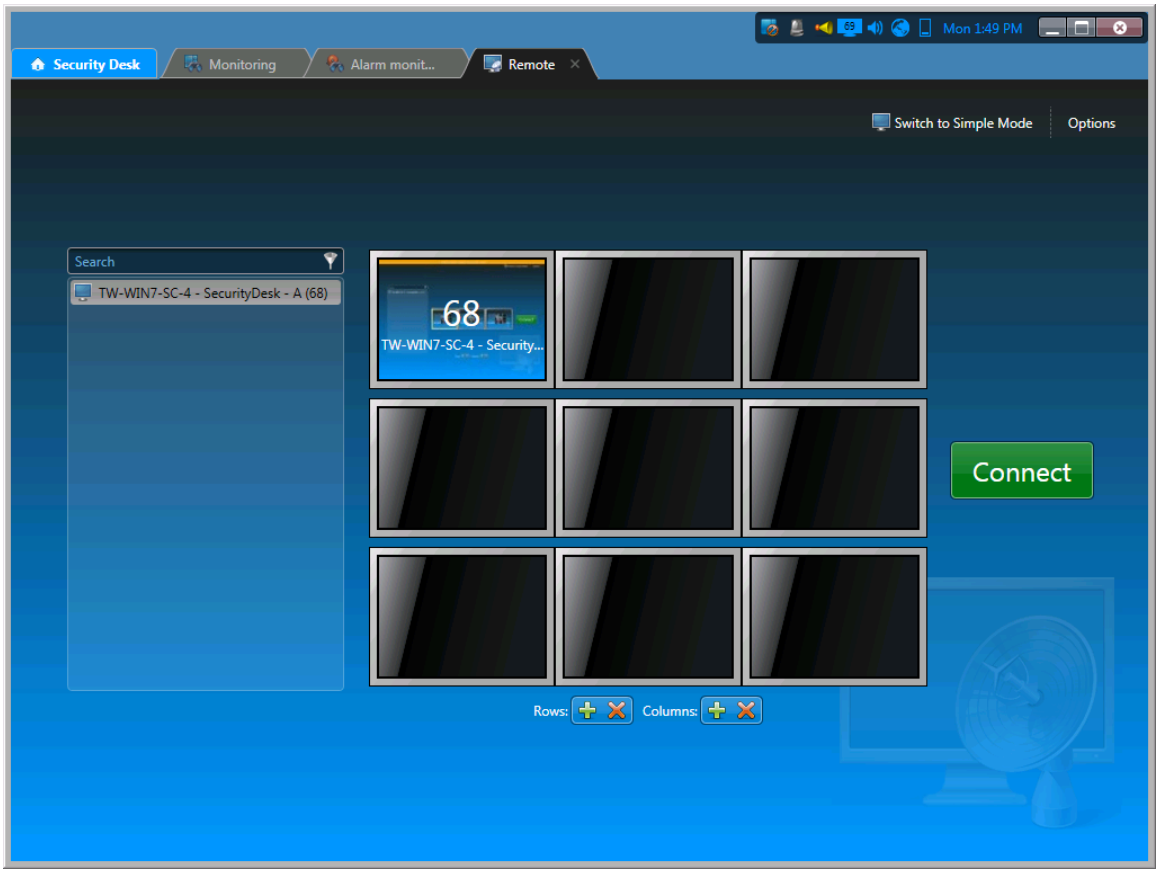
- The remote Security Desk must be running and connected to the same Security Center Directory.
- You must have *remote user control* of each Security Desk workstation you want to connect to. In Config Tool, your system administrator must select which workstations you can remotely control, from the *Advanced* configuration page of your user. For more information, see the *Security Center Administrator Guide*.

  NOTE: This step is only required if the user is not part of the Administrators group.
- You must have the same or more user privileges than the user who is logged on to the remote Security Desk. If you are missing some user privileges that the remote user has, your request to connect to the remote Security Desk is denied.
- You must be a member of all the partitions that the user who is logged on to the remote Security Desk is a member of. If you do not have access to some of the partitions that the remote user has access to, your remote connection is also denied.
- You must have the *Spy mode* privilege to connect to remote Security Desks in Spy mode.

To connect to remote Security Desks:

1 From the home page, open the *Remote* task.

2 To connect to one remote Security Desk, select a remote Security Desk workstation from the drop-down list, or to connect to multiple remote Security Desk monitors, proceed as follows:
   a) Click **Switch to Wall mode**.
   b) To configure the layout of your wall, use the ➕ and ✖ buttons in the *Rows* and *Columns* sections.
   c) From the drop-down list, double-click the remote Security Desk monitors you want to connect to.
   The monitors you select populate the empty tiles. To remove a monitor from a tile, click ✖ in the tile.



3 (Optional) Click **Options** and select one or both of the following:

- **Spy mode:** Allows you to connect to a remote Security Desk undetected. In this mode, you cannot perform any actions, you can only observe.
- **Low bandwidth:** Ensures that your bandwidth does not increase while remotely monitoring a Security Desk.

  This option is helpful because every command executed on the remote Security Desk is also executed on your local Security Desk, which might increase your bandwidth.

4 Click **Connect**.

You are connected to the remote Security Desk. If you are using Wall mode, the monitor that was placed in the first tile is displayed.

After you finish

When you are connected, you can view the tasks that were already opened on the remote Security Desk. However, you can only use the *Monitoring* task and the *Alarm monitoring* task. For all other tasks, the following message is displayed: *This task cannot be remotely controlled*.

NOTE: On the remote Security Desk, the number of users that are remotely controlling it are indicated on the **Remote monitoring** icon in the notification tray (), unless those users are in Spy mode. Click the **Remote monitoring** icon to view which users are remotely controlling your Security Desk, and which system they are on. If you have the user privilege, you can kick those users out of your Security Desk.

Related Topics

Overview of the Remote task on page 577

Monitoring events on remote Security Desk applications

In the *Monitoring* task on the remote Security Desk, you can use a subset of the actions available to you in a local *Monitoring* task. For example, you can only monitor video and access control and video entities (cameras, areas, doors, areas, elevators, intrusion detection areas, and so on).

Before you begin

Connect remotely to one or more Security Desk applications.

To monitor events on remote Security Desks:

1 Open the *Monitoring* task.

If the remote workstation does not have a *Monitoring* task open, proceed as follows:

a) Right-click the **Home** tab, and click **New task** ().
b) Click **Monitoring**, and type a name for the task.
c) Click **Create**.

2 Select which entities to monitor

This is done the same way as in a local *Monitoring* task.

3 To view an entity in a canvas tile, drag or double-click the entity from the area view.

¸The entity is displayed in your local Remote task, and on the remote workstation.

Related Topics

Selecting entities to monitor on page 85

Monitoring alarms on remote Security Desk applications

In the *Alarm monitoring* task on the remote Security Desk, you can acknowledge active alarms.

Before you begin

Connect remotely to one or more Security Desk applications.

To monitor alarms on remote Security Desks:

1 Open the *Alarm monitoring* task.

If the remote workstation does not have an *Alarm monitoring* task open, proceed as follows:

a) Right-click the **Home** tab and click **New task** ( ).

b) Click **Alarm monitoring**, and then click **Create**.

2 Select an active alarm in the canvas, and acknowledge the alarm.

Related Topics

Acknowledging alarms on page 465

Actions you can perform on remote Security Desk applications

The following table lists what you can do while remotely monitoring a Security Desk from the *Remote* task.

All the commands listed are already described elsewhere in this user guide. If you want to find out more information about these commands, click the *See also* links.

Command	Description	Default keyboard shortcut	See also
Controlling cameras			
View live video	You can view video in the *Monitoring* task. **NOTE:** You cannot hear audio from the remote monitor on your local Security Desk.		Live and playback video modes on page 221
Change the stream selection	Change the video stream on the selected camera.		Changing the video stream on page 198
Switch to playback	Switch to playback video when you are currently viewing live video.	P	Live and playback video modes on page 221
Pause/play	Pause or play the video recording.	G	Live and playback video modes on page 221
Previous frame	When your playback video is paused, go to the previous video frame.	N	Camera widget on page 39
Next frame	When your playback video is paused, go to the next video frame.	M	Camera widget on page 39
Jump backward	Jump backwards in the recorded video according to the seek time specified in the Video options tab.	Ctrl+Shift+N	Camera widget on page 39
Jump forward	Jump forward in the recorded video according to the seek time specified in the Video options tab.	Ctrl+Shift+M	Camera widget on page 39
Go to specific date/time	Jump to a specific time in the video recording.		Switching between video modes on page 223
Switch to live	Switch to live video.	L	Switching between video modes on page 223
Controlling PTZ cameras			
PTZ pan left	Pan the PTZ camera image to the left.	Left arrow	PTZ widget on page 47
PTZ pan right	Pan the PTZ camera image to the right.	Right arrow	

Command	Description	Default keyboard shortcut	See also
PTZ tilt down	Tilt the PTZ camera image down.	DOWN ARROW	
PTZ tilt up	Tilt the PTZ camera image up.	UP ARROW	
PTZ zoom in	Zoom in the PTZ camera image.	Hold the PLUS SIGN (+)	
PTZ zoom out	Zoom out the PTZ camera image.	Hold the HYPHEN (-) key	
Go to preset	Go to preset position.		
Rename preset/pattern/ auxiliary	Rename a preset, pattern, or auxiliary.		
Save preset	Save preset position.		
Go to home position	Go to PTZ home (default) position.		
Adjust PTZ motor speed	Adjust the speed of the PTZ motor.		
Lock/unlock PTZ motor	Lock the PTZ controls from other users.		
Focus near/far	Manually focus the image near or far.		
Flip horizontally/ vertically	Flip the PTZ motor 180 degrees.		
Start PTZ pattern	Start a PTZ pattern. Click any preset of PTZ button to stop the pattern.		
Record new PTZ pattern	Record a new PTZ pattern.		
Set/clear auxiliary	Start or stop the PTZ auxiliary command.		
Controlling remote Security Desk layout			
Close all open tasks	Close all open tasks on the remote Security Desk workstation.		Opening tasks on page 53
Save the workspace	Save the task list so that it is automatically restored the next time same user logs on to the remote Security Desk.		Saving tasks on page 54

Command	Description	Default keyboard shortcut	See also
Start task cycling	Automatically switch between all loaded tasks in the Security Desk. By default, a 4 second dwell time for each task is used.		Opening tasks on page 53
Stop task cycling	Stop the task cycling rotation.		Opening tasks on page 53
Full screen	Toggle between displaying Security Desk in full screen and windows mode.		Opening tasks on page 53
Rename task	Rename the selected task.		Opening tasks on page 53
Change tile pattern	Change the tile pattern in the canvas.	Ctrl+P	• Changing tile patterns on page 31 • Customizing how tiles are displayed on page 33

7

Advanced tasks

This section includes the following topics:

Starting macros

You can start and stop a macro from the *System status* task.

Before you begin

You need the *Execute macros* privilege to start or stop macros.

What you should know

A macro is an entity that encapsulates a C# program that adds custom functionalities to Security Center. For more information about creating and configuring macros in Config Tool, see the *Security Center Administrator Guide*.

To start a marco:

1. From the home page, open the System status task.
2. From the **Monitor** drop-down list, select **Macros**.
   The macros that are part of your system are listed in the report pane.
3. Start a macro:
   - Select a macro in the report pane, and click **Start** ( ).
   - Click **Start** ( ), select a macro, and then click **Start**.
4. To stop an executing macro, select the macro in the report pane, and then click **Stop** ( ).

Using correlation to derive useful intelligence

You can use records imported from external sources to derive new information in Security Center using the *Records* investigation task.

Before you begin

Make sure that your system administrator has granted you the necessary privileges to use the *record types* you need.

What you should know

The *Records* task in an investigation task that you can use to query the *record providers* registered in Security Center and find relevant information based on known or suspected correlations.

Correlation refers to the relationship that exists between two types of events, A and B. A correlation exists between A and B if whenever event A occurs, event B is expected. For example, if whenever there is a large gathering of people, the number of new cases of COVID-19 increases in the following days, we can say that there is a correlation between large gatherings and the increase of the number of new cases of COVID-19.

To derive useful intelligence using the Records task:

1. On the Security Desk home page, open the *Records* task.
2. Click **Record types** and select the record types you want to analyze.

   Assuming your record types correspond to types of event, such as *arrests* or *thefts*, you can test whether a correlation exists between two record types by filtering them on a common property.

   NOTE: By default, the timestamp and the location properties are always available for correlation. The timestamp and location properties are the fields that your system administrator assigned the *Timestamp* and *Location* (or *Latitude* and *Longitude*) functions to. The actual field names might be different.

3. To correlate your record types by timestamp, click the **Event timestamp** filter and specify a range of dates or times.

   Use this option to filter the fields assigned to the *Timestamp* function in the record type. If you have other timestamp fields in your record type that are not assigned to the *Timestamp* function, you must specify them in the **Conditions** filter.

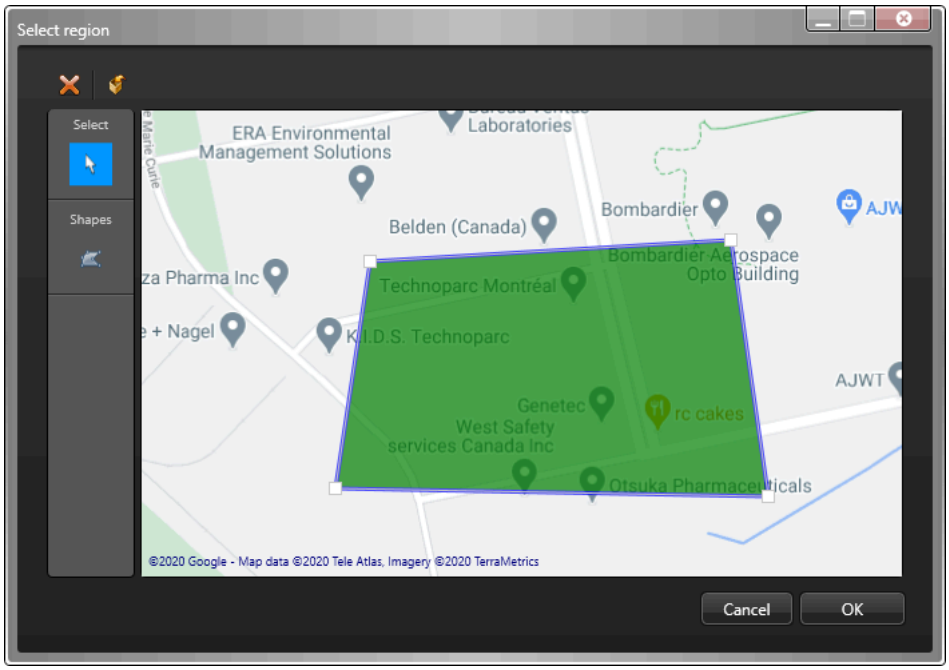
4 To correlate your record types by location, click the **Location** filter and draw the *regions* where the data must be found or excluded from.

a) Click **Edit**.

A map window opens.

b) Click **Draw polygon** ( ) to start drawing.

Click once for each endpoint, and click the first endpoint to close the polygon.



c) If necessary, click and drag a point to adjust the shape of the polygon.

d) If necessary, draw more regions.

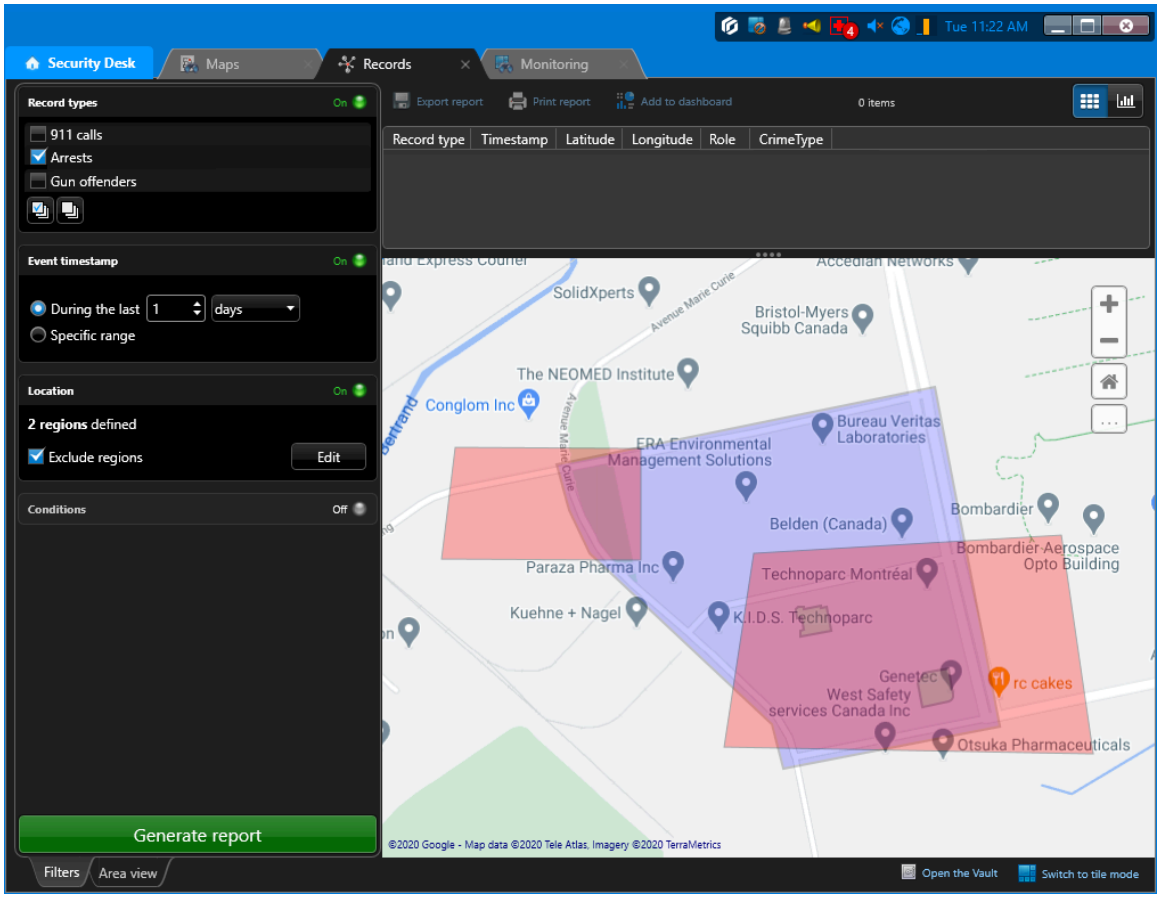
e) Click **OK** to save your changes.

f) Click **Switch to map mode** to change the canvas to the map display.

The regions added as location filter are displayed in green. Only records found within these regions are returned as results.

g) To exclude the records found within these regions from the results, select the **Exclude regions** option.

The color of the regions changes to red.


Tue 11:22 AM
Security Desk
Maps
Records
Monitoring
Record types
On
911 calls
Arrests
Gun offenders
Event timestamp
On
During the last 1 days
Specific range
Location
On
2 regions defined
Exclude regions
Edit
Conditions
Off
Generate report
Filters
Area view
Export report
Print report
Add to dashboard
0 items
Record type
Timestamp
Latitude
Longitude
Role
CrimeType
SolidXperts
Avenue Marie Curie
Bristol-Myers Squibb Canada
The NEOMED Institute
Conglom Inc
Bureau Veritas Laboratories
ERA Environmental Management Solutions
Belden (Canada)
Bombardier
Bombardier Aerospace Opto Building
Paraza Pharma Inc
Technoparc Montréal
Kuehne + Nagel
K.I.D.S. Technoparc
Genetec
West Safety services Canada Inc
rc cakes
Otsuka Pharmaceuticals
©2020 Google - Map data ©2020 Tele Atlas, Imagery ©2020 TerraMetrics
Open the Vault
Switch to tile mode

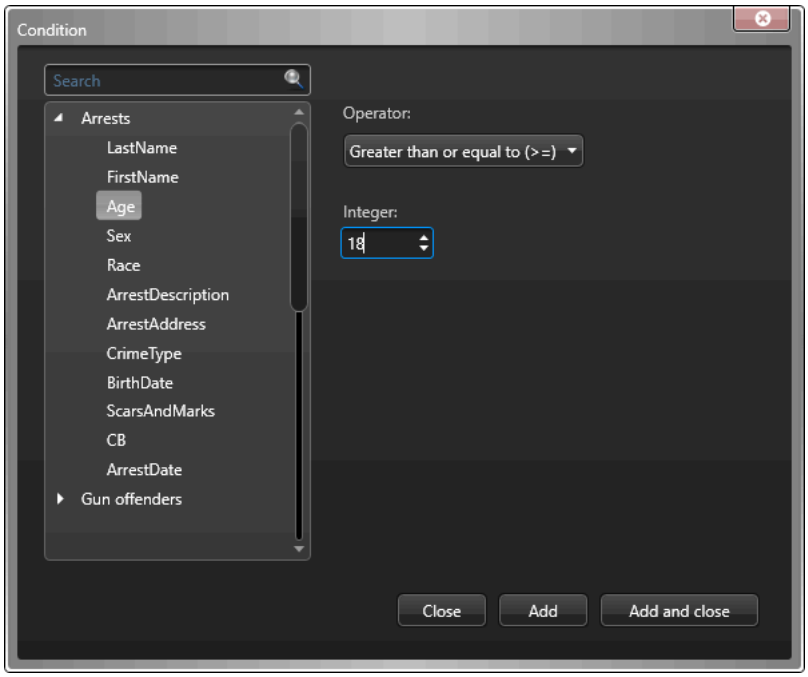
5 To add conditions on fields other than timestamp and location, click the **Conditions** filter.

If two record types each have a field with the same name and data type, conditions applied to one field are also applied to the other. If you add a condition for a field that doesn't exist in some record types, those records are not filtered based on that condition.

a) Click **Add an item** (+) under the **Conditions** filter.

The *Condition* dialog box opens.

b) Click the record type and the field you want to filter.



c) Select a comparison operator and a value, and then click **Add**.

NOTE: Enter string values without using double quotes.

For the **In** and **Not in** operators, enter a list of comma-separated values without adding a space after the comma, unless the space is part of the value you want to match.

For the pattern matching operator, enter the value as a regular expression.

- Click **Pattern matching options** > **General** for a list of the most commonly used metacharacters.
- Click **Pattern matching options** > **ALPR** to transform a license plate number you entered into a regular expression for matching OCR-equivalent characters, such as '8' and 'B', '1' and 'I', and '0' and 'O' and 'D'.

The condition is added to the **Conditions** filter.

d) Add more conditions on the same or different fields as needed.

6 Select the columns you want to see in your report.

Six columns are included by default:

- **ID:** Corresponds to the fields assigned to the *ID* function.
- **Record type:** Name of the record type the record belongs to.
- **Timestamp:** Corresponds to the fields assigned to the *Timestamp* function and used for the **Event timestamp** filter.
- **Latitude, Longitude:** These two columns correspond to the fields assigned to the *Location* (or *Latitude* and *Longitude*) functions and are used for the **Location** filter.
- **Role:** Name of the role that manages the record type.

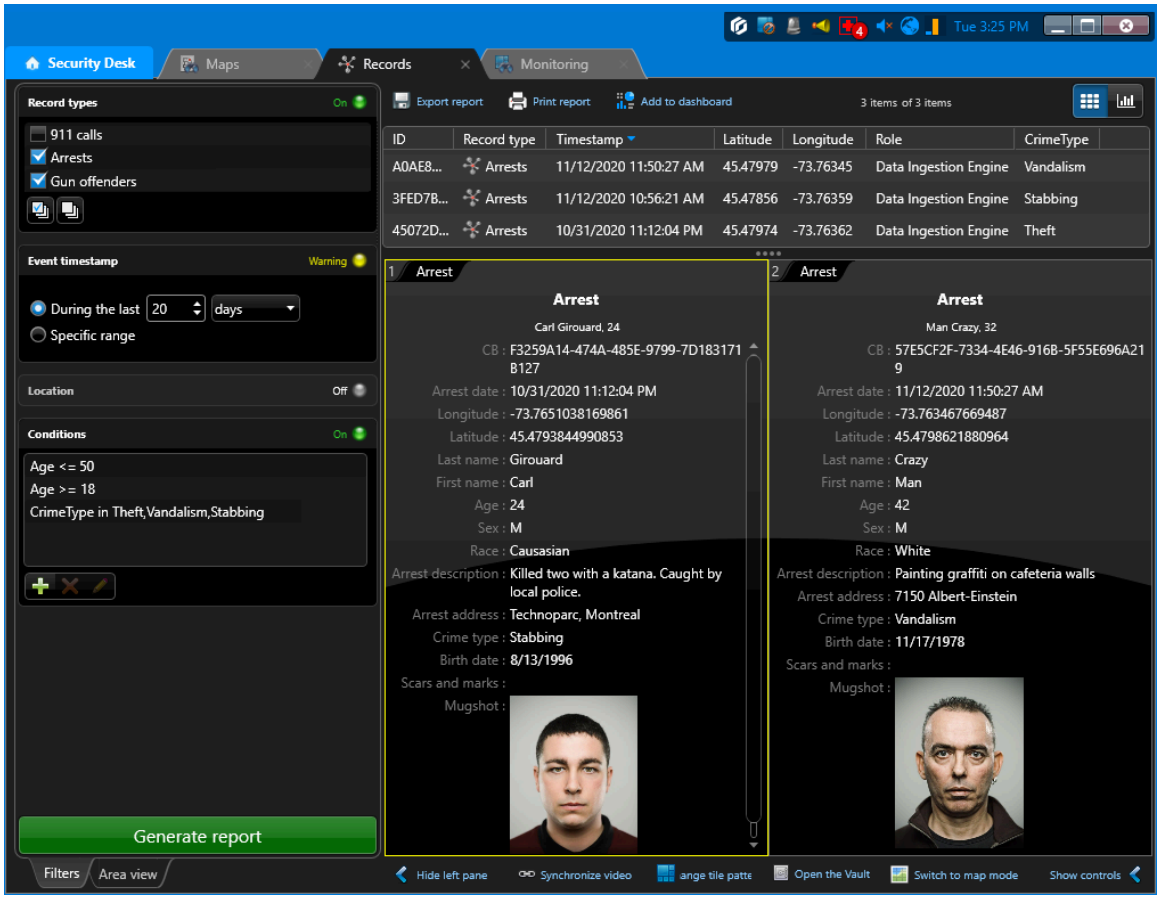
Some field names are unavailable because they could each have a different name in their respective record type. You can add or remove columns from the report as needed.

NOTE: Fields with the same name and type are considered to be identical in all record types and can only be included once in the report.

7 Click **Generate report**.

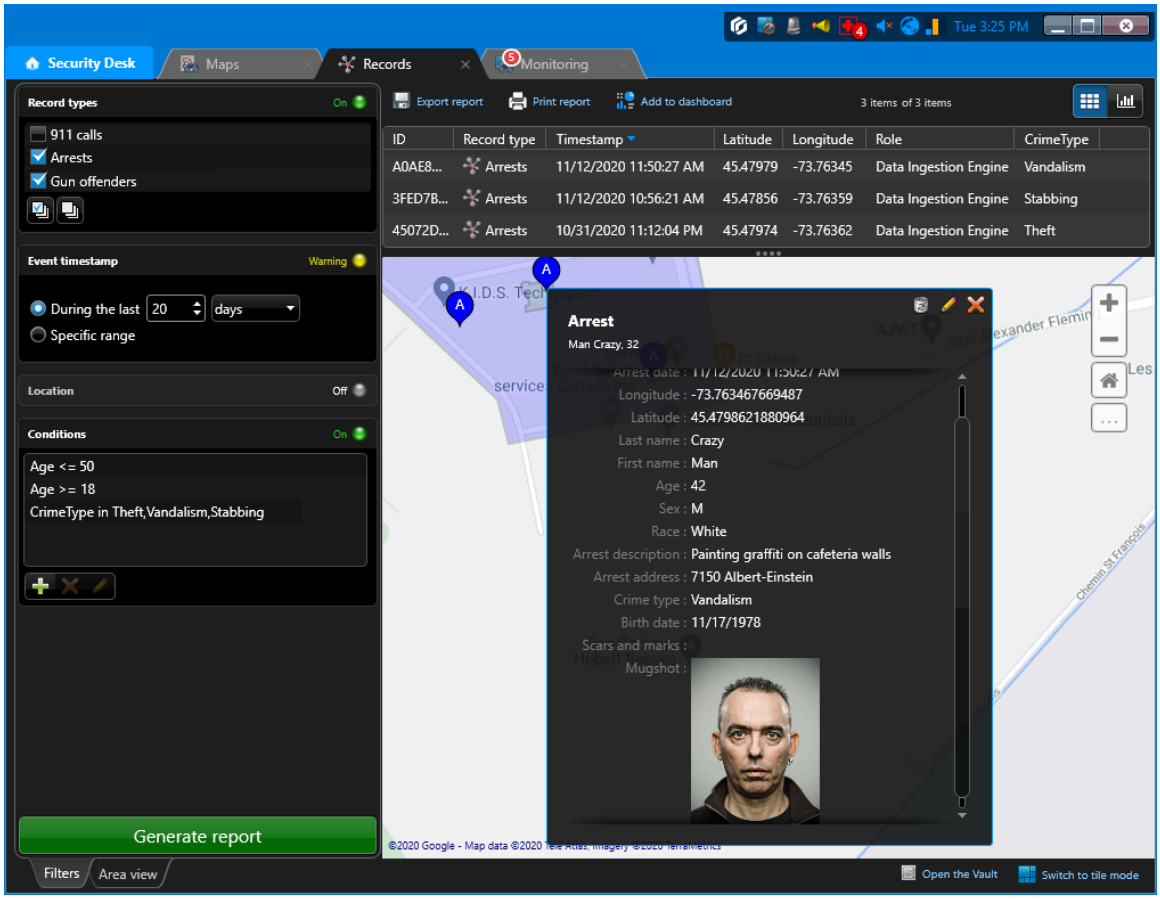
The query results are displayed in the report pane.

8 Double-click a row to display it in a tile in the canvas.



9 If the record types are georeferenced, click **Switch to map mode** to display the results on the map.

10 Click a map object of a record type to open the information bubble with the details of the record.



11 In the information bubble, click to edit the record or to delete the record.

12 Click to close the information bubble.

Related Topics

Customizing the report pane on page 81
Customizing report behavior on page 82
Adding records on maps on page 163

Performing complex scenario analysis using the aggregation widget

You can perform complex scenario analysis on records registered with the Record Fusion Service using the *Aggregation* widget in the *Dashboards* task. With this widget, you can easily drill down large amounts of data to discover new information.

Before you begin

Make sure that your system administrator has granted you the necessary privileges to use the *record types* you need for your analysis.

What you should know

The Aggregation widget provides a comprehensive set of data analysis tools. It generates simple charts by summarizing large amounts of data using aggregation functions, such as Sum, Count, Average, Maximum, and so on.

NOTE: The Aggregation widget only works on data managed by *record providers*. Record aggregation is performed on the servers hosting the record provider roles. Only the summary data is sent to the client, minimizing the network bandwidth usage and processing requirements on client workstations.

To create a scenario analysis chart:

1 Create a dashboard.

2 Drag the **Aggregation** widget to the dashboard.

3 Move the widget into position and resize as needed.

4 In the widget-specific options, select the **Aggregation options**.

- **Operation:** Select the aggregation function you want to apply on the selected field for records matching the specified filter criteria. The aggregation functions are: Count, Count distinct, Average, Maximum, Minimum, Standard deviation, Sum, Variance, and Median.
- **Apply over:** Select the field on which you want to apply the aggregation function. You can either select a field assigned to one of the standard functions: *ID*, *Time*, *Latitude*, *Longitude*, or select a field by name.

  To select a field by name, click **Custom**, then click , and then select the field you want from the list.
- **Group by:** You can optionally group the aggregation results by the value of another field. You have the following grouping options:
  - **Timestamp:** If all your record types have a *Timestamp* field, you can group the results by year, month, day of the week, hour of the day, or minute of the hour. If one of the record types you selected lacks the *Timestamp* field, that record type is excluded from the results.
  - **Record type:** If you are reporting on multiple record types, you can group by record type.
  - **Role:** If you have more than one record provider in your system, you can opt to group your results by role. The roles that can act as record providers are the Record Caching Service roles, the Map Manager role, and the Plugin roles.
  - **Custom:** You can use any field that is common to all your selected record types for grouping. To select a field, click **Custom**, then click , and then select the field you want from the list.

5 Select the record types you want to analyze.

a) In the *Record types* section, click **Add and item** ().

b) Select the record types you want and click **OK**.

Ensure that all the record types you select have the fields used for aggregation and grouping.

6 (Optional) Add filters for the records you want to analyze.

You can set three types of filters:

- **Time range:** Include only records falling within a specified time range. You can set this filter if all selected record types have the *Timestamp* field.
- **Location:** Include or exclude records found within the boundaries of regions drawn on the map as polygons. You can set this filter if all selected record types are georeferenced.
- **Conditions:** Include only records that meet certain conditions. These conditions can be based on any record fields.

To learn how to set up the record filters, see Using correlation to derive useful intelligence on page 109.

NOTE: If a filter or a condition does not apply to a record type, it is ignored for that record type.

7 Click **Rendered as** and select the type of chart you want.

You can choose from the following types:

- Columns (default)
- Doughnut
- Stacked columns
- Lines
- Pie
- Rows
- Stacked rows

8 To give a title to your chart, turn **Show title** on and set the **Title**.

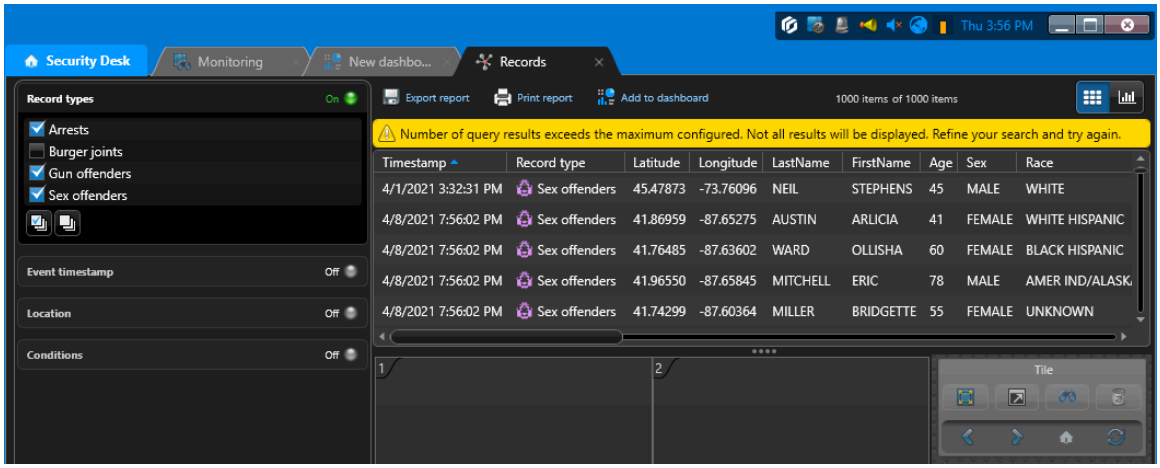
9 To change the background color, click **Background** and select a color.

10 To force the widget to refresh at regular interval, turn **Auto refresh** on and set the refresh interval.

11 Click **Done**.

12 Click **Show in records report** to open the *Records* task to display a report using the same record types and filters.

The aggregation function is not applied by the *Records* report, therefore, you might get a large number of records back. If the number of results exceeds the maximum allowed, you get a warning message.



TIP: You can change the **Maximum number of results** that the *Records* task can return in the *Performance* page of the *Options* dialog box.

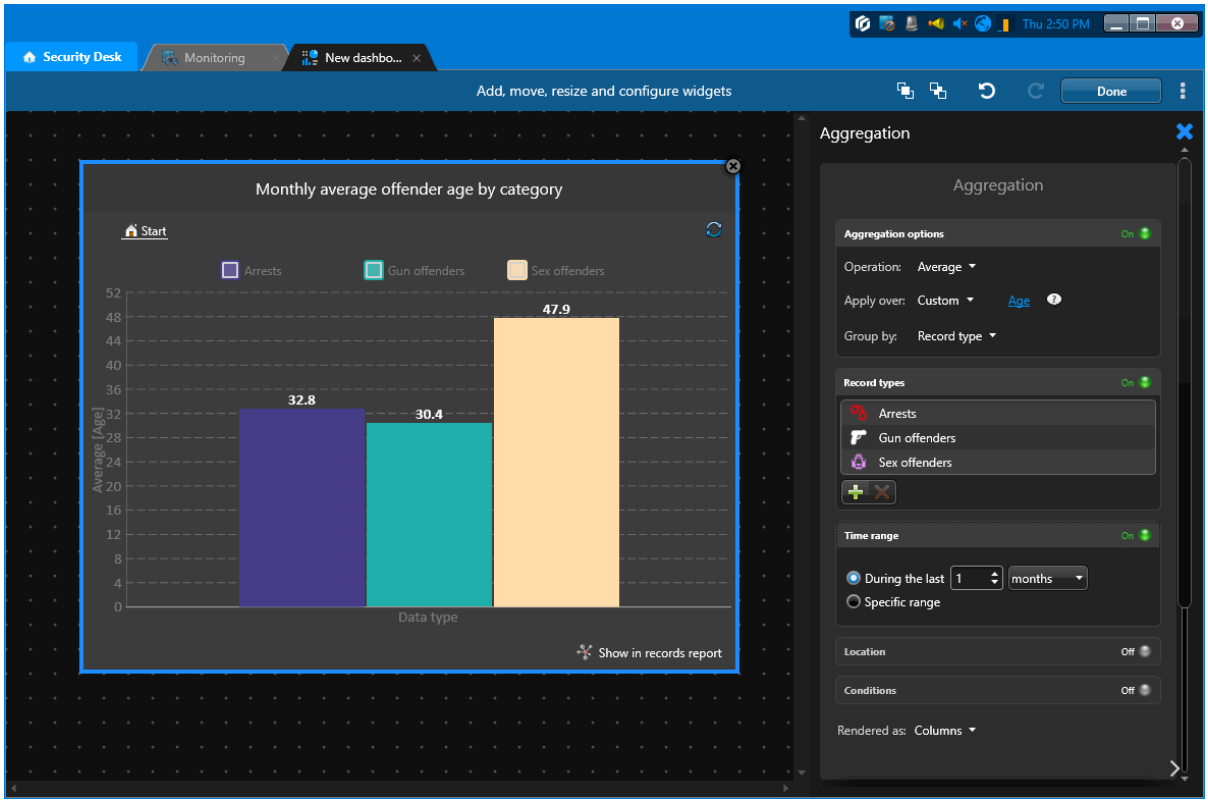
Example

Suppose you have three record types defined as follows:

- **Arrests:** Arrest date, Last name, First name, Age, Sex, Crime type, Race, and so on.
- **Gun offenders:** Report date, Last name, First name, Age, Sex, and so on.

- **Sex offenders:** Report date, Last name, First name, Age, Sex, and so on.

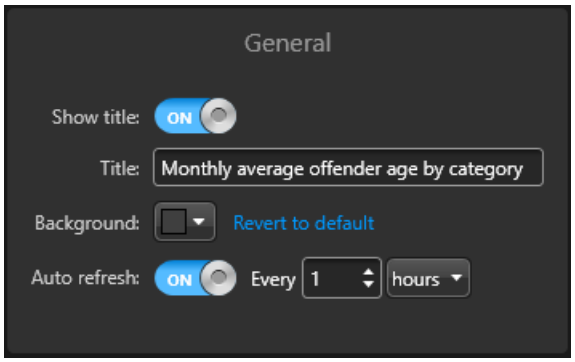
To create a chart that shows the average monthly offenders age by category, meaning by record type, select the **Average** operation, apply it to the **Age** field, and group the results by **Record type**.



In the *Record types* section, add the record types **Arrests**, **Gun offenders**, and **Sex offenders**.

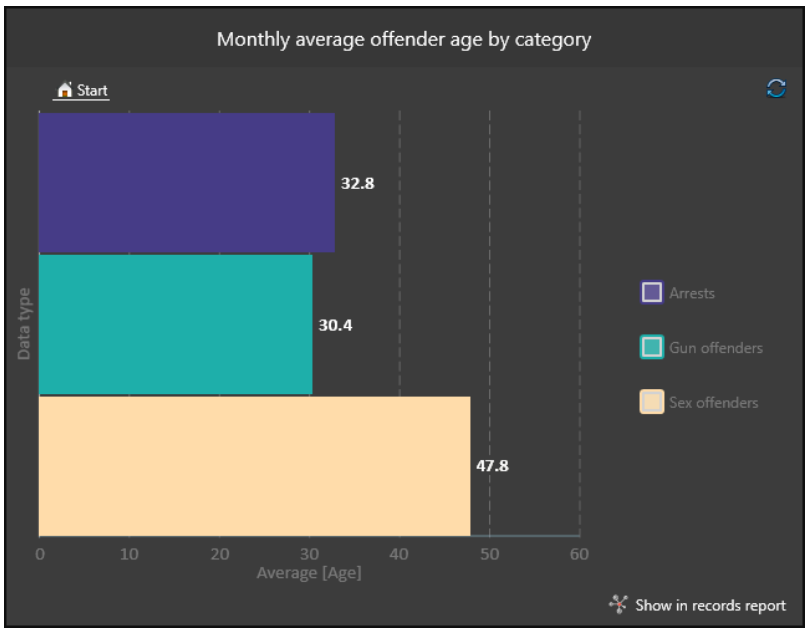
In the *Time range* section, select **During the last** 1 **month**.

Scroll to the bottom of the **Aggregation** settings, configure the **Title**, the **Background** color, and the **Auto refresh** option of the widget, and then click **Done**.



To change the type of chart, click **Edit dashboard** and then click your widget. Click **Rendered as**, select the type of chart, and then click **Done**.

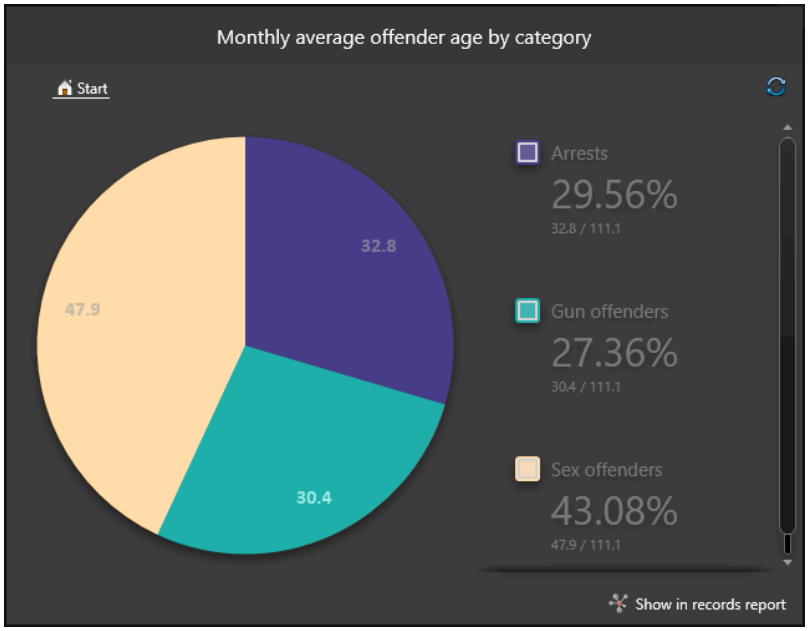
The **Rows** chart is like the **Columns** chart rotated 90 degrees. However, the results are displayed with greater precision.



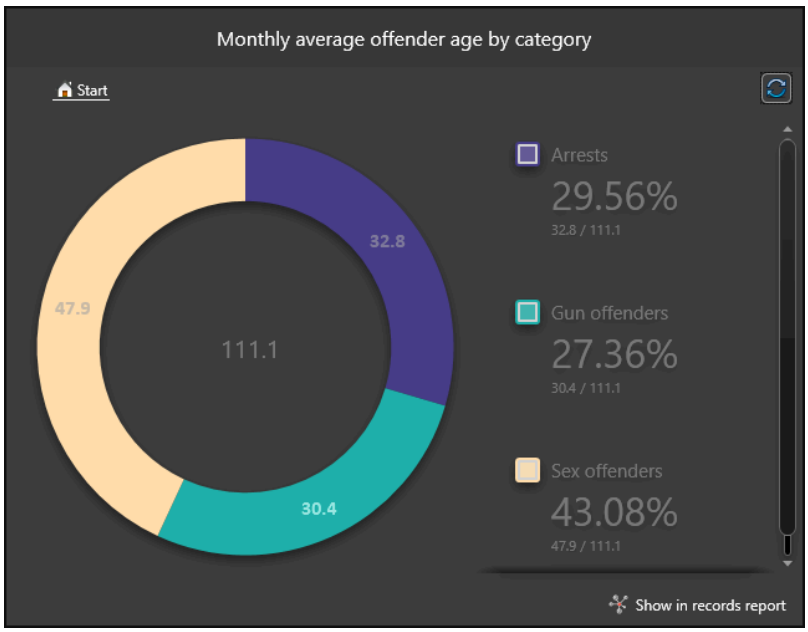
Click a result legend to temporarily hide it from the chart.

Click to restore all results.

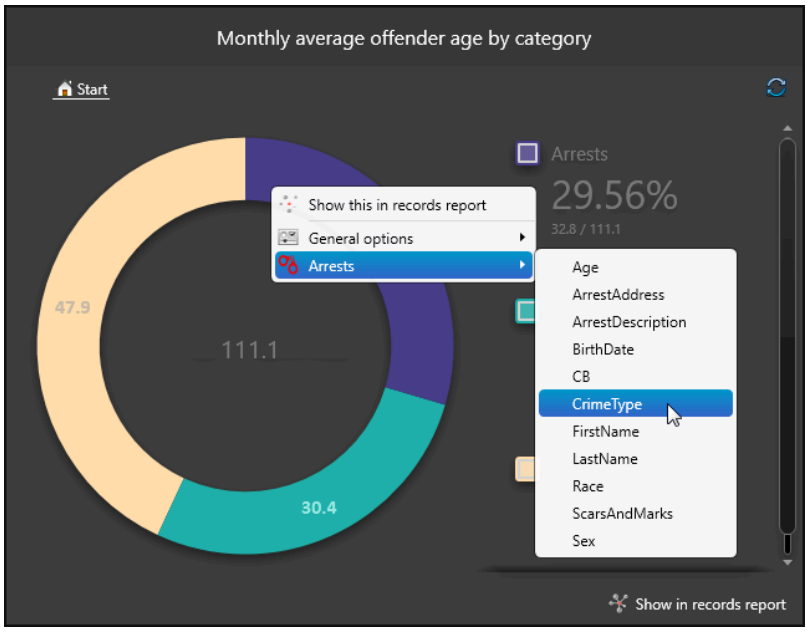
If you choose the **Pie** chart, the percentage of records in each category is also indicated.



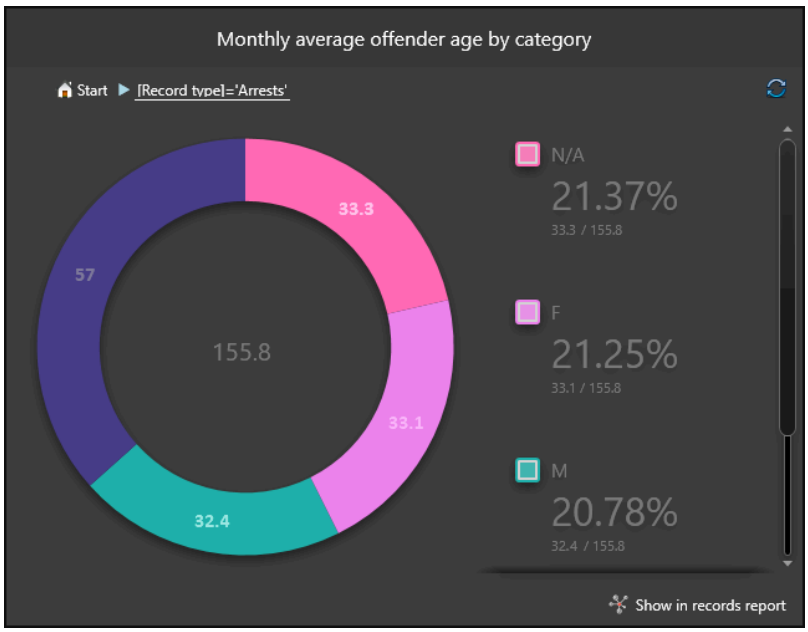
If you choose the **Doughnut** chart, the sum of the results is also displayed in the center.



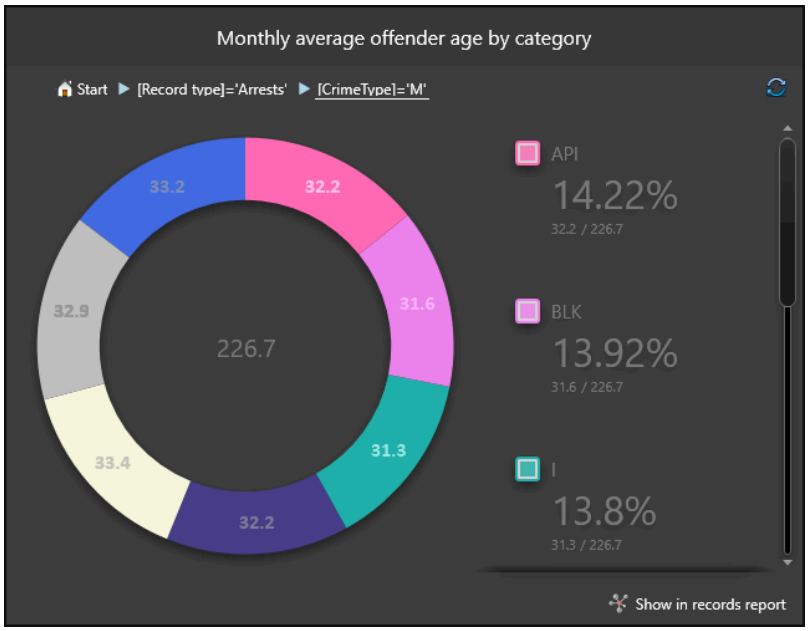
To drill down, right-click a result on the chart and select how you want to further explore that result. In our current example, you can right-click the purple section (Arrests), and select **CrimeType** to view the breakdown of arrests by crime type.



The result is a new chart showing the distribution of all arrests by crime type. You can scroll down to see all crime types.



You can further drill down by clicking the turquoise section ("M" for murder) and selecting **Race**. The result is a breakdown of all murders by race. Scroll down to see all the categories.



As you drill down, the widget leaves a bread-crumb. Click any bread crumb to go back to that step.

Click **Show in records report** to view the current results in the *Reports* task.

Click **Start** to view the original chart without loosing your drill-down steps.

Click to clear all drill-down steps.

Related Topics

Customizing the report pane on page 81
Customizing report behavior on page 82

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 home page, 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 client application 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.

Investigating user-related activity on your Security Center system

You can view all user activity related to video, access control, and ALPR, using the *Activity trails* report.

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 in Config Tool. For more information, see the *Security Center Administrator Guide*.

What you should know

For example, you can use the *Activity trails* task to find out 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, or who enabled hotlist filtering.

To investigate user related activity on the system:

1. From the home page, 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 client application was used for the activity.
   - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
   - **Events:** Select the events of interest. The event types available depend on the task you are using.
   - **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.
- **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.
- **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 Genetec 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 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.

Viewing unit properties

At a glance, you can view a list of all the local and federated units that are part of your system, and can see their information, such as unit type, manufacturer, model, IP address, and so on, using the *Hardware inventory* report.

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 needs to 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, and properties such as *Password*, *Proposed firmware version*, *Proposed firmware description*, and all certificate-related information, are not available for federated units.

To view the properties of units in your system:

1 From the home page, 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, Intrusion detection, ALPR, or Video).
- **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, Intrusion detection, ALPR, 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.
- **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.
- **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.

Monitoring your computer resources

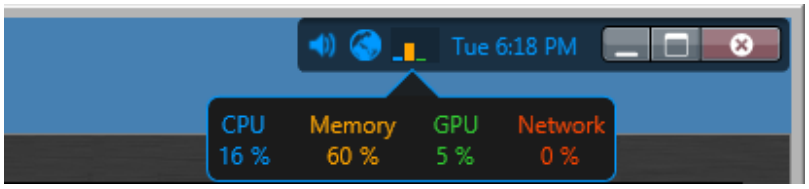
You can monitor the usage percentage of your computer resources by hovering the mouse pointer over the **Resources meter** icon in the notification tray. Click the same icon to view a summary of the hardware installed on your computer and their current use in a dialog box.

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.

2 Click the **Resources meter** icon in the notification tray to view detailed information about your computer resources in the Hardware information dialog box.

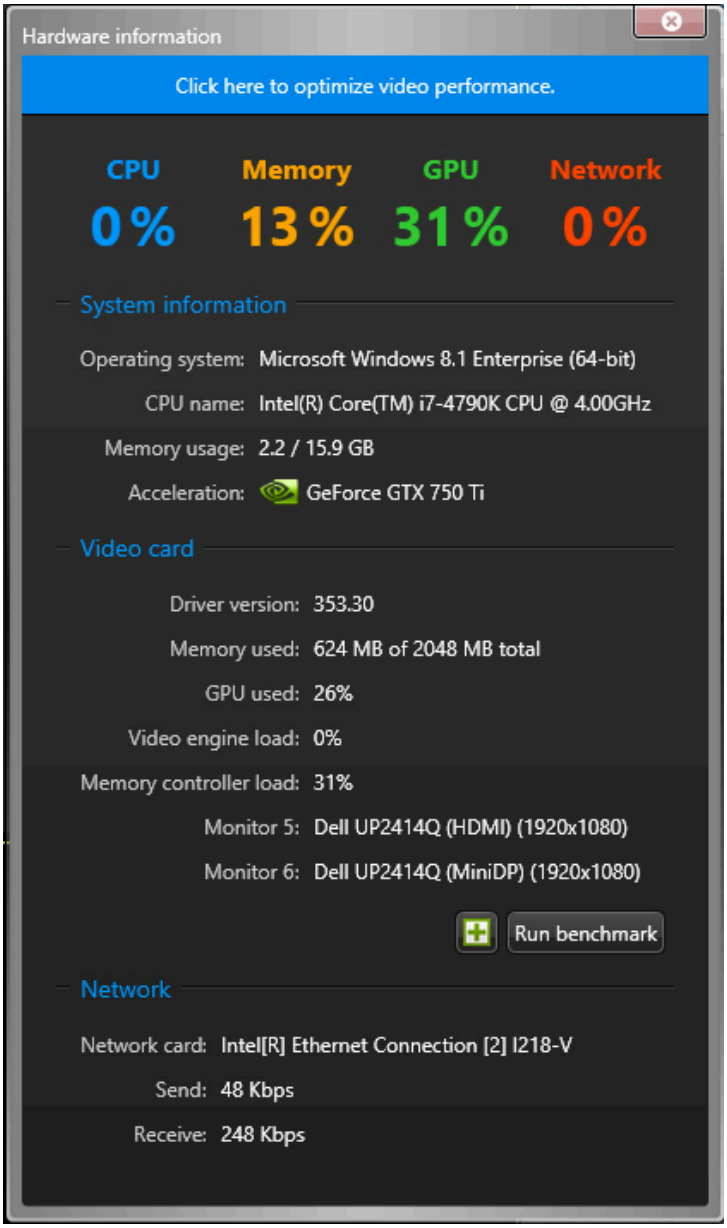
Related Topics

Video options on page 280

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.



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** drop-down list to pick the one you want to monitor.

For more information about running the hardware benchmark tool, see Using the hardware benchmark tool on page 131.

Related Topics

Video options on page 280
Optimizing video decoding performance on your computer on page 219

Using the hardware benchmark tool

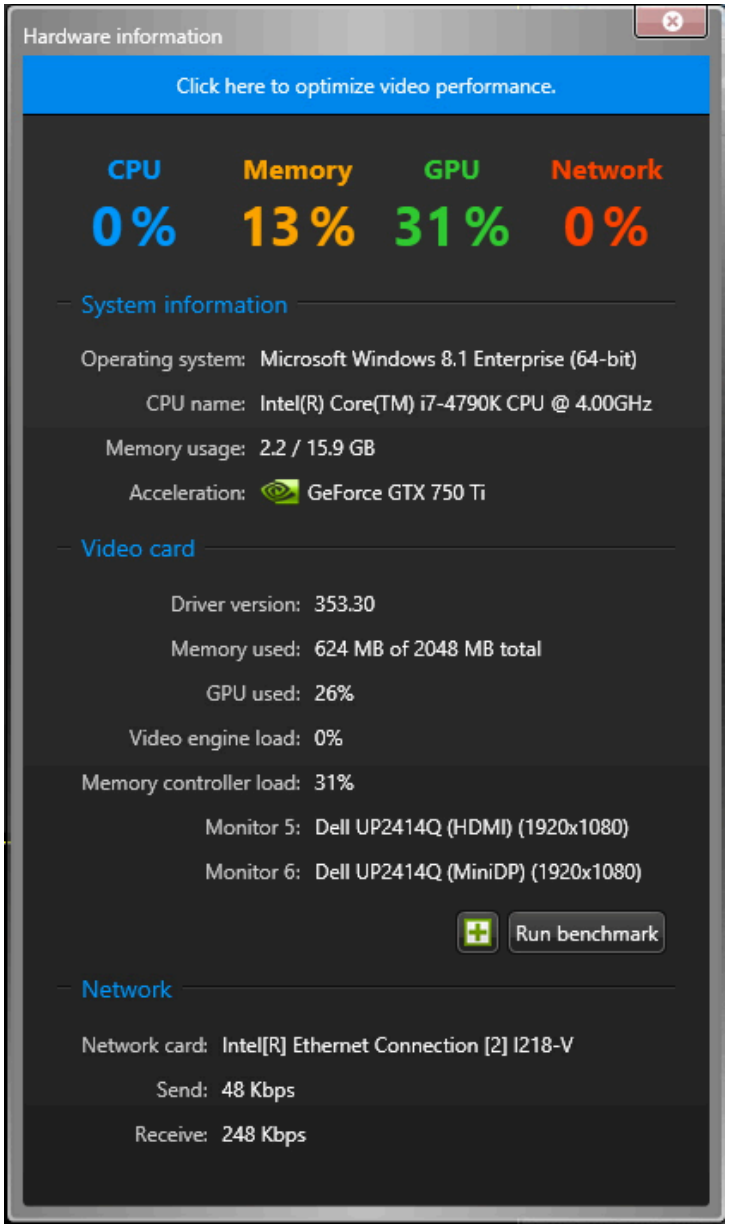
The hardware benchmark tool enables you to calibrate your settings to optimize the performance of your installed video cards. You can run the hardware benchmark tool in Config Tool or Security Desk.

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.

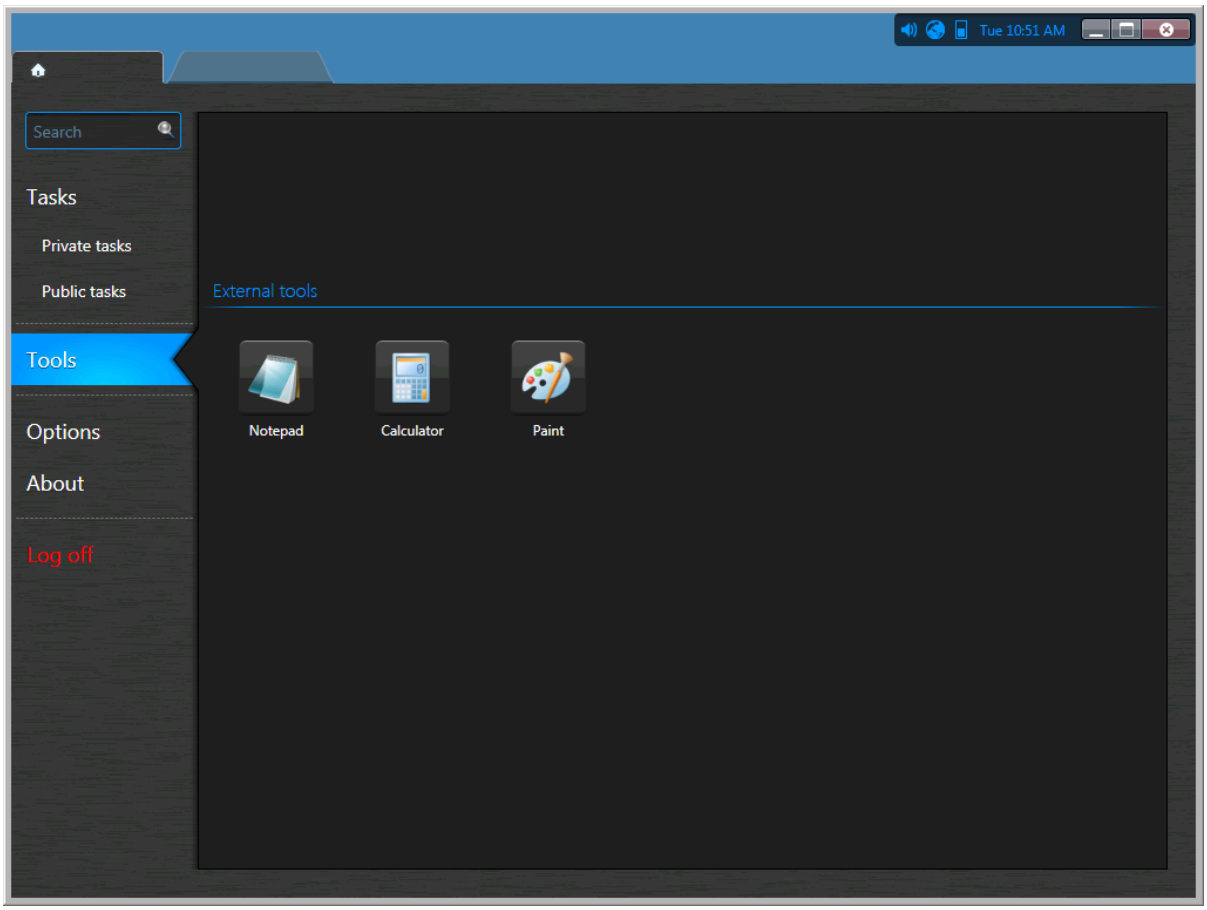


2 From the **Acceleration** drop-down list, select the video card you want to run the benchmark test on.
3 Click **Run benchmark**.
Once the benchmark test is complete, the **Frame rate** capability of the selected card is listed.
4 Click **Close**.

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 5.10* on a 64-bit computer, and in *C:\Program files\Genetec Security Center 5.10* 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-...>
    <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 be 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 on 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>
```

Customizing user logon options

You can select how and when users are allowed to log on to Security Center.

What you should know

You must be an administrator to configure the logon options. 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.

To customize user logon options:

1 From the home page in Config Tool, click **Options** > **General**.

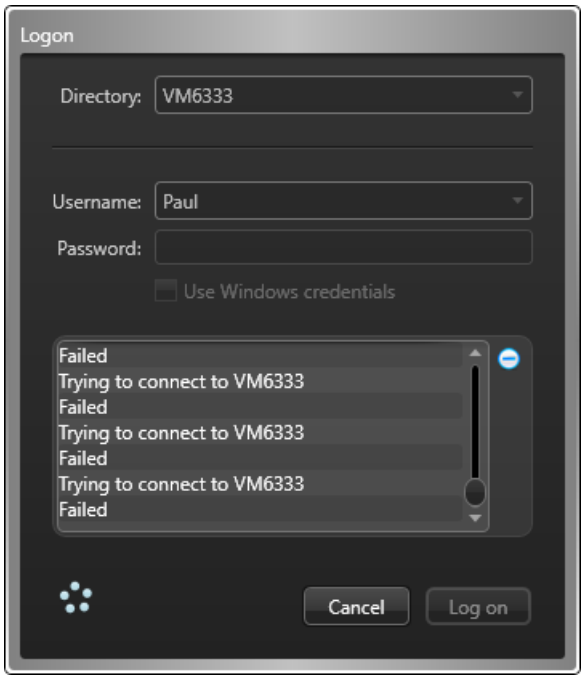
2 To force users to log on using Windows credentials, set the **Use Windows credentials** option to **Always**.

For this option to work, the users who are expected to log on using this computer must be imported from an *Active Directory*. For more information about importing users from a corporate Active Directory, see the *Security Center Administrator Guide*.

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), then the next time users try to log on, they will not be able to connect.



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 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.

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 home page, 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** drop-down 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

Dashboards

This section includes the following topics:

About dashboards

The *Dashboards* task is an operation task that provides a blank canvas on which you can pin widgets, including Security Center tiles, reports, and charts. These widgets track key indicators, and provide an overview of the activity and events recorded by the system.

Security Center dashboards have a broad range of uses. You can use them to:

- Create a command and control dashboard to help you monitor events, and dispatch guards.
- Track key performance indicators, such as the number and type of incidents, or wait times in queues.
- Monitor system health, from important health events to the availability statistics of system hardware and software.

  NOTE: A default *Health dashboard* is available as an operation task to monitor your system health information.

By customizing a dashboard to your needs, you can easily monitor the information that matters to you.

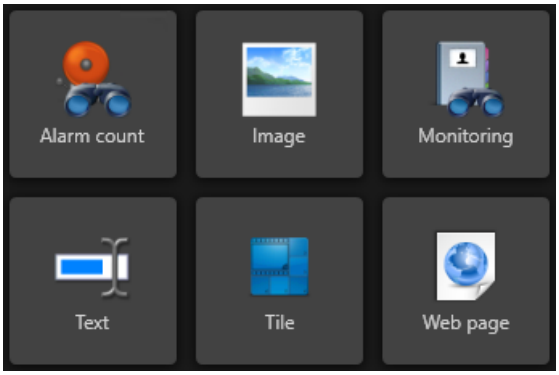
Dashboard configurations can be saved as public tasks or private tasks in Security Desk. Your dashboard can be personal, or shared with an entire organization.

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

Dashboard widgets

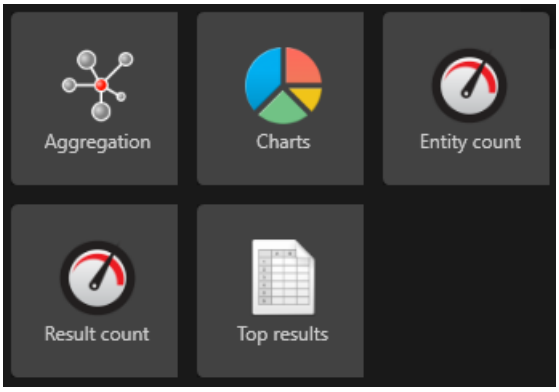
Widgets are the building blocks of dashboards. Security Center comes with various dashboard widgets in the following categories:

- **General:**



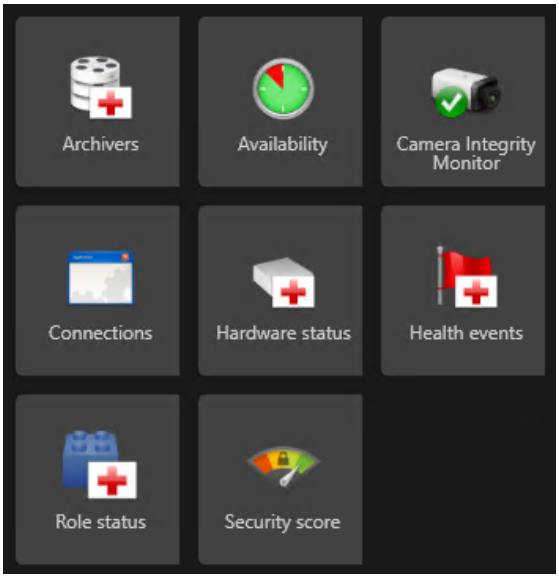
Embed images, text, and web pages in your dashboard, or display Security Center tiles.

- **Report:**



Provide a snapshot of key information in your Security Center system. Reports can be configured to refresh automatically on an interval.

- **Health:**



Monitor system health and performance metrics that can be configured to refresh automatically on an interval.

Security Center provides a framework to create custom widgets through the Security Center *SDK*. If you need help developing custom widgets, 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 https://www.genetec.com/about-us/contact-us.

Privilege requirements

The *Dashboard* task is controlled by privileges. To work with dashboards, users must have the following privileges:

Task	Minimum required privileges
Viewing dashboards	• *View dashboards* • *View public tasks*
Modifying dashboards	• *Modify dashboards* • *Manage private tasks* or *Modify public tasks*
Creating dashboards	• *Modify dashboards* • *Manage private tasks* or *Add public tasks*
Deleting dashboards[1]	*Manage private tasks* or *Delete public tasks*

[1] Dashboards are removed by deleting the associated task.

Specific widgets might require privileges of their own.

Related Topics

Standard dashboard widgets on page 142
Creating a dashboard on page 145

Standard dashboard widgets

A collection of standard widgets is included with Security Center.

The following widgets are available:

Name	Widget icon	Description	Required privileges
Alarm count		Counts the number of alarms that are active, under investigation, or that require acknowledgment. You can configure the widget to change color based on the alarm count.	None
Image		Displays static images in the following formats: • *.jpg* • *.jpeg* • *.gif* • *.png* • *.bmp*	None
Monitoring		Displays the live report of events or alarms selected for monitoring. You can switch between monitoring events and alarms if the **Allow display mode toggle** option is selected. The same commands available in the *Monitoring* task when alarm monitoring is enabled are available in the widget.	None
Text		Displays text.	None
Tile		Displays any entity that can be shown in a Security Center tile.[1]	None[2]
Web page		Displays web pages.	*View web pages*
Aggregation		Displays a chart using an aggregation function (Count, Average, Maximum, and so on) applied to one or many *record types*, and optionally grouped by a specific property.	None[3]
Charts		Displays a selected report visually.[4]	*View charts*[5]

Name	Widget icon	Description	Required privileges
Entity count		Counts the number of entities of the selected type.	None
Result count		Counts the number of results in a selected report.[2]	None[5]
Top results		Displays the top results from a selected report.[4]	None[5]
Archivers		Displays Archiver role statistics.	*Archiver statistics*
Availability		Displays system availability statistics.	*Health history*
Camera Integrity Monitor		Displays the tampering status for cameras configured for camera integrity monitoring, and can trigger an update for their associated thumbnail and data model.	*Reset Camera Integrity Monitor*
Connections		Counts the number and type of users connected to the system.	None
Hardware status		Displays the hardware status of selected devices.	None
Health events		Displays system health events.	*Health history*
Role status		Displays the status of selected roles.	*View role properties*
Security score		Displays your system security score.[6]	*View security widget*

[1] You can also add an entity to your dashboard from the *Monitoring* task by right-clicking the associated tile and selecting **Add to dashboard**.

[2] Specific entities might require their own privileges.

[3] Requires a specific privilege for each record type you want to report on.

[4] Only reports saved as public tasks are supported. You can also add a report to your dashboard by selecting **Add to dashboard** in the associated reporting task in Security Desk.

[5] Specific reports might require their own privileges.

[6] For more information, see "How the Security score widget works" in the *Security Center Administrator Guide*.

Related Topics

About dashboards on page 139
Creating a dashboard on page 145

Creating a dashboard

You can create custom dashboards and save them as public tasks or private tasks in Security Desk.

Before you begin

To create a dashboard, users must have the following privileges:

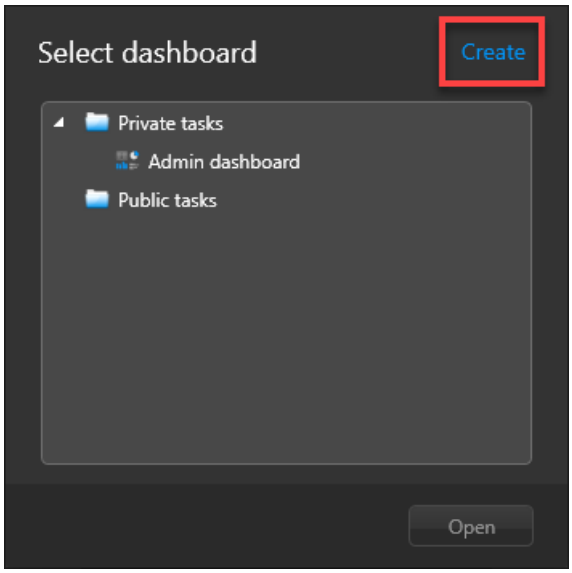
- *Modify dashboards*
- *Manage private tasks* or *Add public tasks*

Specific widgets might require privileges of their own. For more information, refer to Standard dashboard widgets on page 142.

To create a dashboard:

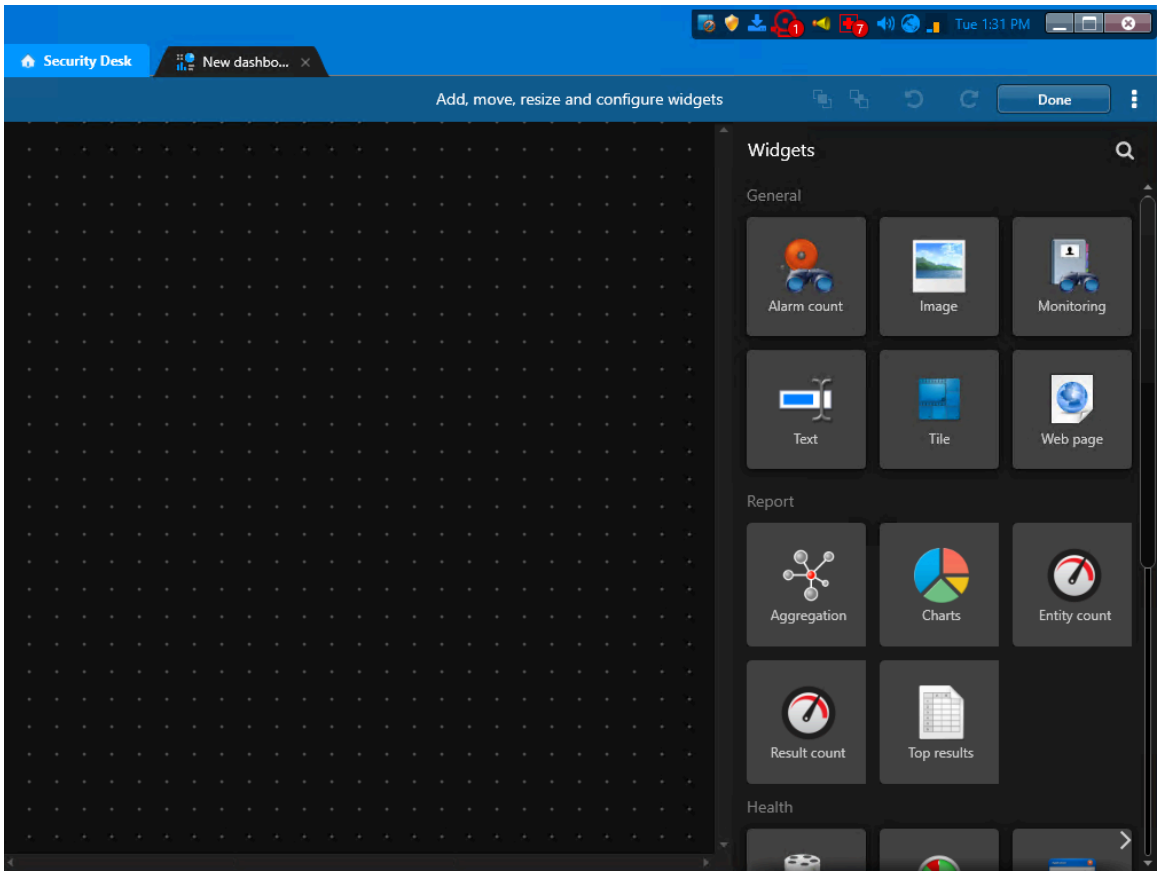
1 In Security Desk, open the *Dashboards* task.

2 On the *Select dashboard* screen, click **Create**.



3 Provide a name for your new dashboard and save it as a private task or a public task.
An empty dashboard is created.

4 Click **Add widgets**.
The dashboard canvas opens with the available widgets shown in the *Widgets* palette.



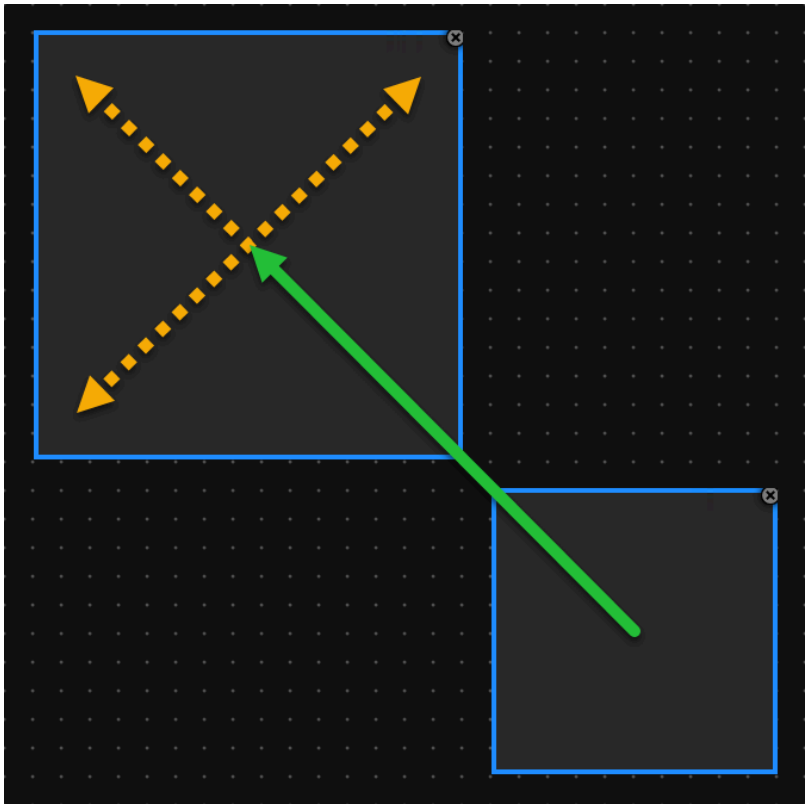
5 Populate the dashboard by dragging and dropping widgets from the palette to the canvas.

TIP: You can perform a search for the widget you are looking for.

By default, all changes to the dashboard layout and widget configuration are saved automatically. To disable this behavior, deselect **auto-save** in the dashboard menu.

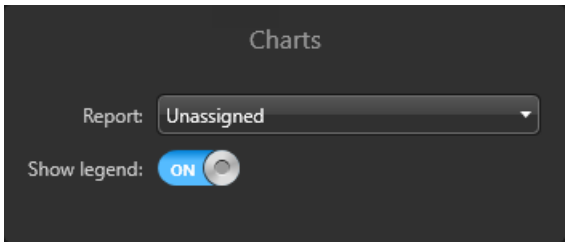
For each widget, you can do the following:

- Move the widget into position and resize it as needed.



The widget frame will snap to the grid lines on the canvas. Widgets can overlap. You can place a widget in front of others ( ) or behind ( ).

- In the widget-specific options, set what the widget displays.



- In the general options, configure the look and behavior of the widget. These options include the widget title, background color, and whether or not the data refreshes automatically.

Counts, charts, reports, and web pages must be refreshed to show the latest information. Dashboard widgets can be refreshed manually or on an interval. An auto refresh interval can be specified per widget, or once for the entire dashboard in the dashboard *Options*.

6 After populating your dashboard with widgets, click **Done**.

Your dashboard layout is ready for use. Public dashboards are available to all users who have the *View dashboards* and *View public tasks* privileges. Private dashboards are only available to the current user.

After you finish

To access your dashboard, you can select it in the *Dashboards* task, or open it directly with the associated public task or private task.

Related Topics

About dashboards on page 139
Standard dashboard widgets on page 142

9

Maps

This section includes the following topics:

How to work with maps in Security Center

To enhance your situational awareness and system security, you can use maps in Security Center to view and navigate your facilities in real time, and manage your 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.

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

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

Related Topics

Overview of the Monitoring task on page 575
Overview of the Maps task on page 167

Basic map commands

In Security Desk, you can interact with your maps and security devices represented on your maps using standard commands, such as clicking and dragging to move the map, or clicking on the map objects. The shape of the mouse cursor indicates what action you can take.

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.

Overlaid command buttons

You can perform the most common map commands using the command buttons overlaid on the top-right corner of the map.

Button	Name	Alternative inputs
	**Zoom in**	You can also use the following: • Roll the mouse wheel • Double-click • Press the '+' key
	Zoom out	You can also use the following: • Roll the mouse wheel • Double-right-click • Press the '-' key
	Select preset	Click the button, then select a *map preset* to reposition the map. You can also use Ctrl+preset number.
	**Select map**	(Security Desk canvas only) Click the button, then select an area with a map () to display the associated map. Hold the Ctrl key when you select the map to preserve the current *map view*. **NOTE:** The button icon matches the icon of the selected area.
	**Smart click**	Click to enable the *Smart click* mode. The button turns blue and the cursor changes to a cross. When *Smart click* is on, click anywhere on the map to cause all PTZ cameras that support *position feedback* to turn to that location if their field of view is not obstructed by walls. To zoom your PTZ cameras, draw a rectangle around the area to zoom in to. You can also hold the Shift key while clicking to achieve the same result as *Smart click*. If you are in the *Monitoring* task, all cameras whose field of view includes the location you clicked are displayed in the remaining tiles in the canvas.

Button	Name	Alternative inputs
	Send selection to tiles	Click ..., then click **Send selection to tiles** ( ) to enable the multi-select functionality. You can also use Alt+Click. The cursor changes to a cross. Click and drag to select multiple map objects in a rectangle. When you release the mouse, each map object within the rectangle is displayed in a tile in the *Monitoring* task.
	Area zoom	Click ..., then click **Area zoom** ( ) to enable the area zoom functionality. You can also use Ctrl+Click. The cursor changes to a cross. Click and drag to draw a rectangle to zoom into the selected area.

Floor controls

When maps are configured as floors of a building, you can quickly navigate the building using the overlaid controls (bottom right).

All floors in the same building are linked. You can navigate between floor maps by pressing the button for the floor you want to see. Floors are labeled with a configurable abbreviation of the area name.

NOTE: If **Display alarms from linked maps** is enabled in the map options, the number of active alarms on other floors is shown on the floor controls.

When the same area is included in multiple buildings, like a shared parking lot, the floor controls can be used to navigate between buildings by following the arrow.

Navigation between floors uses the same view by default. Press and hold the Ctrl key while changing floors to restore the default view.

Maps toolbar and keyboard commands

Other map commands are available from the Maps toolbar or as keyboard commands. Specific commands related to each type of map objects are described in Supported map objects on page 157.

Result	Action
Move the map	Drag.
Zoom in on a section of the map	Hold the Ctrl key and draw a rectangle around the section of the map you want to zoom in on.
Span the map across all monitors	(Maps task only) In the Maps toolbar, click **Settings** > **Span map across all monitors**.
Switch to your default map	(*Maps* task only) In the Maps toolbar, click **Default map**.

Result	Action
Switch to a different map	Do one of the following: • Click a map thumbnail. • Click a map link, which is typically a colored semi-transparent polygon. • Click a floor in the floor controls. • (*Maps* task only) In the Maps toolbar, click **Select map** or click a map name. • (Security Desk canvas only) Click the **Select map** button overlaid on the current map. To synchronize map positions, hold the Ctrl key while switching maps. The new map opens at the same GPS location or map view. Map positions are automatically synchronized between floors.
Show information about any map object	Do one of the following: • For map objects representing Security Center entities, point to the map object, or press and hold the Ctrl+Alt keys to display the names of all map objects at the same time. • For KML objects and Esri objects, click the map object to show all available information in a text bubble. If objects overlap, a list of the layers is displayed so that you can select the layer that contains the object you want to see.
Find an entity on a map	Do one of the following: • In the *Maps* task: In the Maps toolbar, click **Search** and enter an entity name. • In the *Monitoring* task: Right-click an entity displayed in a tile and click **Locate me**. If the entity is displayed on more than one map, the map icons are displayed in a pop-up, and you must select which map to view the entity on.
Search for records correlated by location and time	(*Maps* task only) In the Maps toolbar, click **Record search**.
Show or hide information on a map	Do one of the following: • From the *Maps* task: In the Maps toolbar, click **Layers**. • From the *Monitoring* task: Right-click anywhere on your map and click **Layers**. In the dialog box that opens, select the layers you want to show on your map, and then click **OK**.
Select a map object	By default, click the map object. This only applies to Security Center entities. When applicable, this action also: • Displays the related entity in a tile bubble. • Displays the related widgets in the *Controls* pane.

Result	Action
Show the contextual menu of a map object	Right-click the map object. This only applies to Security Center entities.
Configure an entity	Right-click the map object, and click **Configure entity** to open the configuration page of the entity it represents. **NOTE:** You need the privileges to run Config Tool and to view entity configurations.
Display map object in the *Monitoring* task	By default, double-click the map object. This only applies to Security Center entities.
View multiple map objects in the *Monitoring* task	By default, hold the Alt key and draw a rectangle around the map objects to display in the *Monitoring* task. This only applies to Security Center entities.

Showing or hiding information on maps

You can choose the amount of information you want to show on your map by selecting the layers to display.

What you should know

A map is composed of a static background image with various information layered on top, called *map objects*. You can control the amount of information you see on your map by showing or hiding any of these layers (map objects).

To show or hide information on map:

1 Do one of the following:

- From the *Maps* task, in the Maps toolbar, click **Layers**.
- From the *Monitoring* task, right-click anywhere on your map and click **Layers**.

2 In the dialog box that opens, select the layers you want to show on your map.

3 Click **OK**.

NOTE: The option to cancel your changes is not available in this dialog box.

Differences between Monitoring and Maps tasks

To work with maps in Security Desk, you can use either the *Maps* task which is dedicated to working with maps, or the generic *Monitoring* task. In both tasks, the behavior of the maps are mostly the same, but there are differences with the workspace layout.

The *Monitoring* task is better suited when Security Desk is only controlling one monitor. The *Maps* task is better suited when Security Desk is controlling multiple monitors.

Map feature	Monitoring task	Maps task
When to use	Only one monitor is controlled by your Security Desk workstation, and you need to see map and video side by side at all times.	Multiple monitors are controlled by your Security Desk workstation.
Map display area	Maps are displayed in tiles.	One map covers the entire workspace.
Multiple map display	Each tile can display a different map.	Displays one map at a time.
Span the map across all monitors	Not supported.	In the Maps toolbar, click **Settings** > **Span map across all monitors**.
Double-click an entity on the map	Displays the entity in a free tile in the canvas. When all tiles are filled, replaces the oldest displayed entity. May replace the map itself if it happens to be the oldest entity.	Displays the entity in a Monitoring task if one is already open. If not, opens one.
Switch to a different map	Drag a different map (area) from the area view to the tile showing the current map.	Click a different map in the task toolbar.
Find entities on maps	Right-click an entity displayed in a tile and click **Locate me**. If the entity is displayed on more than one map, the map icons are displayed in a pop-up, and you must select which map to view the entity on.	In the Maps toolbar, click **Search** and enter an entity name..
Switch to your default map	Not supported.	In the Maps toolbar, click **Default map**..
Switch to a favorite map	Not supported.	Click **Select map** in the task toolbar, and click a favorite.
Show alarm list	Type **F9** and click **Alarms**.	Click **Alarms** in the task toolbar.
Show event list	Type **F9** and click **Events**.	Click **Past events** in the task toolbar.
Show or hide controls	Type **F7** or click **Hide controls**.	Type **F7** or click **Settings > Show controls** in the task toolbar.

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 map 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 on 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	•  - 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 (+). •  - If the cluster includes active alarms, a red badge shows the number of active alarms in that cluster.	• 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.

Map object	Default appearance on maps	Usage and specific actions
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, and shunt the reader by using the *Door* widget or by right-clicking the door on the map.
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 additional 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 will display 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.

Map object	Default appearance on maps	Usage and specific actions

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.

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 on 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	•  - 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*. •  - 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.

Adding records on maps

If your software license supports *Record caching*, you can add records to preconfigured *record types*, such as *Accidents*, *Arrests*, *Emergency calls*, and so on, by right-clicking on the map. If the selected record type has georeferencing data, the record you add is automatically tagged with the location you clicked.

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.

The records you add can be used to enhance you and your peers' awareness and response, and provide contextual information on maps. You can also visualize this data on your dashboards.

To add a record on a map:

1 Open the *Maps* task.

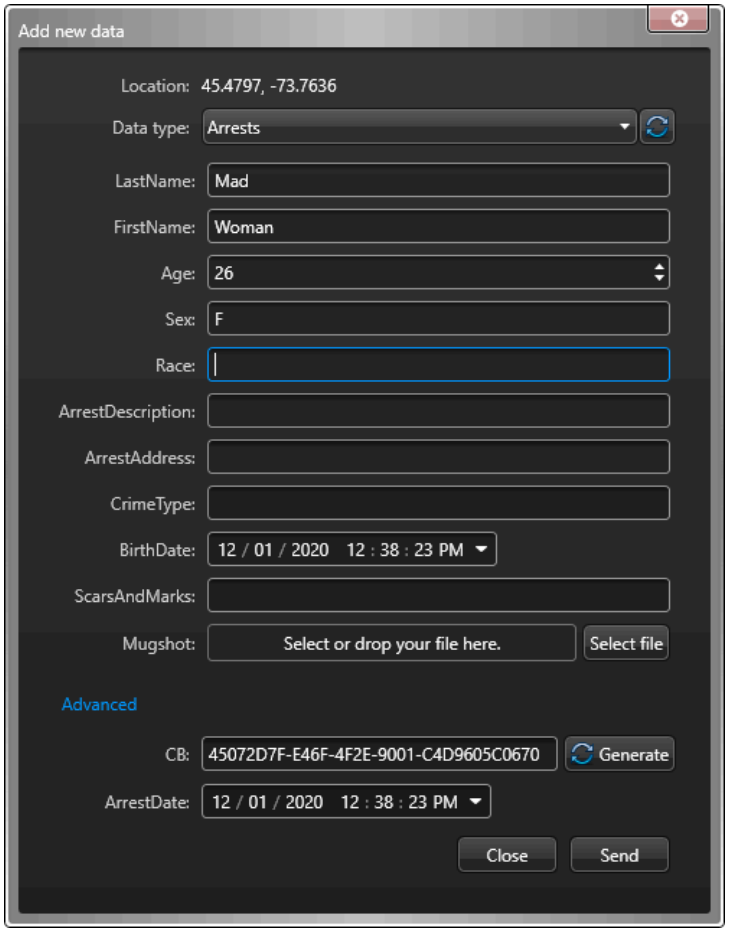
2 Right-click on the map where you want to tag your record with and select **Add new data on map**.

The *Add new data* dialog box opens, and the location you clicked is indicated.

3 If you have more than one record type defined in your system, select the type you want to add the record to.

NOTE: If the selected record type is not georeferenced, you can still add records to it, but you cannot view your record on the map.

4 Enter the rest of the information required by your record type.



5 (Optional) Manually enter the values for the ID and timestamp of the record.

The record ID and timestamp correspond to the fields assigned respectively to the *ID* and *Timestamp* functions in the record type definition. By default, the system generates a random unique value for the ID and uses the current time as the timestamp.

You can click **Advanced** and enter the ID and timestamp values manually. For more information, see "Defining the record format" in the *Security Center Administrator Guide*.

6 Click **Send**.

The new record is added.

If the record type is configured to raise an event when data is added, a new map object for the record type is displayed on the map where you clicked. If not, the only way to view the record you added is to use the *Records* investigation task.

Related Topics

Using correlation to derive useful intelligence on page 109

Searching maps using correlated records

You can search for records correlated by location and time from the *Maps* task.

Before you begin

Make sure that your system administrator has granted you the necessary privileges to use the record types you need.

To search for correlated records on a map:

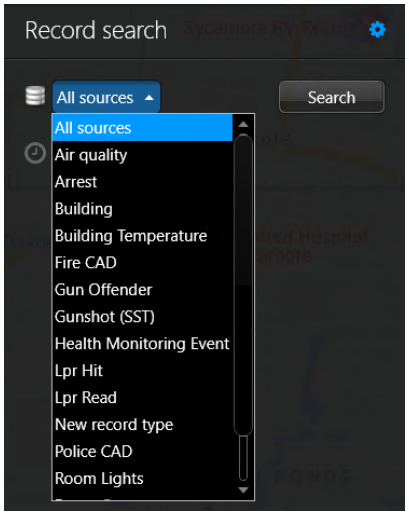
1 Open the *Maps* task.

2 Position the map in the required map view.

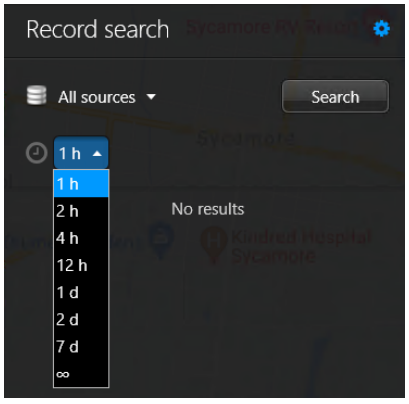
- Click and drag to reposition the map.
- Use the mouse wheel or the overlayed ➕ and ➖ buttons to zoom in and out.

3 Click the **Record search** button.

4 Select the record type source you want to search for.



5 To correlate your record types by timestamp, select the desired time frame.



6 Click **Search**.

The query results are displayed in the search pane.

7 Double-click a result to zoom in on the map location.

8 Click a map object of a record type to open the information bubble with the details of the record.
9 To search a new area with the same filters, change the map view position and click **Search this area**.
10 Deselect the **Record search**  button to close the search pane and clear the map.

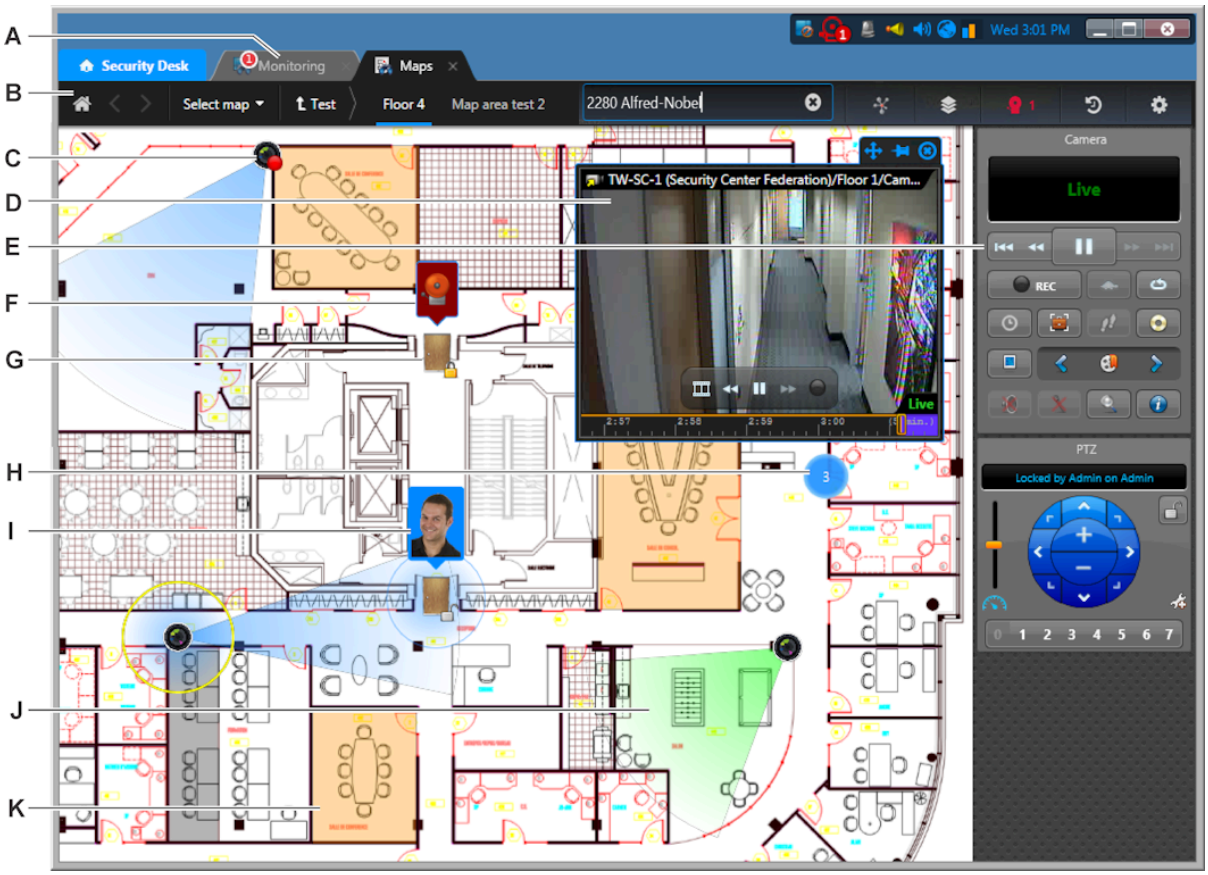
Related Topics

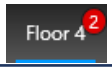
Using correlation to derive useful intelligence on page 109

Overview of the Maps task

You can use the *Maps* task to monitor *events* and *alarms* in real time, manage entities in your security system, and dynamically navigate your facilities.

The following figure shows a *Maps* task in an access control and video monitoring system. Security Center entities are represented by clickable icons and colored areas on the map, called *map objects*.



A	By default, double-click any map object that can be displayed in a tile to open it in the *Monitoring* task. Double-click behavior can be customized in the map options.
B	Switch to different maps and configure your map display options using the buttons in the Maps toolbar on page 168. If **Display alarms from linked maps** is enabled in the map options, the number of active alarms on a linked map is shown next to the map name. 
C	Fixed camera objects can include a field of view (FOV) indicator. The object can also be configured to show the recording state ( ) and *Motion on* events (with green ripple effect) in real time.
D	Click a map object, a camera in this example, to display it in a tile bubble. You can also hold Ctrl and click to open multiple tile bubbles. When you point to the tile bubble, the corresponding map object is circled in yellow. At the top of the tile bubble, you can click **Move** ( ) to move the bubble, **Pin on screen** ( ) to pin the bubble on the map, or **Close** ( ) to hide the bubble.

E	Widgets corresponding to the selected map object (a camera in this example) are displayed in the *Controls* pane. To hide the controls, click **Settings** > **Show controls** in the Maps toolbar.
F	A map object linked to an active alarm is flagged with an alarm notification bubble that has the same color as the alarm. Point to the bubble to show more details. Click the notification bubble to replace it with a tile bubble.
G	Doors are represented on maps with an icon that indicates their current state: *open* or *closed*, and *locked* or *unlocked*.
H	Three or more map objects, placed too closely to be visible at a given zoom level, are represented by a blue cluster bubble. Click to zoom in on the map to view the individual map objects.
I	Events are displayed in event notification bubbles. The color of the bubble matches the color assigned to the event. Point to the bubble to show more details. Click the notification bubble to replace it with a tile bubble.
J	PTZ camera objects can include an FOV indicator. When enabled, click and drag the FOV to pan and tilt. Drag the mouse cursor closer to the camera icon to tilt the camera down, or further from the camera icon to tilt it up. The object can also be configured to show the recording state ( ) and *Motion on* events (with green ripple effect) in real time.
K	Areas are represented on maps by colored polygons. Click the polygon to switch to the map linked to the area.
L	If mobile tracking is enabled and you have the *View mobile users* privilege, mobile users that share their location are automatically displayed on georeferenced maps with their photo.

Related Topics

Customizing map behavior on page 171

Maps toolbar

To display different maps and configure your map display options, you can use the toolbar in the *Maps* task.

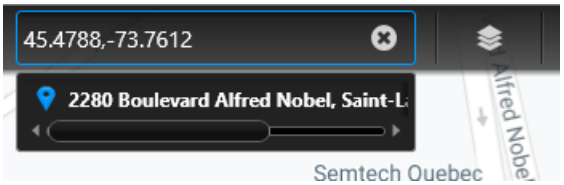
The *Maps* toolbar is divided in two parts. On the left, you have the map navigation commands. Click a map name to switch to the default view of that map. To preserve the currrent *map view* when you switch, hold Ctrl when you click the map name.

On the right, you have the display option commands:

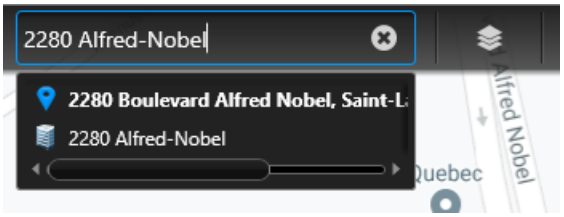
- **Default map:** Switches to the default map defined for the whole system.
- **Select map:** Shows your list of favorites and the map hierarchy. Listed beside this command are the siblings of the current map.
- **Search:** Searches for maps, map objects, and features on the map.

- To search for a map object or any point of interest, enter a name.

  Example: `Building A - Cam 2`.
- To search for a GPS location, enter the latitude and the longitude separated by a comma.
  Example: `45.4788,-73.7612`.
  If **Geocoding** is enabled on one of your map providers, the corresponding street address is displayed.

- To search for a street address, enter a full or partial address.
  Example: `2280 Boulveard Alfred-Nobel, Montreal`.
  This feature works only if **Geocoding** is enabled on one of your map providers.

  The current map view is used in the geocoding query for more precise results. For exemple, if you are currently viewing a map of Montreal and searching for "Alfred-Nobel", the address in Montreal is returned instead of all the "Alfred-Nobel" that exist in the world.

If your search returns more than one result, click on the one you want to locate on the map.

- **Record search:** Search on map for records correlated by location and time.
- **Layers:** Show or hide information on the map
- **Alarms:** Lists all active alarms in a floating window. The icon turns red when there are active alarms in the system.
  - Right-click an alarm in the list to access the alarm contextual menu.
  - Double-click an alarm to switch to a map where the alarm is displayed.
  - Click to change the sorting order of the alarms or the position of the window.
  - Click **Trigger an alarm** to show the list of alarms you can trigger manually.
  - Click **Force ack all** to forcibly acknowledge all alarms in the system.
- **Past events:** Lists all past events in a floating window.
  - Right-click an event in the list to access the event contextual menu.
  - Double-click an event to switch to the map showing the source of the event.
  - Click to change the sorting order of the events or the position of the window.
  - Click **Clear** to clear the event list.
- **Settings:** Opens the **Settings** menu.
  - **Show controls:** Show or hide the controls. Same as typing **F7**.
  - **Span map across all monitors:** Use all monitors attached to Security Desk to display the map.
  - **Manage:** Configure favorites and default maps.

    - **Add map to favorites:** Add the current map to your list of favorites.
    - **Edit map:** Open the *Map designer* task in Config Tool to edit the current map. You need the *Map designer* privilege to use this command.
    - **Set map as default:** Set the current map as your default map, the first map that's loaded when you open the Maps task.
    - **Set map as global default:** (Administrators only) Set the current map as the global default map for all users.
- **Options:** Opens the *Map options*.
- **Help:** View tips to help you get started using maps.

Customizing map behavior

You can customize map behavior from the *Options* dialog box.

What you should know

Map options in Security Desk are associated with the current Windows user.

To customize map behavior:

1 Open *Map options*.
- From the home page, click **Options** > **Map**.
- From the *Maps* task, click **Settings** > **Options** > **Map**.

2 If required, change one or more of the following options:
- In the *Panel position* section, select the default position of map panels. Panels can be floating, docked to the left side of the map, or docked to the right side of the map.
  - **Alarms:** Default position of the *Alarm* panel.
  - **Events:** Default position of the *Events* panel.
  - **Map layers:** Default position of the *Layers* panel.
- In the *Map items* section, select the action to take when interacting with map entities.
  - **On single-click:** Action to take when clicking a map entity.
    - **Display tile in a pop-up window:** Default. Opens the entity in a pop-up window.
    - **Display in a Monitoring task:** Opens the entity in a Monitoring task on a local screen. The entity will occupy an empty tile, if available, or replace the content of an existing tile.
    - **Display on remote monitor:** Opens the entity in a Monitoring task on any screen connected to the same Directory. You must specify the logical ID of the monitor.
    - **Do nothing:** Disables the single-click action.
  - **On double-click:** Action to take when double-clicking a map entity.
    - **Display in a Monitoring task:** Opens the entity in a Monitoring task on a local screen. The entity will occupy an empty tile, if available, or replace the content of an existing tile.
    - **Display on remote monitor:** Opens the entity in a Monitoring task on any screen connected to the same Directory. You must specify the logical ID of the monitor.
    - **Do nothing:** Disables the double-click action.
  - **On lasso:** Action to take when selecting map entities with the lasso (Alt+click and drag).
    - **Display in a Monitoring task:** Opens the selected entities in a Monitoring task on a local screen. The entities will occupy empty tiles, if available, or replace the content of existing tiles.
    - **Display on remote monitor:** Opens the selected entities in a Monitoring task on any screen connected to the same Directory. You must specify the logical ID of the monitor.

    NOTE: To display the logical ID of a monitor in the notification tray:

    a. In Security Desk on the machine connected to the monitor, click **Options** > **Visual**.
    b. In the *In tray* section, set **Monitor ID** to **Show**.
- In the *Alarms* section, select **Display alarms from linked maps** to show the number of active alarms on a linked map on the *Maps* task toolbar, floor controls, and links to that map.
- In the *Mobile* section, select **Hide mobile offline users** to avoid showing mobile users who are offline on maps.

3 Click **Save**.

4 If *Basic record fusion* is enabled on your system, click **Performance** and configure how records are loaded on maps.

Under the *Record display on maps* section, configure the following:

- **Display active records for the past:** Records that are recently upated are displayed as a pin on maps. Use this setting to tell the system how far to look back. The default is four hours.
- **Maximum number of records:** The maximum number of records to display on maps. The default is 1000.

5 Click **Save**.

Related Topics

Overview of the Maps task on page 167

10

Keyboard shortcuts

This section includes the following topics:

Default keyboard shortcuts

This table lists the default keyboard shortcuts 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		
Auto lock	Lock the workstation.	Ctrl+Shift+L
Controls	Show/hide the controls.	F7
Cycle through canvas only, report only, and both	Show only the canvas, only the report pane, or both.	F9
Exit application	Close the application.	Alt+F4
Full screen	Toggle between displaying the application in windows and full screen mode.	F11
Go to next content in cycle	When you are viewing a packed entity in a tile, switch to the next attached entity, or the next camera in the sequence.	Ctrl+Right arrow
Go to next content in cycle (all tiles)	When you are viewing a packed entity in a tile, switch to the next attached entity, or the next camera in the sequence.	Ctrl+Shift+Right arrow
Go to next page	Switch to the next task tab.	Ctrl+Tab
Go to previous content in cycle	When you are viewing a packed entity in a tile, switch to the previous attached entity, or the next camera in the sequence.	Ctrl+Left arrow
Go to previous content in cycle (all tiles)	When you are viewing a packed entity in a tile, switch to the previous attached entity, or the next camera in the sequence.	Ctrl+Shift+Left arrow
Go to previous page	Switch to the previous task tab.	Ctrl+Shift+Tab
Help	Open the online help.	F1
Home page	Go to the home page.	Ctrl+Grave accent (`)
Hot action x	Execute hot actions 1-10, once you've configured them.	Ctrl+(F1-F10)
Options	Open the *Options* dialog box.	Ctrl+O
Select columns	Select which columns to show/hide in the report pane.	Ctrl+Shift+C
Selector	Show/hide the selector pane.	F6

Command	Description	Shortcut
Start cycling	Automatically switch between all loaded entities in Security Desk. By default, a 4 second dwell time for each entity is used.	Ctrl+Up arrow
Start cycling (all)	Automatically switch between all loaded entities in Security Desk. By default, a 4 second dwell time for each entity is used.	Ctrl+Shift+Up arrow
Tiles only	Show only the display tiles and task list. The selector pane, event pane, and controls are hidden. This is mainly used for the *Monitoring* task.	F10
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.
Alarm commands		
Acknowledge (Default)	Acknowledge the selected alarm in the *Alarm report* task.	Spacebar
Acknowledge all (Default)	Acknowledge all alarms in the *Alarm report* task.	Ctrl+Shift+Spacebar
Show alarm page	Open the *Alarm monitoring* task.	Ctrl+A
Snooze alarm (all)	Put all alarms to sleep for 30 seconds. When an alarm is snoozing, it is temporarily removed from the canvas.	Alt+Ctrl+Shift+S
Snooze the alarm	Put the alarm to sleep for 30 seconds. When the alarm is snoozing, it is temporarily removed from the canvas.	S
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
Export video	Export video from the selected tile.	Ctrl+E
Export video from all tiles	Export video from all the tile in the canvas.	Ctrl+Shift+E
Forward	Forward the video playback.	Period (.)
Forward all	Forward the video playback of all cameras that are displayed in the canvas.	Ctrl+Shift+Period (.)

Command	Description	Shortcut
Instant replay	View an instant video replay in the selected tile.	I
Jump backward	Jump backwards in the recorded video according to the seek time specified in the *Options* dialog box.	Ctrl+Shift+N
Jump backward all	Jump backwards in the recorded video according to the seek time specified in the *Options* dialog box, for all cameras that are displayed in the canvas.	Alt+Ctrl+Shift+N
Jump forward	Jump forward in the recorded video according to the seek time specified in the *Options* dialog box.	Ctrl+Shift+M
Jump forward all	Jump forward in the recorded video according to the seek time specified in the *Options* dialog box, for all cameras that are displayed in the canvas.	Alt+Ctrl+Shift+M
Next frame	When your playback video is paused, go to the next video frame.	M
Next frame all	When your playback video is paused, go to the next video frame. This applies to all cameras that are displayed in the canvas.	Ctrl+Shift+J
Play/Pause	Pause or play the video recording.	G
Play/Pause all	Pause or play the video recording for all cameras that are displayed in the canvas.	Ctrl+Shift+G
Previous frame	When your playback video is paused, go to the previous video frame.	N
Previous frame all	When your playback video is paused, go to the previous video frame. This applies to all cameras that are displayed in the canvas.	Ctrl+Shift+H
Rewind	Rewind the video playback.	Comma (,)
Rewind all	Rewind the video playback for all cameras that are displayed in the canvas.	Ctrl+Shift+Comma (,)
Show diagnostic timeline	Show the timeline of the video stream diagnosis.	Ctrl+Shift+T
Show video stream diagnosis	Show/hide the video stream diagnosis, where you can troubleshoot your video stream issues.	Ctrl+Shift+D
Show video stream statistics on the tile	Show/hide the statistics summary of the video in the selected tile.	Ctrl+Shift+A
Show video stream status	Show/hide the status summary of the video stream connectins and redirections in the selected tile.	Ctrl+Shift+R
Slow motion	Switch the playback to slow motion.	Shift+En dash (-)
Slow motion (all)	Switch the playback to slow motion for all cameras that are displayed in the canvas.	Ctrl+Shift+En dash (-)

Command	Description	Shortcut
Switch to live	Switch to live video.	L
Switch to live (all)	Switch to live video for all cameras that are displayed in the canvas.	Ctrl+Shift+V
Switch to playback	Switch to playback video.	P
Toggle recording	Start/stop recording video for the selected tile.	R
Toggle recording (all)	Start/stop recording video for all cameras that are displayed in the canvas.	Alt+Ctrl+Shift+R
Visual tracking	Enable/disable visual tracking for the selected tile.	Alt+F
Visual tracking (all)	Enable/disable visual tracking for all cameras that are displayed in the canvas.	Ctrl+Shift+F
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
Door commands		
Unlock	Unlock the selected door.	U
Unlock (all)	Unlock all the doors that are displayed in the canvas.	Ctrl+Shift+U
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 home page.	Ctrl+N
Tile commands		
Back	Switch to the previous tile content.	Alt+Left arrow

Command	Description	Shortcut
Change tile pattern	Change the tile pattern in the canvas.	Ctrl+P
Clear	Clear a specific tile in the canvas.	<Tile ID>+Backspace
Clear all	Clear all the tiles in the canvas.	Ctrl+Backspace
Cycle next pattern	Cycle to the next tile pattern.	W
Cycle previous pattern	Cycle to the previous tile pattern.	Q
Display camera sequence	Display a camera sequence in a specific tile.	<Camera sequence ID> +Ctrl+ENTER
Display entity	Display an entity in a specific tile.	<Entity ID>+ENTER
Forward	Switch to the next tile content.	Alt+Right arrow
Home	• **Map mode:** Jump to the home web page associated with the map. • **Tile mode:** Return to the first content you dragged into the tile.	Alt+HOME
Maximize tile	Maximize the selected tile to the whole canvas. Press E again to shrink the tile.	E
Maximize tile fullscreen	Maximize the selected tile to full screen mode. Press Alt +ENTER again to shrink the tile.	Alt+ENTER
Monitor alarms	Enable/disable alarm monitoring for the selected tile. When alarm monitoring is enabled, alarms automatically appear in the tile.	Alt+A
Monitor all alarms	Enable/disable alarm monitoring for all tiles in the canvas. When alarm monitoring is enabled, alarms automatically appear in the tiles.	Alt+Ctrl+Shift+A
Monitor events	Enable/disable event monitoring for the selected tile. When event monitoring is enabled, events automatically appear in the tile.	Alt+T
Pack/unpack	Pack/unpack the area or camera sequence in the selected tile.	Alt+U
Refresh	Refresh the page, or reload the selected tile.	F5
Select next tile	Select the next tile in the canvas.	Y
Select previous tile	Select the previous tile in the canvas.	T
Start task cycling	Automatically switch between all loaded tasks in Security Desk. By default, a 4 second dwell time for each task is used.	Ctrl+Q

Command	Description	Shortcut
Stop task cycling	Stop the task cycling rotation.	ESC
Toggle monitoring (all)	Enable/disable event monitoring for all tiles in the canvas. When event monitoring is enabled, events automatically appear in the tiles.	Alt+Ctrl+Shift+T

Related Topics

Customizing keyboard shortcuts on page 182

Switching tasks using your keyboard

You can open a saved public task, or switch between public tasks on your local workstation using a keyboard shortcut sequence.

Before you begin

You need the logical ID of the public task. To find the logical ID of a task, check in the *System* task in Config Tool.

IMPORTANT: Multiple entities can use the same logical ID. If this is the case, then a camera or analog monitor entity with the same logical ID takes priority over the public task, and is displayed in the canvas instead of switching tasks.

To switch tasks using your keyboard:

- Type the task ID, and then press **ENTER**.
  Example: <50><ENTER>.

Switching tasks on a remote monitor using your keyboard

If you are controlling a video wall or analog monitor, you can open a saved public task, or switch between public tasks on the remote workstation using a keyboard shortcut sequence.

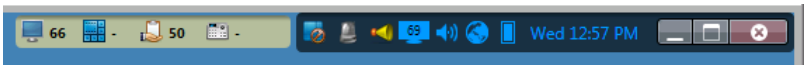
Before you begin

You need the logical ID of the public task. To find the logical ID of a task, check in the *System* task in Config Tool.

IMPORTANT: Multiple entities can use the same logical ID. If this is the case, then a camera or analog monitor entity with the same logical ID takes priority over the public task, and is displayed in the canvas instead of switching tasks.

What you should know

As you type the shortcut, the monitor and task IDs are displayed at the top of your local Security Desk window beside the notification tray. This helps you keep track of what numbers you have entered.



To switch tasks on a remote monitor using your keyboard:

1. Type the remote Security Desk monitor ID, and then press the **PERIOD** (.) key.

   TIP: The Security Desk monitor ID is shown in the notification tray (

). If it is not displayed, you can show the monitor ID icon from the *Options* dialog box.
2. Type the logical ID of the task, and then press **ENTER**.
   Example: <65><PERIOD><50><ENTER>.

Related Topics

Configuring the notification tray on page 94

Displaying cameras using your keyboard

You can display a camera in a tile, or switch cameras on your local workstation using a keyboard shortcut.

What you should know

Tile IDs range from 1-26, depending on the tile pattern you are using. It is easier to select which camera to display when their logical IDs are shown in the area view. You can enable this option from the *Options* dialog box.

To display a camera using your keyboard:

1 Type the tile ID, and then press the **Period** (.) key.

2 Type the camera ID, and then press **Enter**.

Example: <2><Period><15><Enter>.

The camera is displayed in the tile you selected. If you did not select a tile, the camera is displayed in the first free tile.

Related Topics

Customizing how entities are displayed in the canvas on page 27

Displaying cameras on a remote monitor using your keyboard

If you are controlling a video wall or analog monitor, you can display a camera a tile or switch cameras on the remote workstation using a keyboard shortcut.

Before you begin

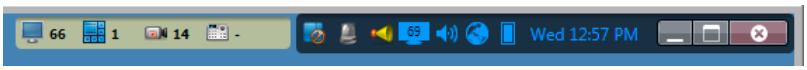
You must know the remote monitor ID. You can find the Security Desk monitor ID in the notification tray (

). If it is not displayed, you can show the monitor ID icon from the *Options* dialog box.

What you should know

Tile IDs range from 1-26, depending on the tile pattern you are using. It is easier to select which camera to display when their logical IDs are shown in the area view. You can enable this option from the *Options* dialog box.

As you type the shortcut, the monitor, tile, and camera IDs are displayed at the top of your local Security Desk window beside the notification tray. This helps you keep track of what numbers you have entered.



To display a camera on a remote monitor using your keyboard:

1 Type the remote Security Desk monitor ID, and then press the **Period** (.) key.

2 Type the tile ID, and then press **Period**.

3 Type the camera ID, and then press **Enter**.

Example: <65><Period><3><Period><12><Enter>.

If you did not select a tile, the camera is displayed in the first free tile.

Related Topics

Configuring the notification tray on page 94

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. Assigning an existing keyboard shortcut to a new command removes it from the previous one. The keyboard shortcut configuration is saved as part of your user profile and applies to Security Desk and Config Tool. If your company is using a standard set of shortcuts, you can also 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 home page, 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 home page, 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 home page, click **Options** > **Keyboard shortcuts**.
   b) Click **Restore default** > **Save**.

Related Topics

Default keyboard shortcuts on page 174

Part II

Introduction to video in Security Desk

This part includes the following chapters:

11

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

12

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.

Viewing cameras in tiles

From any video-related task in Security Desk, you can view cameras in the canvas.

To view a camera in a tile:

1 Do one of the following:
   - Find a camera in the area view, and then double-click or drag it to a tile.
   - Drag a camera from the report pane to a tile.
2 To control the camera, right-click inside the tile and use the tile menu commands, or use the widgets in the *Controls* pane.
3 To clear cameras from the canvas, do one of the following:
   - Right-click on a tile, and then click **Clear** ( ).
   - Select a tile, and then press the Backspace key.
   - (Empties all tiles) At the bottom of the canvas, click **Clear all** ( ).
   - (Empties all tiles) Press Ctrl+Backspace.

Example

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

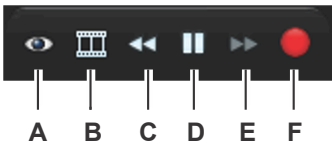
On-tile video controls

When viewing a camera in the canvas, a set of on-tile video controls appear on top of the video image when your mouse pointer hovers over the tile.

You can also hide the on-tile controls from the *Options* dialog box.

The following figures show the on-tile video controls when viewing live and playback video.

Live video:



Playback video:

A	• Go to PTZ preset Only available for PTZ cameras with defined preset positions. Commands the PTZ camera to go to the specified preset position. • Go to digital zoom preset Only available for fixed cameras with defined digital zoom presets. Commands the fixed camera to go to the specified digital zoom preset.
B	Show/hide thumbnail images
C	Rewind (reverse playback)
D	Pause
E	Forward
F	The command depends on whether you are viewing live or playback video: • Live video: Recording state • Playback video: Switch to live video If the camera is also controlled by an Auxiliary Archiver, you can manually start recording on the Auxiliary Archiver by right-clicking the recording state button, selecting **Auxiliary recording**, and then clicking the record button (●) next to the Auxiliary Archiver role name. **NOTE:** Various buttons and button colors can be displayed depending on the task you are performing. For more information, see Camera widget on page 39.

Related Topics

Camera widget on page 39
Customizing how tiles are displayed on page 33

Controlling camera sequences

From any video-related task in Security Desk, you can control camera sequences that are displayed in the canvas.

What you should know

Camera sequences are groups of cameras that are saved as a single entity. They are represented in the area view by a camera icon with a clock overlay ( ). If a camera in a sequence goes offline, you do not see the entity state change to red (offline), but the video stream is not available.

When a camera sequence is displayed in a tile, all the cameras in the sequence are displayed in rotation. If you add additional camera sequences to the canvas, the camera rotation is synchronized.

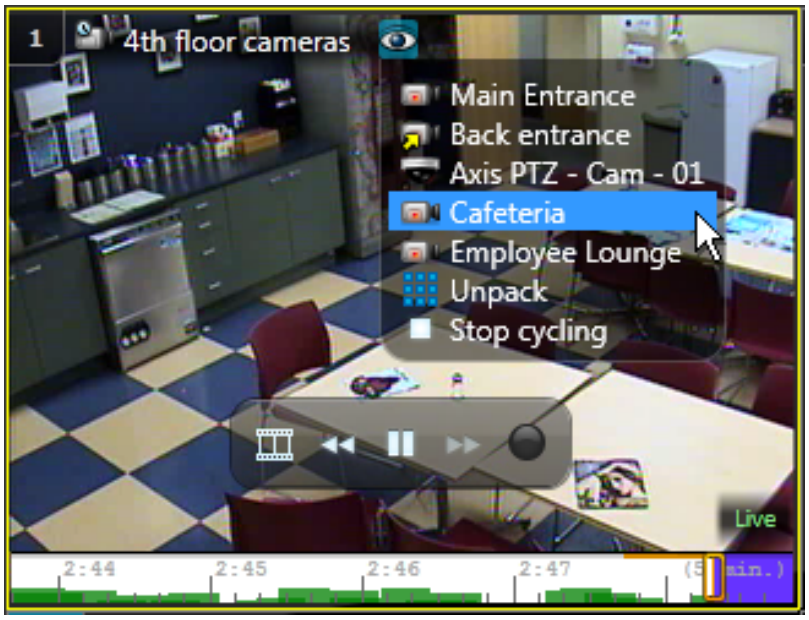
NOTE: If there is a PTZ camera in the sequence and you start controlling the PTZ, the rotation stops. You can click **Start cycling** again once you are done controlling the PTZ.

To control a camera sequence:

1 Display the camera sequence one of the following ways:

- Find the camera sequence in the area view, and then double-click or drag it to a tile.
- Drag the camera sequence from the report pane to a tile.

2 In the tile toolbar, click .



3 From the drop-down list of packed entities, do one of the following:

- To pause the sequence and stay with the current camera, click **Stop cycling**.
- To display all cameras simultaneously, click **Unpack**.
- To force the sequence to display a specific stream, click the individual camera.

Related Topics

Synchronizing video in tiles on page 197

How PTZ cameras are displayed in the canvas

When a PTZ-enabled camera ( ) is displayed in a tile, a zoom slider appears when the mouse pointer hovers over the video, which indicates that the PTZ controls are available.

The following illustration shows the different components of a tile when a PTZ camera is displayed.

A	Direction that the PTZ motor is panning. The longer the arrow, the faster the motor moves. The shorter the arrow, the slower the motor moves.
B	Slider that is used to zoom in and out.
C	Current PTZ motor position and zoom value.

Controlling PTZ cameras

From any video-related task in Security Desk, you can control PTZ cameras that are displayed in the canvas.

What you should know

Some PTZ camera models support the following two additional PTZ controls:

- **Zoom box:** Zoom in on an area by drawing a box on the video image. 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.

To enable these commands, you must configure the PTZ for zoom box and center-on-click in Config Tool. For more information about configuring PTZ motors, see the *Security Center Administrator Guide*).

TIP: It is easier to use the PTZ controls when the on-tile video controls are hidden. You can hide the on-tile video controls from the *Options* dialog box.

You might be locked from controlling the PTZ if a user with a higher user level is currently controlling it. If you have the same user level as another user, the priority is decided on a first come first served basis.

To control a PTZ camera:

1 To display the PTZ camera, double-click or drag it from the area view or report pane into a canvas tile.
2 To expand the tile, double-click on the tile toolbar.
3 Zoom in and out one of the following ways:
   - Move your mouse pointer over the tile, and then move the zoom slider handle up to zoom in or down to zoom out.

     TIP: You can also use your mouse wheel to zoom in and out.
   - If your PTZ camera supports the *Zoom box* feature, draw a box on the video image to zoom in.
4 To pan the PTZ motor, you can either:
   a) Click on the PTZ camera tile.

      A white arrow appears.
   b) Click on the white arrow once to change it to a blue arrow.

      A blue arrow indicates the direction of movement. The longer the arrow, the faster the motor moves. The shorter the arrow, the slower the motor moves.
   c) Click your mouse pointer in the direction you want the PTZ motor to move.

   a) Click once on the blue dot in the middle of the PTZ tile.
   b) Click your mouse pointer in the direction you want the PTZ motor to move.

      Blue arrows are following your movements.
5 To command the PTZ camera to go to a specified preset position, do any of the following:
   - In the video tile, click the (Go to PTZ presets) button, and then select a preset from the list.
   - In the widget, click a numbered quick access button.
   - In the widget, click the (toggle to advanced mode) button, select a preset from the **Presets** list, then click the (Preset) button.
6 If your PTZ camera supports the *Center-on-click* feature, click in the video image to center the image on that point.

Related Topics

Customizing keyboard shortcuts on page 182

Dewarping 360 degree camera lenses

To display a 360 degree fisheye or panoramic camera lens image as a rectangular image in a Security Desk tile, you can dewarp, or flatten it by zooming into the camera image.

Before you begin

Configure the camera lens in Config Tool. For manufacturer-specific information about configuring 360 degree fisheye or panoramic camera lenses, see the *Security Center Video Unit Configuration Guide*.

What you should know

The dewarping time varies, depending on your computer and the dewarped resolution. For example, the dewarping time will be four times longer using a 640x480 resolution instead of a 320x240 resolution.

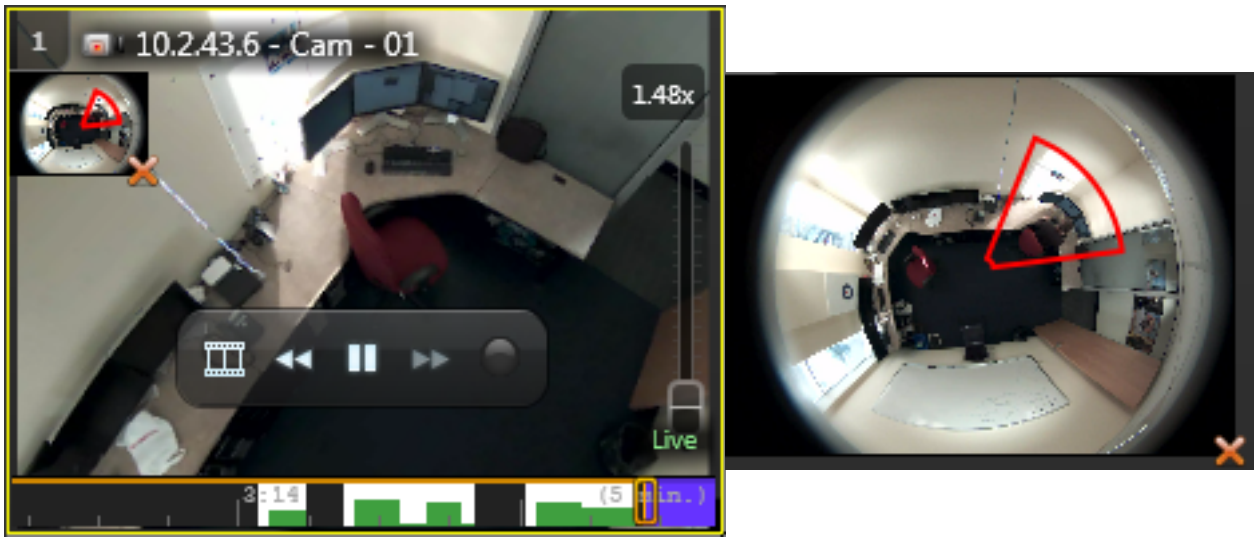
To dewarp a 360 degree camera lens:

1 Display a 360 degree fisheye or panoramic camera in a tile.

2 To zoom in the image, use your mouse wheel, or draw a box on the region you want to zoom to.

NOTE: If you zoom using your mouse wheel, it zooms to the center of the image, not where your cursor is pointing.

3 To navigate the zoomed image, click the image thumbnail at the top-left of the tile.



4 To zoom out, use the mouse wheel, or the zoom slider on the right-side of the tile.

Viewing video on analog monitors

You can view live video on an analog monitor by displaying a camera or camera sequence in an analog monitor entity ( ) in the canvas. You can also receive alarms on an analog monitor if the analog monitor entity is a recipient of those alarms.

Before you begin

Your decoder unit needs to be connected to an analog monitor and it must be added in Security Center as a video decoding unit entity.

What you should know

If your decoder unit supports more than one analog monitor (for example, it is connected to multiple monitors on a video wall), each monitor is added as a separate analog monitor entity in Security Center. You can reproduce the physical layout of your video wall by adding the analog monitor entities to the canvas in a similar tile pattern. For more information about configuring analog monitors in Config Tool, see the *Security Center Administrator Guide*.

Omnicast™ 4.x federated cameras are not supported on analog monitors in Security Center.

To view video on an analog monitor:

1 Double-click or drag the analog monitor entity from the area view to a tile in the canvas.

2 Double-click or drag a supported camera or camera sequence into the tile that is displaying the analog monitor.

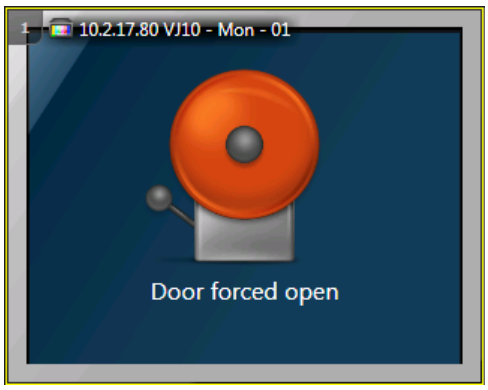
NOTE: Supported cameras must be from the same manufacturer as the video decoding unit and use the same video format.

The live video from the camera is displayed on the physical analog monitor. In Security Desk, only the camera name and camera icon are displayed.

3 To control the displayed cameras, use the widgets in the *Controls* pane (for example, the camera or PTZ widget).

4 To remove the camera from the analog monitor, click in the tile.

If your analog monitor entity is a recipient of an alarm, you can receive alarms on your physical analog monitor. When you receive an alarm, the following is shown in the tile that is displaying the analog monitor.



5 To acknowledge the alarm, click **Acknowledge (Default)** ( ) in the alarm widget.

Related Topics

Camera widget on page 39
PTZ widget on page 47

Synchronizing video in tiles

You can force the live or playback video that is displayed in all the tiles to become synchronized in time.

What you should know

You cannot synchronize the video of entities that are displayed in a tile as part of an event or alarm. The video associated to the event or alarm is meant to show what occurred during that time period.

To synchronize video displayed in tiles:

1 Select a tile.

2 At the bottom of the canvas, click **Synchronize video** ( ).

All the tiles are forced to display live or recorded video. The reference point is the currently selected tile. One of the following happens:

- If selected tile is displaying recorded video, synchronization forces all tiles to display playback video. All the playback videos display the same recording date and time, synchronized to the millisecond.
- If the selected tile is displaying live video, synchronization forces all tiles to display live video. This is useful if you have multiple cameras with overlapping coverage. Forcing playback synchronization produces different perspectives of the same recorded event

3 To turn synchronization off, click **Stop synchronizing video** ( ) at the bottom of the canvas.

Changing the video stream

You can change the video stream of a camera displaying live video in a tile.

Before you begin

If your camera supports multiple video streams, the streams must be enabled and configured in Config Tool before you can select the default video stream. For information about configuring video streams, see the *Security Center Administrator Guide*.

What you should know

Most *video encoders* and *IP cameras* supported by Security Center can generate multiple *streams* per individual camera. This is helpful when you want your live monitoring stream to be configured with a different video quality than the recorded stream. Additional streams can be configured for other needs, such as remote access (low bandwidth) or low resolution versus high resolution streams.

To change the video stream:

1 Right-click on the live video image in a tile.

2 Click **Camera** > **Select live stream**.

3 Select one of the following video streams to view:

- **Live:** Default stream used for viewing live video.
- **Recording:** Stream recorded by the Archiver for future investigation.
- **Remote:** Stream used for viewing live 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.
- **Automatic:** Security Desk uses the *Low resolution* or *High resolution* stream, depending on the size of the tile and the zoom level.

Related Topics

Tile menu commands on page 25

Zooming in and out of video

To get a better view of the finer details of what you are monitoring, you can zoom in on the live or playback video that is displayed in a tile, regardless of whether you are using fixed cameras or PTZ cameras.

What you should know

If the default video stream of the camera is set to *Automatic*, the video stream switches to high resolution when you apply digital zoom.

To zoom in and out of tile content:

1 Select a tile that is displaying live or playback video.

2 Do one of the following:

- Click and drag your mouse to create your desired zooming area (blue rectangle), and then release the mouse button. This method does not work with PTZ cameras.
- Scroll your mouse wheel forwards to zoom in and backwards to zoom out. With PTZ cameras, this method only works once you apply the digital zoom.
- In the camera widget, click **Toggle digital zoom** ( ).
- Right-click in the tile and click **Camera** > **Toggle digital zoom** ( ).

A zoom thumbnail of the full image appears in the upper-left corner of the tile, and the zoom level is displayed in the tile.

3 In the zoom thumbnail, you can do the following:

- Click and drag the red box to reposition the zoom area.
- Click and drag the mouse cursor on the zoomed-in image to reposition the zoom area.
- Use the slider to increase and decrease the zoom level.

4 To stop zooming, click **Toggle digital zoom** ( ) in the camera widget.

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 video stream options on page 278
Video options on page 280

Creating digital zoom presets

When you zoom into a camera image in a tile, you can create digital zoom presets for areas of interest in the image.

What you should know

You can create as many presets as you want. Digital zoom presets are not supported on PTZ cameras.

NOTE: PTZ presets created in the current version might not be available in older versions of Security Desk.

To create a digital zoom preset:

1. Apply a digital zoom method to an image displayed in a tile.
2. In the camera widget, click **Add** ( ).
3. In the *Create preset* dialog box, type a name for the digital zoom preset and then click **Create**.

   A preset is created for the current camera image position. You can now zoom to the preset by selecting it from the **Digital zoom presets** drop-down list in the camera widget.
4. If you move the camera image, you can click **Preset** ( ) to return to the preset position.
5. In the *Digital zoom presets* section, click the drop-down arrow beside **Preset** ( ) for the following additional preset options:
   - **Save:** Save the preset selected in the drop-down list, using the current PTZ position.
   - **Delete:** Delete the preset.
   - **Add preset:** Create a new digital zoom preset.

Related Topics

Zooming in and out of video on page 199

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.

Tracking moving targets

You can follow an individual through your facility in real time or in playback mode after an incident, using the visual tracking feature within a canvas tile.

Before you begin

Configure visual tracking in Config Tool (see the *Security Center Administrator Guide*).

To track a moving target:

1 Select a tile displaying live or playback video.

2 Enable visual tracking for that tile, one of the following ways:

- In the camera widget, click **Enable visual tracking** ( ).
- Right-click in the tile and click **Camera** > **Enable visual tracking** ( ).
- On your keyboard, press `Alt+F`.

3 As the subject moves out of the camera's field of view, click the shape (colored overlay) representing a link to the next camera.

Hover your mouse pointer over the shape to view a preview of the next camera image.

Example

If someone steals something from your facility, you can investigate the theft using a combination of visual tracking and incident reporting.

In the Monitoring task, start incident recording ( ) and enable visual tracking ( ). Play back the video and track the person as they moved around in your facility. When you stop incident recording, the cameras you switched to during the recording are included in the incident report. More importantly, the included video segments have the correct timestamps that correspond with when the person went into those areas. When you review the exported or saved report, the video segments are played back in sequence like a movie.

Adding bookmarks to video sequences

If you see something worth noting, you can add a bookmark to the video you are viewing.

What you should know

- 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.
- If a camera is not currently recording, adding a bookmark forces it to begin recording.
- If you add a bookmark to an exported video clip, the bookmark is only stored in the exported video clip and not the original archived video.

To add a bookmark to a video sequence:

1 In the camera widget, click **Add a bookmark** ( ).

2 (Optional) In the *Add a bookmark* dialog box, type a short text in the **Message** field.

The timestamp of the bookmark is fixed at the **Time** indicated in the dialog box.

3 (Optional) Protect the video sequence containing the bookmark against routine archive cleanup as follows:

NOTE: You can only protect the video sequence if the bookmark is added to a local (non federated) camera.

a) Select the **Protect video from deletion** option.

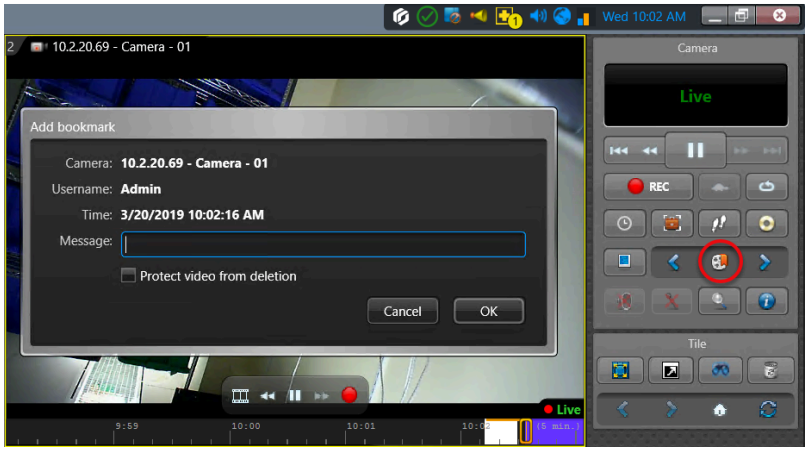
b) In the *Protect archives* dialog box, set the start time and end time of the video sequence to protect, and the duration of the protection.

By default, the protected sequence starts one minute before your bookmark and ends 4 minutes after. The default duration of the protection is 5 days.

c) Click **Protect**.

4 If you did not select the **Protect video from deletion** option, click **OK** to add the bookmark, or click **Cancel** to exit without adding a bookmark.

Leaving the **Message** field blank does not cancel the 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

Overview of the Bookmarks task on page 578

Viewing bookmarked videos

To view a video sequence that was previously bookmarked, you can generate a report of all the stored bookmarks in the *Bookmarks* task.

To view bookmarked video:

1. From the home page, open the *Bookmarks* task.
2. Set up the query filters for the report. Choose from 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.
   - **Message:** Enter any text you want to find in the bookmark. A blank string finds all the bookmarks.
   - **Time range:** The time range for the report.
3. Click **Generate report**.

   The bookmarks appear in the report pane. If your query does not generate a result, a warning message appears.
4. To view the video associated with a bookmark, drag the bookmark from the report pane to a tile in the canvas.

Example

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

Taking snapshots of video

Whether you are viewing live or playback video in a tile, you can save the current video frame as an image file, and then organize and share all files using the Vault tool.

What you should know

- All snapshots are saved with the following naming convention: *CameraName (Date Time).png*. By default, snapshots are saved as PNG file in the following location: *C:\Users\Username\AppData\Local\Genetec Inc\Vault*.
- If you plan to use the snapshot for incident investigation, note that only JPEG files include EXIF tags that provide chain of custody information.

To take a snapshot of video in a tile:

1 Select the tile that is displaying the video image you want to save as a snapshot.

2 Do one of the following:

- In the camera widget, click **Save a snapshot** ( ).
- Right-click in the tile, and click **Camera** > **Save a snapshot** ( ).

A thumbnail preview is displayed in the upper-right corner of your Security Desk window for 2 seconds.

3 To open the Vault, from the home page, click **Tools** > **Vault**.
Thumbnails of all snapshots are displayed in the Vault.

4 To edit a snapshot, do one of the following:

- Select the snapshot and click **Edit** ( ).
- Right-click the snapshot and click **Edit**.

5 To print a snapshot, do one of the following:

- Select the snapshot and click **Print** ( ).
- Right-click the snapshot and click **Print**.

6 To delete a snapshot, right-click the thumbnail and click **Delete**.
If you delete the snapshots, the image files are no longer available.

7 To rename a snapshot, right-click the thumbnail and click **Rename**.

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

Editing video snapshots on page 207

Customizing snapshot options

Before taking snapshots of video, you can choose the file format and folder location of your saved snapshots, and enable the printing of an overlay on the snapshot image that shows the camera name, timestamp, and user name.

What you should know

- The **Write camera name and timestamp** and **Write user name** options are saved as part of your Security Center user profile. The other snapshot settings are saved locally for your Windows user profile.

  IMPORTANT: Snapshots are saved in the same folder as exported video files. If you change the folder location, existing video and snapshots can no longer be viewed from the Vault.
- The system can add EXIF tags to snapshots that are exported as JPEG. The EXIF tags contain information such as camera name, snapshot creation date, and camera coordinates, which is useful during incident investigation. EXIF data is only available if the **Include additional properties on export/snapshot** option is enabled on the **Advanced** tab for a user in Config Tool.

To customize snapshot options:

1 From the Security Desk home page, click **Options** > **Video**.
2 In the *Vault* section, configure the following options:
   - **Location:** The Windows folder path where exported video files and snapshots are saved. The default path is: *C:\Users\Username\AppData\Local\Genetec Inc\Vault*.
   - **Automatic cleanup:** When enabled, the retention period in days of exported video and snapshots in the Vault. When disabled, exported video and snapshots in the Vault are never deleted automatically.
3 In the *Snapshots* section, configure the following options:
   - **File format:** Choice of supported file formats: BMP, JPG, PNG and GIF. The default file format is PNG.
   - **Write camera name and timestamp:** The date, time, and camera name are stamped on the snapshot image.
   - **Write user name:** The *First* and *Last* name of the user are stamped on the snapshot image. If the user does not have a first and last name, their *Username* is stamped on the image.
4 Click **Save**.

Editing video snapshots

To ensure privacy or to hide elements of a video snapshot, you can use the editing tools in the video snapshot image editor.

Before you begin

Take a video shapshot.

What you should know

- Snapshots are stored in the Vault.
- All snapshots are saved with the following naming convention: *CameraName (Date Time).png*. By default, snapshots are saved in PNG format in the following location: *C:\Users\Username\AppData\Local\Genetec Security Desk version#\Vault*.

To edit a video snapshot:

1 From the home page, click **Tools** > **Vault**.

2 From the Vault, open the *Image editor* by doing the following:

- Select the snapshot and click **Edit** ( ).
- Right-click the snapshot and click **Edit**.

3 Edit the snapshot using the following editing tools:

- Rotate the image
- Flip the image
- Crop the image ( )
- Adjust the transparency ( )
- Adjust the brightness and contrast ( )
- Hide or blur sections of the image using the **Mask** tool ( )
- Zoom the image in or out by holding the `Ctrl` key, and scrolling using your mouse wheel

  After the image is zoomed in, you can pan and scroll the image. Pan the image by holding the `Ctrl` key, and clicking and dragging your mouse. Scroll vertically using your mouse wheel. Scroll horizontally by holding the `Shift` key, and using your mouse wheel.

4 Click **Save as** and save the edited snapshot.

IMPORTANT: If you need to keep the original snapshot, you must save the edited snapshot with a different file name.

Related Topics

Taking snapshots of video on page 206

Viewing snapshot EXIF data

Exchangeable Image File (EXIF) encodes additional information in an image file, such as when and where the image was taken. This additional information provides chain of custody information that can be can be used by internal or external authorities in the analysis of a case and in a court of law where admissible.

Before you begin

Set your snapshot options.

What you should know

- All snapshots are saved with the following naming convention: *CameraName (Date Time).png*. By default, snapshots are saved as a PNG file in the following location: *C:\Users\Username\AppData\Local\Genetec Inc\Vault*.
- EXIF data is only available if the **Include additional properties on export/snapshot** option is enabled on the **Advanced** tab for a user in Config Tool.
- EXIF data is only available for JPEG files.
- EXIF data can be changed. You know that a file has been changed if the **Date modified** no longer matches the **Date created**.
- There are free third-party EXIF viewers available online or for download. Some online EXIF viewers include: http://metapicz.com or http://regex.info/exif.cgi.
- The labels of the EXIF tags differs across viewers. For example, the name of the user that created the snapshot appears as **Authors** in *Windows Properties* and as **Artist** in metapicz.com.

To view additional file information in Security Desk:

1 Open the Vault: from the home page, click **Tools** > **Vault**.

Thumbnails of all snapshots are displayed in the Vault.

2 Right-click a file in the Vault and select **Show properties**.

To view the EXIF data of a snapshot in Microsoft Windows:

1 From *File Explorer*, right-click an image, click **Properties**, and then click the **Details** tab.

The following EXIF data is available.

- **Camera Model:** The name of the camera from which the video snapshot originated.
- **Date Time:** The date and time that the snapshot was exported.
- **Date:** Same as Date Time.
- **Host:** The name of the computer where the snapshot was created.
- **Artist:** The name of the Security Desk operator who exported the snapshot.
- **Latitude/LatitudeRef:** The latitude of the camera's location, which can be used to plot the camera's location on a map.
- **Longitude/LongitudeRef:** The longitude of the camera's location, which can be used to plot the camera's location on a map.
- **Comment:** Additional information about the snapshot in XML format.

2 Click the *Comments* box to view all of the information there.

The following list contains the XML tags and sample data.

- **<G64xAuditMetadata>:** The XML tag that indicates the beginning of the Comments data.
- **<Version>1</Version>:** The version number of the image.
- **<OperatorName>Admin</OperatorName>:** The name of the Security Desk operator who exported the snapshot. In this example, the user is Admin.
- **<WorkstationName>SecurityDesk</WorkstationName>:** The name of the computer where the snapshot was created.
- **<ExportTime>10/18/2016 11:23:57 AM EDT</ExportTime>:** The date and time when the snapshot was exported from Security Desk.
- **<Sequences>:** An XML tag that indicates the beginning of camera information.
- **<CameraName>Front Lobby Camera</CameraName>:** The name of the camera from which the video snapshot originated.
- **<StartTime>10/18/2016 11:23:56 AM EDT</StartTime>:** The date and time that the snapshot was exported.
- **<EndTime />:** Applies to video only. This will be blank for a snapshot.
- **<CameraLocation>< Altitude>0</Altitude>< Latitude>85.051128779806589</Latitude>< Longitude>-180</Longitude></CameraLocation>:** The map coordinates of the camera's location, which can be used to plot the camera's location in a map.
- **</Sequences>:** An XML tag that indicates the end of the camera information.
- **<Encryption>false</Encryption>:** Indicates if fusion stream encryption was enabled (true) or disabled (false) when the camera captured the video image. Encryption protects the privacy of your video archives.
- **<MetadataType>Snapshot</MetadataType>:** Indicates if this is a snapshot or a video.
- **</G64xAuditMetadata>:** An XML tag that indicates the end of the EXIF comments.

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 blocking is targeted for installations that provide the general public with access to live video. In such cases, cameras might be streaming video that is not suitable for certain users. As a result, you can restrict users from viewing a segment or entire video capture by blocking the camera.

How it works

Camera blocking is based on a user attribute called the user level. The highest user level is 1 and the lowest user level is 254. If you block a camera, users with a lower user level than the one that you select cannot view video (live, playback, or cached) or export video for the amount of time that you set.

When blocking cameras, the following applies:

- A user can only block a camera for someone that has a lower user level. As a result, users with a user level equal to 254 cannot block anyone, and users with a user level equal to 1 cannot be blocked by anyone.
- A user with a user level that is higher than the blocking level of a camera can view the camera.
- A user can unblock or change the blocking level of a camera if their user level is higher or equal to the user who initially blocked the camera.
- If there's more than one blocking setting applied to a camera, the highest user level that was specified is the active blocking level.
- A user can unblock past video by selecting a section of the playback video timeline.

Example

You block a camera from 1 P.M. to 4 P.M, and set a user level of 20. Another user blocks the same camera from 3 P.M. to 5 P.M., and sets a user level of 100. From 3 to 5 P.M., the blocking level is 100.

Related Topics

Blocking users from viewing video on page 211

Blocking users from viewing video

If something critical occurs during a video capture and must be made inaccessible to certain users, you can restrict certain user levels from viewing a segment or entire video by blocking the camera.

Before you begin

Do the following:

- Make sure you have the *Block and Unblock video* user privilege.
- Make sure that the camera you want to block is not from a federated Omnicast™ system.

What you should know

You can block a camera that is displaying live or playback video in a tile from any Security Desk task. You can also block and unblock cameras, and view the current block status of a camera from the *System status* task.

To block video in Security Desk:

1 Select a camera displayed in a tile.

2 Right click the tile, and then select **Camera** > **Block** ( ).

3 In the **Start** option, select the date and time to start blocking the video.

4 In the **End** option, select the duration of video to be blocked:

- **Until:** The video is blocked from users until the selected date and time.
- **For:** The video is blocked from users for the selected time (days, hours, minutes, or seconds).
- **Indefinitely:** All video from the **Start** time onward (including new recordings) is blocked from users until you manually unblock the camera.

5 From the **User level** slider, select a minimum user level.

NOTE: The highest user level is 1 and the lowest user level is 253.

6 Click **OK**.

All users with a user level lower than the one you select are blocked from viewing the video. Users that have a higher or equal user level can see that the camera is blocked by the dashes shown on the tile's timeline.

7 To unblock the camera, right-click inside the tile and click **Camera** > **Unblock** ( ).

NOTE: To unblock a certain part of playback video, you must select the section of the timeline and right-click from there.

To block or unblock cameras from the *System Status* task:

1 Select **Cameras** from the **Monitor** list.

2 Filter to the camera you want to block.

3 Select the desired camera in the report pane.

4 To block the camera, click **Block**.

5 To unblock the camera, click **Unblock**.

Related Topics

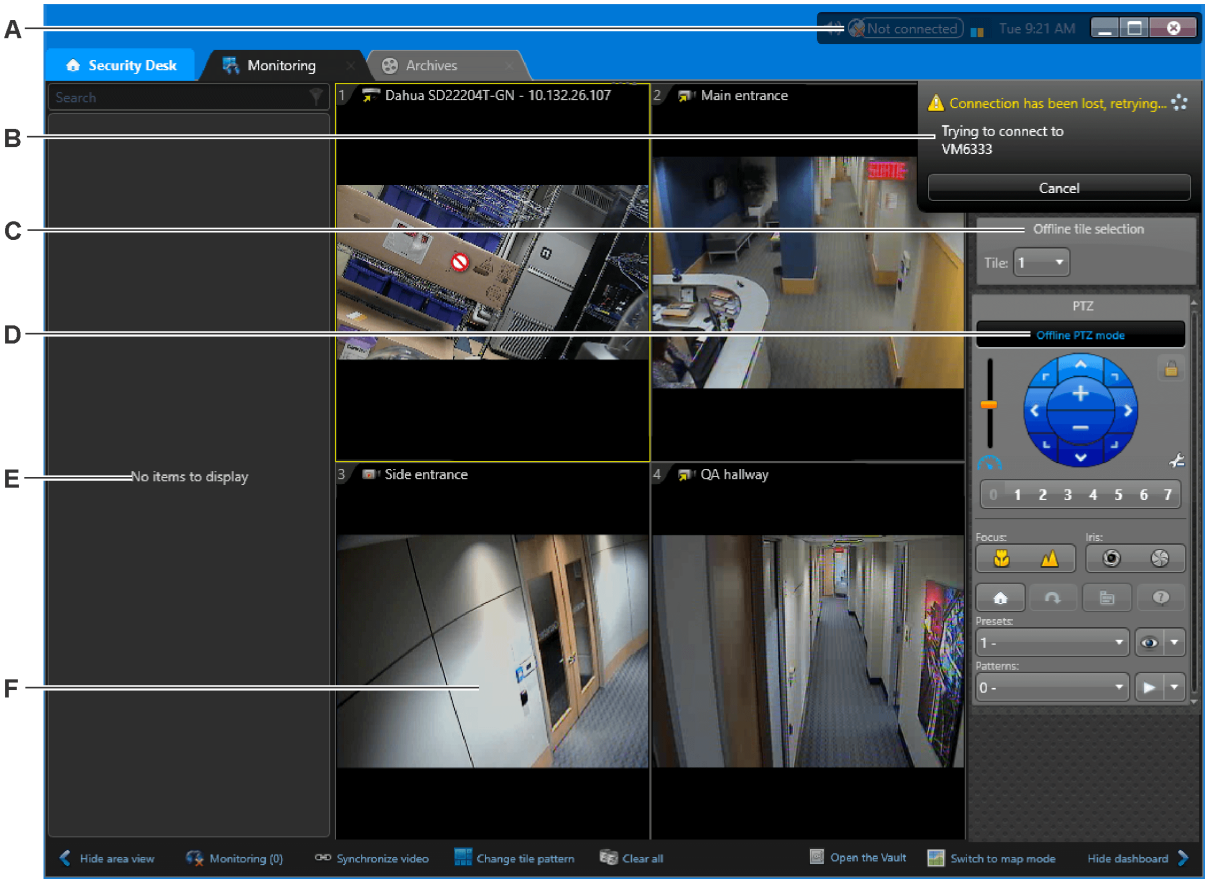
Tile menu commands on page 25
Camera blocking on page 210
Monitoring the status of your Security Center system on page 511

How video is displayed if the Directory role disconnects

The Security Center *Directory* role manages your entire system and without it you cannot log on to the system. If the Directory role is disconnected from the rest of the system, Security Desk starts to operate in a degraded mode.

If you were viewing a camera, you remain connected to that camera's live video stream even after you are logged out of the system. You can also view playback video if the live video was cached to your local workstation. Cached video is indicated by the orange bar at the top of the timeline.

Security Desk continuously attempts to reconnect to the Directory. When reconnected, the operating mode reverts to normal. While Security Desk is offline, you can still control your PTZ cameras through the widgets displayed in the dasboard. The following figure shows what the degraded mode looks like after a Directory failure.



A	Connection state icon shows that you are disconnected.
B	Pop-up message indicates that the Security Desk is trying to reconnect.

C	Use the tile widget to select which camera's PTZ you wish to control.
D	On-tile PTZ control does not work. You must use the PTZ widget, with the following limitations: • You cannot explicitly lock the PTZ, nor can you see who currently holds the lock. • You cannot edit nor see the names of the PTZ presets and patterns. • Specific commands do not work. • Digital zoom is not available. If it is activated, you must deactivate it before you can use the PTZ zoom.
E	The area view is unavailable.
F	Previously displayed cameras remain connected.

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 folder (default=*C:\Program Files (x86)\Genetec Security Center 5.10* 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.

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 (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.
- **Recording mode:** Recording settings for the camera.
- **Type:** Type of camera (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 (yes or no).
- **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.
- **Retention period:** Retention period of the camera.

4 To modify the settings of a camera, right-click an item in the report pane, and then click **Configure** ( ) to jump to that entity's configuration page in Config Tool.

NOTE: You need the user privilege to modify entities to use this command.

Manually recording video on Auxiliary Archivers

For local and federated cameras that are controlled by an Auxiliary Archiver, you can manually start recording video on the Auxiliary Archiver from Security Desk when you see something of interest.

Before you begin

The camera must be controlled by an Auxiliary Archiver, and the recording mode of the Auxiliary Archiver or camera must be set to *manual*. For more information about configuring Auxiliary Archivers and the recording modes of cameras, see the *Security Center Administrator Guide*.

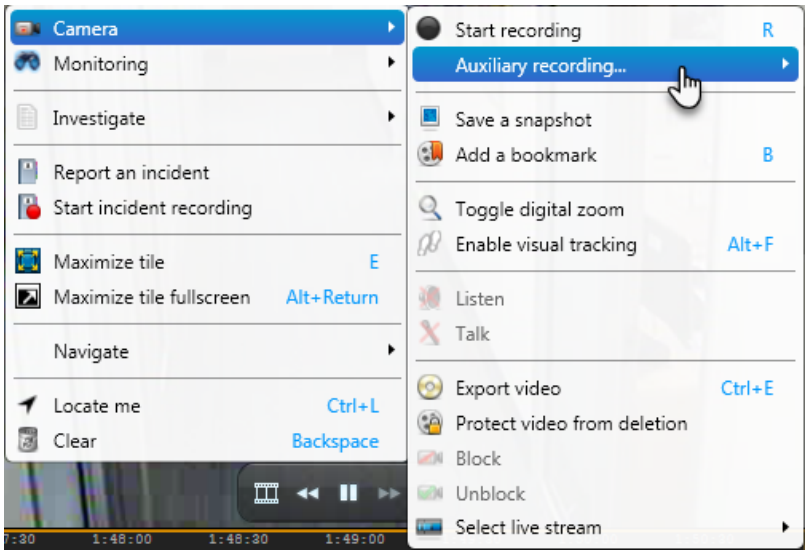
To manually record video on an Auxiliary Archiver:

1 Select a camera displayed in a tile.

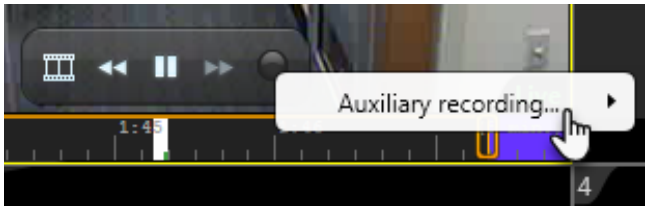
2 Do one of the following:

- Right-click inside the tile to open the tile context menu, and then click **Camera** > **Auxiliary recording**.

  You can also press `Shift+F10` to open the tile context menu. Then press Tab until **Camera** is selected and press `Enter`, and then press Tab until **Auxiliary recording** is selected and press `Enter`.



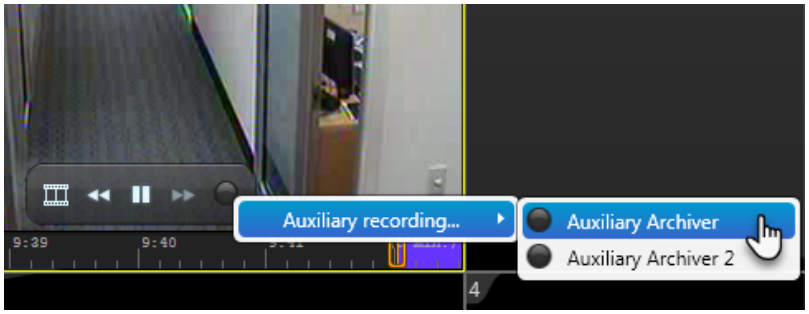
- Right-click the recording state icon inside the tile, and then click **Auxiliary recording**.



- Right-click the recording state button in the camera widget, and then click **Auxiliary recording**.

3 Click the record button (⚫) next to the Auxiliary Archiver role name.

If the camera is associated with multiple Auxiliary Archivers, select which Auxiliary Archiver to record on.



The video starts recording on the Auxiliary Archiver you selected, and is saved in the Auxiliary Archiver database.

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 web site.

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 motherboard'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 a different card to use them in parallel.
- If you have video cards using different drivers (AMD, NVIDIA, Intel), set a monitor connected to an 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) to register them as applications that require NVIDIA GPU. After the initial setup, the application always uses the NVIDIA GPU.

13

Video archives

This section includes the following topics:

Live and playback video modes

When viewing a camera in the canvas, you can alternate between *live* and *playback* video modes from the timeline or from the camera widget in the *Controls* pane.

Using the camera widget, you can pause, rewind, or instantly replay video. When a camera is displayed, the current video mode is shown in the lower-right corner of the tile.

When you are viewing live video, the camera's current recording state is indicated:

- Green with red dot (Live) - The camera is currently recording.
- Green (Live) - The camera is currently not recording.

When you are viewing playback video, the date and time stamp of the recording is indicated.The date/time stamp can be displayed in absolute mode or relative mode. Click the date/time stamp to toggle between the two display modes.

- Yesterday at 2:33 PM Date/Time stamp overlay in *relative* mode.
- 28/08/2011 2:33:19.003 PM Date/Time stamp overlay in *absolute* mode.

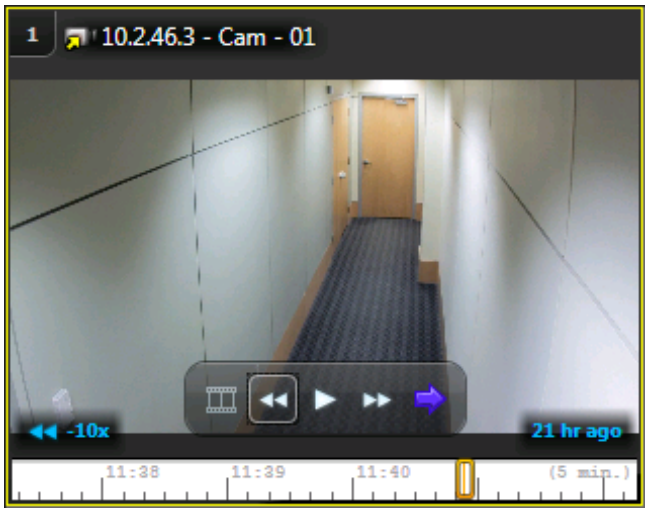
How the video mode is determined

If you decide to view another camera in the canvas, by default the video mode is inherited from the currently selected tile. For example, if the selected tile is displaying playback video, then when you add a camera to a new tile, it also displays playback video.

If the currently selected tile is not displaying a camera, the inherited video mode depends on the task type. The default video mode for *Monitoring* tasks is live video. The default video mode for investigation tasks is playback video.

Video playback states

When you are viewing playback video in a state other than normal playback (1x), a blue overlay appears on the lower-left corner of the image. In the following figure, the playback video is reversing at 10 times (10x) the normal speed.



Possible playback states	
	Pause
	Slow motion playback
	Fast forward playback (2x, 4x, 6x, 8x, 10x, 20x, 40x, or 100x)
	Reverse playback (-2x, -4x, -6x, -8x, -10x, -20x, -40x, or -100x)

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

Switching between video modes on page 223

Switching between video modes

You can alternate between *live* and *playback* video modes from the timeline or from the camera widget in the *Controls* pane.

What you should know

If the camera is not currently recording (indicated with the green Live overlay), the Archiver might not be available. However, even if the camera is not recording on the Archiver, the orange bar at the top of the timeline indicates the video that has been buffered locally on your hard drive. Locally buffered video is available for playback.

To switch video modes:

1 Switch to *playback* video mode one of the following ways:

- On the timeline, click and drag the playback cursor to the left.

  TIP: The timeline scale can be adjusted by scrolling your mouse wheel while hovering your mouse pointer over it.
- To begin reverse playback, click **Rewind** () in the camera widget.

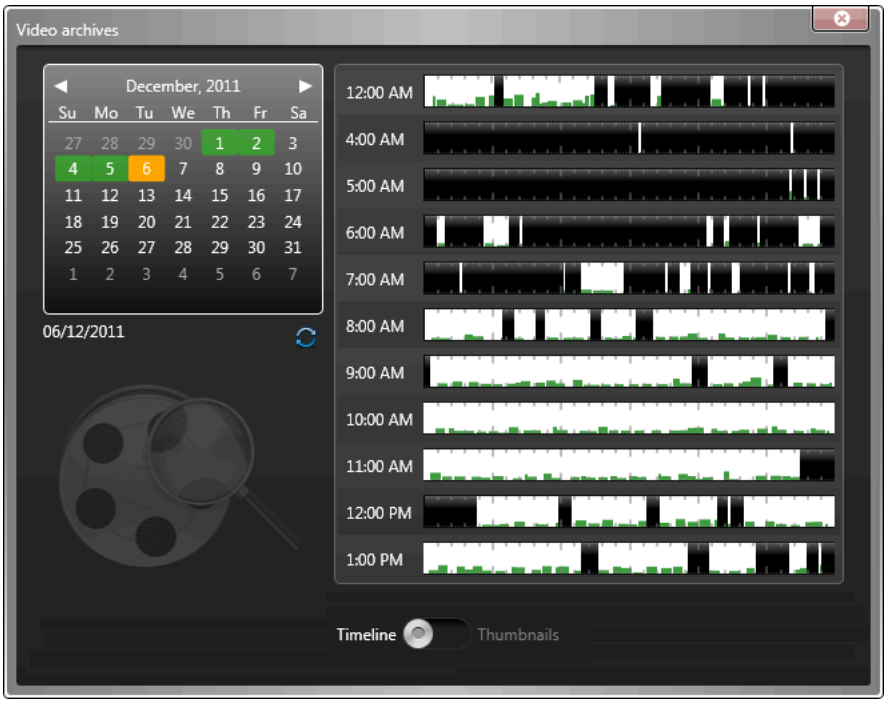
  Successive clicks adjust the playback speed from -1x to -100x.
- To jump backwards in 15-second increments, click **Jump backward** () in the camera widget.

  The seek value is 15 seconds by default. You can change this value in the *Options* dialog box.
- To jump to a specific time in the video playback, do the following:

  a. In the camera widget, click **Go to specific time** ().

  b. In the *Video archives* dialog box, use the calendar to navigate through the months and years, and select a date.

  The hours in the day that video archives are available on are shown on the right in a timeline and are indicated by a white background.



  c. (Optional) Switch between *Timeline* and *Thumbnails* view.

  d. Click a position in the timeline to jump to that hour in the video recording.

2 Switch to *live* video mode one of the following ways:

- In the on-tile video controls, click **Camera** > **Switch to live** ().
- In the camera widget, click **Switch to live** (

).

Related Topics

Live and playback video modes on page 221
Video options on page 280

About cloud playback

Video archives in Cloud storage are available for playback and investigation in Security Center.

Video archives in the cloud are assigned to the Performance tier or the Long-term tier. These access tiers affect the availability of the recordings.

- **Performance tier:** Recordings in the Performance tier are available to all authorized users connected to the system. Subject to certain limitations, you can work with these video archives in the same way as playback video managed by the Archiver.
- **Long-term tier:** Video archives in the Long-term tier are not available immediately, and must be requested 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 organization's Cloud storage policies, video archives typically spend a short time in the Performance tier before moving to long-term storage.

Related Topics

Requesting video archives from long-term Cloud storage on page 226

Limitations for Cloud storage

Cloud storage includes the following known limitations.

Issue	Description
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 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 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	Migration from Cloud Archives to Cloud storage is not currently supported. For more information on migrating Cloud Archives to Cloud storage, contact your local sales representative.

Requesting video archives from long-term Cloud storage

Before you can work with video archives in long-term Cloud storage, you must retrieve that video from Security Desk.

Before you begin

- Cloud storage must be enabled, with video archives stored in the Long-term access tier.
- Your user account must have the *Retrieve cloud archives* privilege.
- To retrieve recordings from a federated system, both the local and federated system must be using Security Center 5.10.2.0 or later.

What you should know

Recordings can be retrieved from the *Camera* widget, or from the *Archives* task.

To retrieve cloud archives from the *Camera* widget:

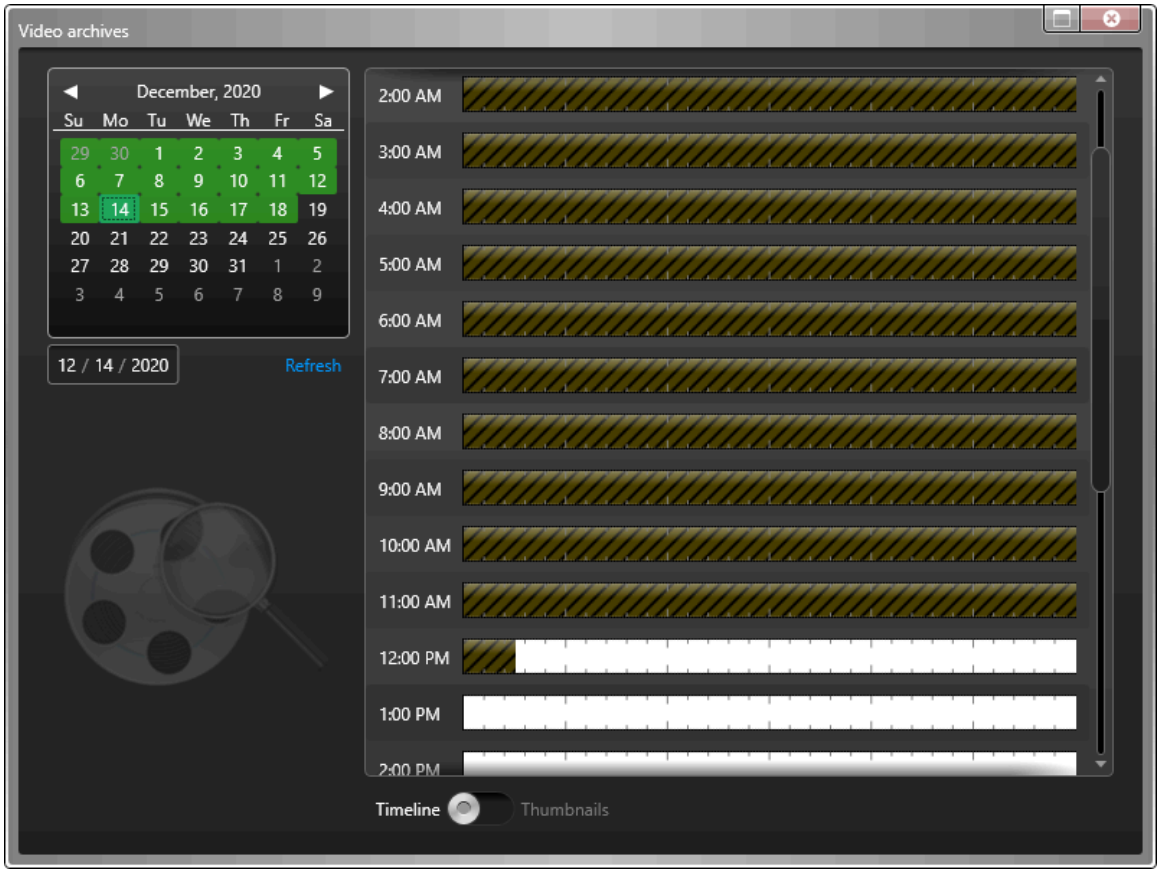
1 From any video-related task in Security Desk, view the required camera in a tile.

2 In the associated *Camera* widget, click **Go to specific time** ( ).

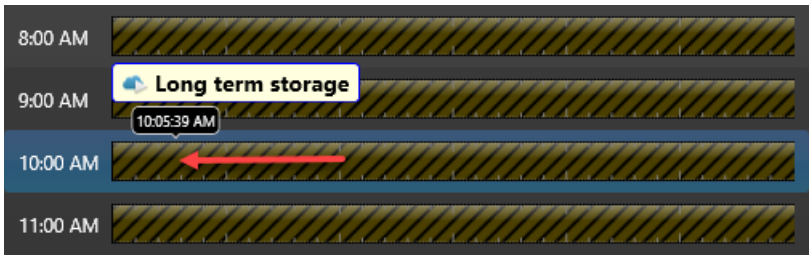
The *Video archives* window opens.

3 Select the required day from the calendar.

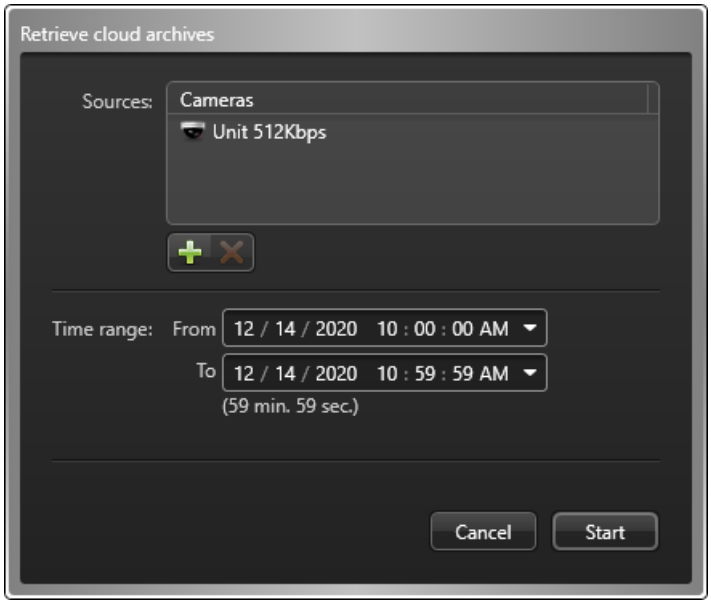
Video archives for that day are displayed by the hour. Recordings in long-term storage are indicated by dark hash marks ( ).



4 Select an hour of video that contains archives in long-term storage.



The *Retrieve cloud archives* window opens.



5 Select the required options. These options default to the selected camera and the selected time.

- **Sources:** The cameras to be retrieved. Only video archives for the selected cameras are retrieved from long-term storage.
- **Time range:** The start and end time of the video to be retrieved.

6 Click **Start**.

The selected video archives are requested from long-term storage. Requested recordings are indicated by bright hash marks ( ).

NOTE: It might take a few minutes for the bright hash marks to show.

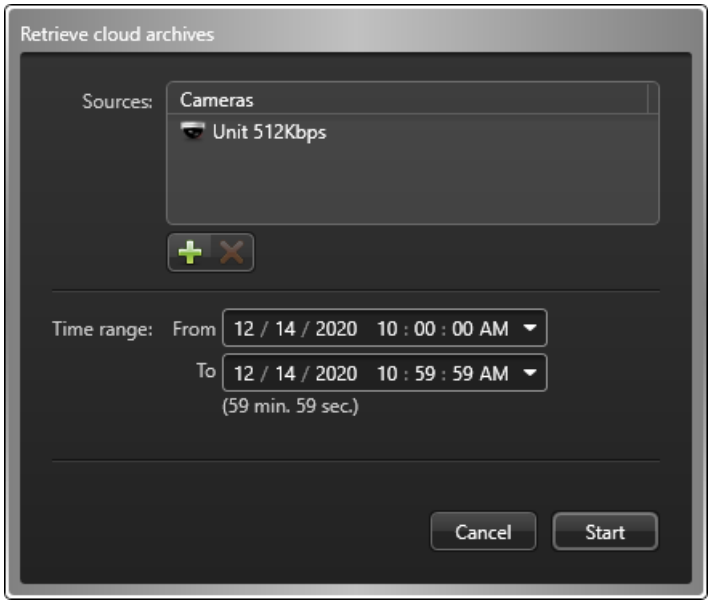
To retrieve cloud archives from the *Archives* task:

1 From the *Archives* task in Security Desk, search for the required video archives.

TIP: You can limit your search to video archives in Cloud storage, by selecting the **Cloud Playback** source in the report filters.

2 Select a video archive with content in long-term storage from the report pane and click **Retrieve cloud archives** ( ). Recordings in long-term storage are indicated by dark hash marks ( )

The *Retrieve cloud archives* window opens.



3 Select the required options. These options default to the selected camera and the selected time.

- **Sources:** The cameras to be retrieved. Only video archives for the selected cameras are retrieved from long-term storage.
- **Time range:** The start and end time of the video to be retrieved.

4 Click **Start**.

The selected video archives are requested from long-term storage. Requested recordings are indicated by bright hash marks ( ).

NOTE: It might take a few minutes for requested archives to display.

After you finish

Access to the requested video is usually granted within 15 hours. Check the status by clicking the **Retrieve cloud archives** ( ) icon in the notification tray.

If the status shows Should retry, Cloud storage encountered a transient error while processing your request. Select the request and click **Retry** to retrieve the same video again. To select multiple requests at the same time, press Ctrl and click.

You will be notified when the requested video becomes available. These archives remain available at the Performance tier for seven days.

Related Topics

About cloud playback on page 225
Viewing cameras in tiles on page 188
Viewing video archives on page 233
Notification tray icons on page 94

About the video timeline

The timeline appears below the video image in canvas tiles.

With the video timeline you can do the following:

- Move the timeline window to the left or to the right by clicking on the timeline itself and dragging it either left or right.
- Shrink or widen the timeline by hovering your mouse pointer over the timeline and turning your mouse wheel.

A	White background indicates that a recording is present.
B	Black background indicates that no recording was made at that time.
C	Green motion bars. The bigger the bar, the more motion is present.
D	Orange ribbon icon indicates the presence of a bookmark. Mousing over the bookmark displays the associated text and time stamp.
E	Orange bar at the top of the timeline indicates video that has been cached (buffered) on your workstation's hard drive.
F	Playback cursor. Drag cursor to playback a different point on the timeline.
G	Playback timestamp. Click to toggle between relative and absolute time.
H	Timeline duration/scale. Hover your mouse pointer and scroll the mouse wheel to zoom in or out on the scale of the timeline.
I	Purple background indicates the future.

Example

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

Creating a playback loop

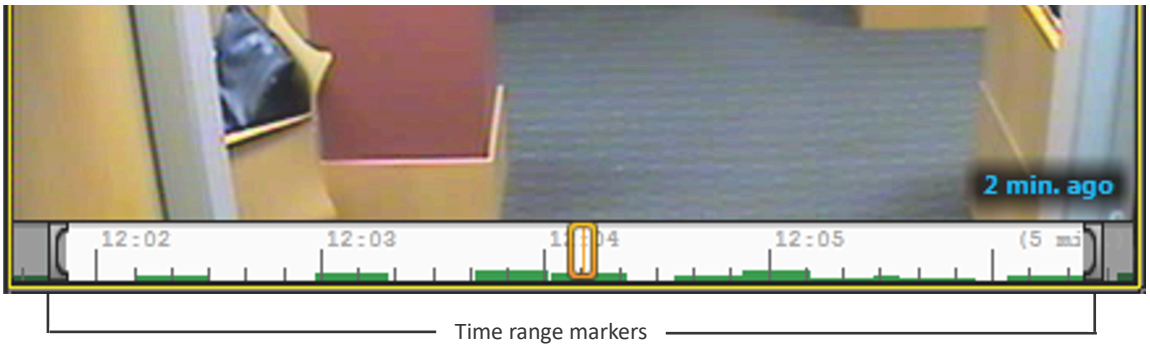
To play the same video sequence repeatedly, you can create a playback loop in the video timeline.

To create a playback loop:

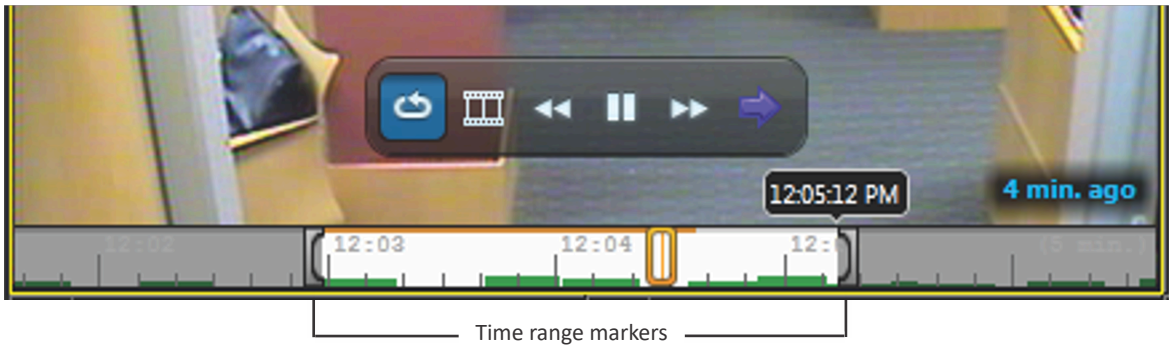
1 Do one of the following:

- In the camera widget, click **Loop playback** ( ).
- Right-click in the timeline.

Two time range markers appear, one on each end of the timeline.



2 Drag the markers to their desired positions. While you are holding a marker with your mouse, the exact time position of the marker is shown.



The playback loop starts instantly. While you are in a playback loop, all the playback controls remain available.

3 To cancel the playback loop, click **Loop playback** ( ) in the on-tile video controls or the camera widget.

Performing targeted video searches

If a camera recorded an event and you know where the event occurred in the camera's field of view, such as a bag removed from a table, you can use *Quick search* on the playback video to find the exact video sequence containing the evidence.

What you should know

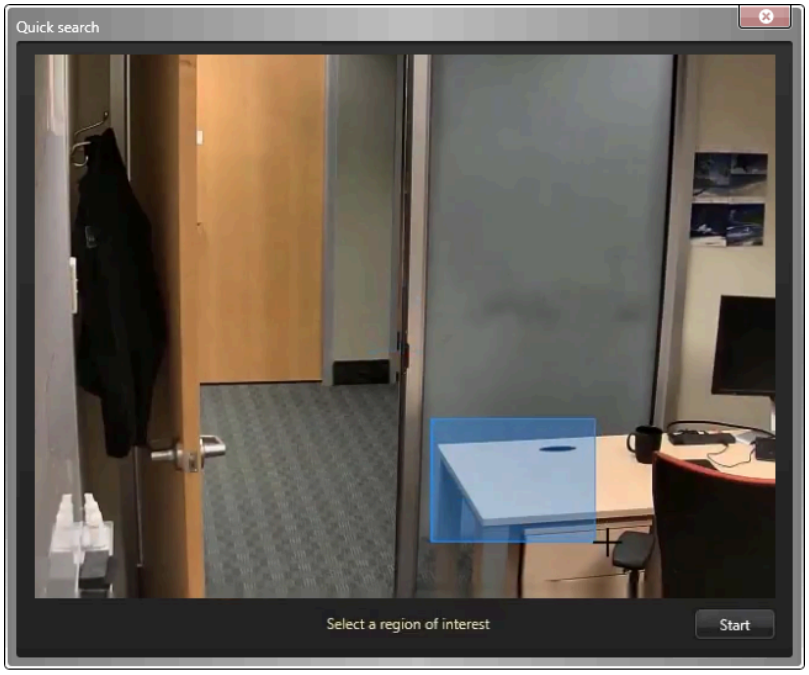
Quick search only supports playback video.

To perform a targeted video search:

1. From the home page, open the *Monitoring* task.
2. From the area view, drag the camera you want to search from to a tile.
3. In the camera widget, click **Quick search** ( ).

   The selected camera is displayed in the *Quick search* dialog box.
4. Draw a rectangle around the area you want to target your search.

   For example, if you are trying to find out who removed an object from a table, circle the corner of the table where the object was supposed to be left.



5 Click **Start**.

An overview of the last six hours of video recording is displayed as a series of thumbnails cropped to the area you selected.

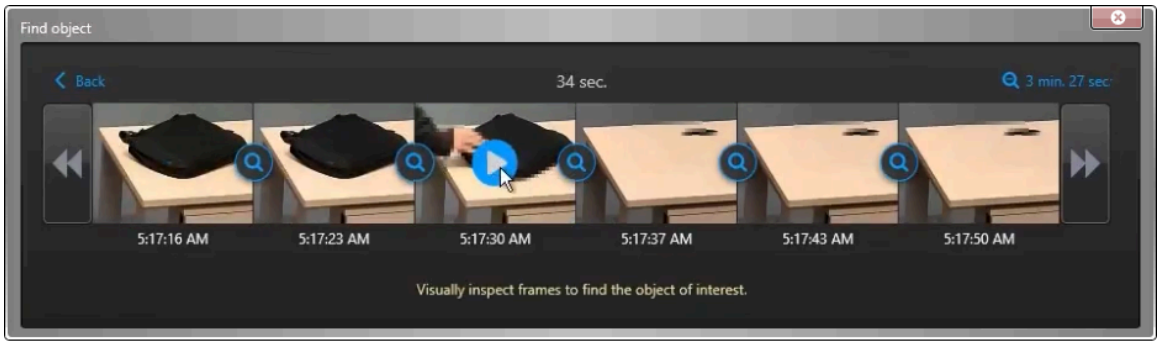
NOTE: No thumbnails are displayed when there is no recorded video. If you know that recorded video exists but do not see any thumbnails, Security Desk might not be configured correctly. Ask your system administrator to resolve this issue for you.

6 Visually inspect the thumbnails and click the button between the two frames when the object was removed.

7 If none of the frames correspond to the moment you are looking for, click or to move backward or forward in the timeline.

8 Continue the search process until you find the exact moment when the incident took place.

9 When you find the exact moment you are looking for, click the corresponding frame to start the playback from that moment.



10 (Optional) Export the video sequence as evidence.

Example

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

Viewing video archives

Using the Archives report, you can find and view video archives on your system by camera and time range.

What you should know

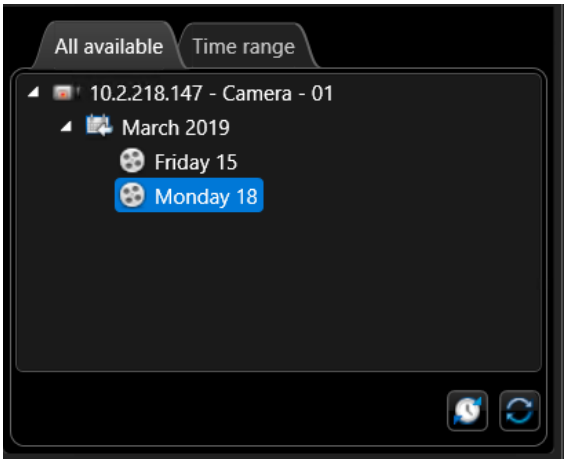
If an important security event occurs, you can do the following in the Archives report:

- Search for available *video archives* from a specific time range or from a specific camera during a given date.
- Search through the video archives to review a video recording.
- Export a video recording to share with colleagues or law enforcement.
- Retrieve cloud archives from long-term storage.

To view a video archive:

1. From the Security Desk home page, open the *Archives* task.
2. Click the **Filters** tab and select the cameras that you want to investigate.
3. Search for video archives by date or by time range:
   - To search for video archives by date:
     a. Click the **All available** tab, and then select the cameras that you want to investigate.

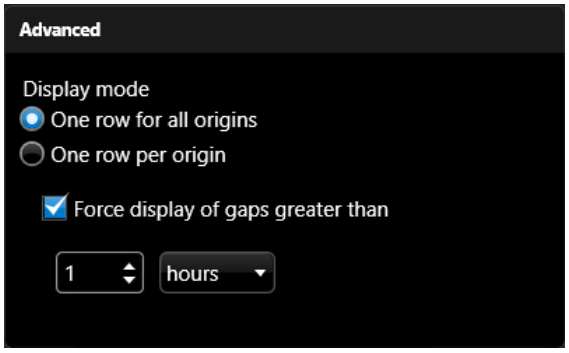
        All days that include video archives for the selected cameras are listed by month and day.

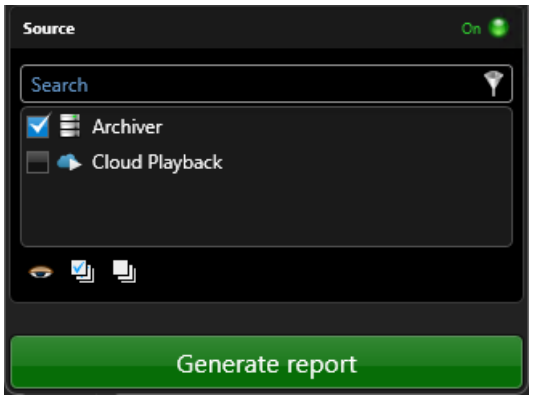
     b. To show the time range for each day that video archives are found for, click .
     c. Select a date.
   - To search for archives by time range:
     a. Click the **Cameras** filter and select the cameras to investigate.
     b. Click the **Time range** tab and set the time range.

4 Select advanced display mode options.

NOTE: The **Force display of gaps greater than** field can be configured for seconds, minutes, hours, or days.



5 Search a specific source.



Possible sources include:

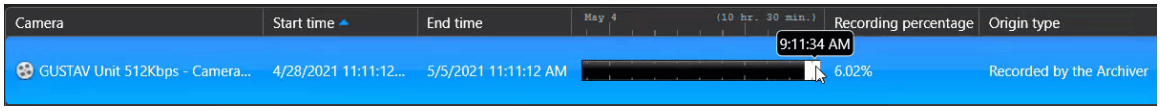
- Archiver roles
- Auxiliary Archiver roles
- Cloud Playback role
- Omnicast™ Federation™ roles
- Security Center Federation™ roles

6 Click **Generate report**.

The related video recordings are listed in the report pane:

- If you searched by date, the hours in the selected day that video is available on are listed.
- If you searched by time range, only cameras with video archives are listed, and the *Preview* column header is replaced with a timeline ruler.

  NOTE: If the report results include cameras in different time zones and your system displays time based on each device's time zone, the timeline ruler is hidden.
- If you searched by time rage, you can hold the Ctrl key and use the mouse wheel to zoom in or out on the timeline ruler.



NOTE: You cannot zoom outside of the original query time span. To view a larger time span, generate a new query.

The *Preview* column shows where video is available within the sequence for each camera. You can hover over this timeline to see specific timestamps.

7 To view the video sequence in a tile, double-click or drag an item from the report pane to the canvas.

The selected sequence starts playing.

NOTE: If you get the message No video available at this time, verify that you have the following:

- A valid certificate if the video stream is encrypted.
- The required privilege to see that particular camera. The camera might be blocked and require a special privilege to see its archives.

8 To control the video recording, use the *Camera* widget.

9 To export an important video archive, select the item in the report pane and click **Export** ( ).

10 To retrieve video archives from long-term cloud storage, select the item in the report pane and click **Retrieve cloud archives** ( ).

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

Exporting video in G64x format on page 250
Exporting video in G64, ASF, and MP4 formats on page 255
Exporting generated reports on page 74
Camera widget on page 39
Overview of the Archives task on page 580
Requesting video archives from long-term Cloud storage on page 226

Report pane columns for the Archives task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Archives 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.

- **Start time:** Beginning of the time range, playback sequence, or video sequence.
- **End time:** End of the time range, playback sequence, or video sequence.
- **Preview:** Timeline showing where video is available during the selected time range.
- **Thumbnails:** Thumbnail images of the recorded video during the selected time range. Thumbnails only appear for video that was recorded by an Archiver or Auxiliary Archiver, not if the video was recorded on the edge. Thumbnails are not available for video archives in Cloud storage.
- **Recording percentage:** Percentage of available video displayed over the queried time range.
- **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.

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.

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) and whether the Archiver is currently recording the data.
- **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.

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. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
- **Events:** Select the events of interest. The event types available 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.

Searching video archives for motion events

You can search the video archives for *video sequences* that detect motion in specific areas of a camera's field of view, using the *Motion search* report.

To search the video archives for motion events:

1 From the home page, open the *Motion search* task.

2 In the *Filters* tab, select a camera from the drop-down list.

When a camera is selected, a preview image based on the default time range appears. If the selected camera does not support motion search, the message "Motion search not available for this camera" is displayed instead of the preview image.

3 To refresh the preview image based on the new time range, click .

4 To view a video instead of a still image, click .

5 Set the time range for the motion search.

6 To define a motion detection zone over the preview image, draw motion detection blocks (blue rectangles) on areas where motion is meaningful for the search, using the following tools:

- 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 interchange 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.

7 To influence the speed and accuracy of the motion query, configure the motion detection criteria options as follows:

- **Motion threshold:** Sets the minimum number of blocks that must be activated for a motion detection result to show up in the query. The total number of blocks in the motion detection zone is indicated as the maximum value allowed for the threshold. A value of zero means any motion detected in the defined zone would qualify for the search.
- **Consecutive frame hits:** Applies the motion threshold to a specified number of video frames. This setting helps to avoid false-positive motion detection (for example, video noise in a single frame). It ensures that motion is detected when the threshold is met over a specified number of consecutive frames, not in a single frame.
- **Minimum time between frames:** Controls the sampling rate for the search by telling the system not to examine every single video frame. The *higher* the value, the more frames the system skips during the search, thus performing the search faster. To examine every frame, set the value to 33 ms or less. The highest archiving frame rate is 30 frames/sec. At this rate, the time between two consecutive frames is only 33 ms.

8 Click **Generate report**.

The motion events are listed in the report pane.

9 To show the corresponding video of a motion event in a tile, double-click or drag an item from the report pane to the canvas.

The selected sequence immediately starts playing.

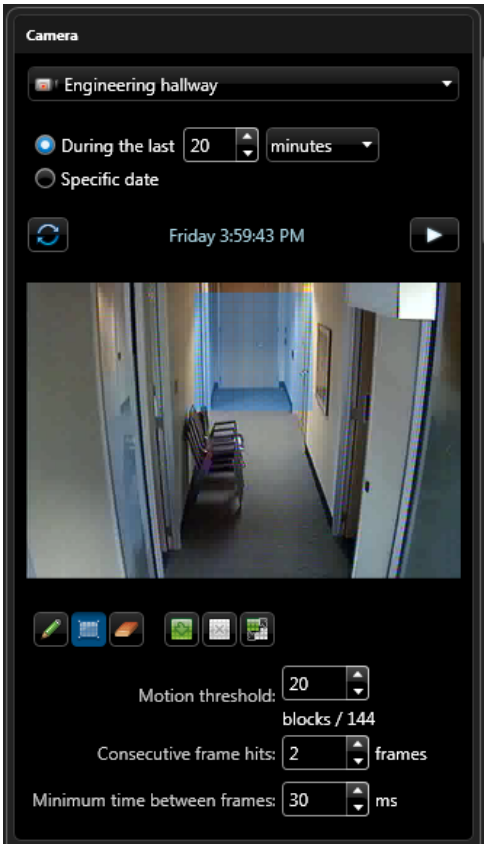
10 To control the video recording, use the camera widget.

11 To export an important video archive, select the item in the report pane, and then click **Export** ( ).

Example

If you want to see the activity that happened around a specific door, you can search for motion using the camera that points at the door. In the following figure, a motion detection zone is defined by the entrance

door. As a result, the search is targeted at the door and motion created by people walking farther down the hallway is ignored.



Related Topics

Exporting video in G64x format on page 250
Exporting video in G64, ASF, and MP4 formats on page 255
Selecting date and time ranges for reports on page 73
Camera widget on page 39
Overview of the Motion search task on page 582

Report pane columns for the Motion search task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Motion search 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.
- **End time:** End of the time range, playback sequence, or video sequence.
- **Source (entity):** The name of the system the camera belongs to.
- **Start time:** Beginning of the time range, playback sequence, or video sequence.

Searching video archives for camera events

You can find events related to selected cameras that were recorded by an Archiver, using the *Camera events* report.

What you should know

This report is helpful if you already know the name of the camera that you are looking for. You can see what events have been triggered from that camera. You can also investigate specific events. For example, recording that was started due to an alarm.

To receive results in your report, the video and analytic metadata must be recorded by an Archiver.

To search the video archives for camera events:

1 From the home page, open the **Camera events** task.

2 Set up the query filters for the report. Choose from 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.
- **Events:** Select the events of interest. The event types available depend on the task you are using.
- **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.

3 Click **Generate report**.

The camera events are listed in the report pane.

4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

5 To control the video recording, use the camera widget.

Related Topics

Camera widget on page 39

Report pane columns for the Camera 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 Camera events task.

- **Archiver:** Archiver role name.
- **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.
- **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.

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 timeshift 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 timeshift from DST to EST occurs at 2:00 am. Before 2:00 am, Security Center uses the DST (UTC-4). Starting from 2:00 am, it uses the EST (UTC-5), as shown in the following table:

	DST		Time change	EST	
Local time	12:00 am	1:00 am	2:00 am = 1:00 am	2:00 am	3:00 am
Offset (hours)	-4	-4	-5	-5	-5
UTC	4:00 am	5:00 am	6:00 am	7:00 am	8:00 am

Because the time was adjusted backward, the following behaviors can be observed when playing back video or exporting archives:

- The time shifts back by one hour in the timeline. After 1:59:59 am, the displayed time falls back to 1:00:00 am.
- The end time of a video sequence can be earlier than the start time.
- Exporting archives between 1:00 am and 2:00 am always includes an additional hour of video. For example, when exporting archives from 1:50 am - 2:00 am on the night of a timeshift, the exported sequence includes 1 hour and 10 minutes of video because the query includes video from 5:50 am - 7:00 am UTC.

To prevent the time from shifting back by one hour during video playback, or to export video without an extra hour of footage, you must 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 timeshift from EST to DST occurs at 2:00 am. Before 2:00 am, Security Center uses the EST (UTC-5). Starting from 2:00 am, it uses the DST (UTC-4), as shown in the following table:

	EST		Time change	DST	
Local time	12:00 am	1:00 am	2:00 am = 3:00 am	4:00 am	5:00 am
Offset (hours)	-5	-5	-4	-4	-4
UTC	5:00 am	6:00 am	7:00 am	8:00 am	9:00 am

Because the time was adjusted forward, the following behaviors can be observed when playing back video or exporting archives:

- The time shifts forward by one hour in the timeline. At 1:59:59 am, the displayed time advances to 3:00 am.
- There are no archives to export between 2:00 am and 3:00 am, because this period was skipped.

To prevent the time from shifting forward by one 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 home page, 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.

14

Video export

This section includes the following topics:

Video export formats

The video export formats that are available in Security Desk determine the media player that is used to view the exported video files. You can export video in G64x, G64, ASF, and MP4.

G64x and G64 formats

G64x and G64 are Security Center video formats that support audio, bookmarks, date-time information, metadata overlays, and motion indicators. All event markers are included in the exported file, except metadata markers. These formats also support variable frame rate and variable image resolution.

NOTE: The G64 format is deprecated and has been superseded by G64x. Only use G64 to ensure compatibility with Security Center 5.2 and earlier, and Omnicast™ 4.8 and earlier.

If present, G64x files automatically inherit the *digital signature* from the original video. There can only be one signature per file. If an exported video sequence has multiple signatures, a separate file is generated for each signature. Additionally, G64x is the only format that can be re-exported, if that option is selected during export.

When you export multiple video sequences from the canvas simultaneously, they can be combined into a single G64x file. G64x files are also created when you export an incident package using incident recording in a tile. Depending on how you export the video, the video sequences are either played back in the same tiles that they were playing in when they were exported, or played back within a single tile, in the order that they were recorded.

NOTE: Federated Omnicast™ cameras cannot be exported in G64x format. If you select G64x format, the video sequences from federated Omnicast™ cameras are exported in multiple G64 files instead of the packaged G64x file. These G64 files will carry a digital signature if the original video was signed.

You need Security Desk or the Genetec™ Video Player to view G64x and G64 files.

ASF format

Advanced Systems Format (ASF) is a Microsoft proprietary data format. This format supports audio information and variable frame rate, but not metadata associated with the video sequence. Date and time information is also not supported, but it can be overlaid on the video images during the exporting process.

If the video sequence that you want to export uses multiple image resolutions (CIF, 2CIF, 4CIF, and so on), the exported video sequence follows the image resolution of the first frame rate in the source video sequence. In addition, metadata associated with the video sequence and digital signatures are not exported. You can use this format if you need to make a copy of a video recording to share with law enforcement, your legal department, or other members of your security team.

When you export multiple ASF video sequences from the canvas simultaneously, a single ASX file is produced so you can view the ASF files in the order they were recorded.

You need Windows Media Player to view ASF video files.

MP4 format

MP4 is a standard format that stores audio and video and can be played back on many media players such as Windows Media Player and QuickTime.

When you export multiple MP4 video sequences from the canvas simultaneously, an ASX file is produced so you can view the MP4 files in the order they were recorded.

Exporting to MP4 supports H.264 and MPEG-4 video, and AAC audio formats. Fusion stream encryption, overlays, and digital signatures are not currently supported.

Related Topics

Exporting video in G64x format on page 250
Exporting video in G64, ASF, and MP4 formats on page 255
Configuring settings for exporting video on page 248

Configuring settings for exporting video

Before exporting video in Security Desk, you must choose where to save the exported video files and configure the settings for each export format.

What you should know

When you export a G64x video, the system can include additional file information, such as camera name, creation date, and camera coordinates, which can be useful for investigation. To view additional file information, right-click a file in the Vault and select **Show properties**.

NOTE: The system only includes this additional file information if an administrator enables the feature in your user settings.

IMPORTANT: Exported video files are saved in the same folder as snapshots, and are available from the *Vault*. If you change the folder location, existing video and snapshots can no longer be viewed from the Vault.

To set default settings for exporting video:

1 From the home page, click **Options** > **Video**.

2 In the *Vault* section, configure the following options:

- **Location:** The Windows folder path where exported video files and snapshots are saved. The default path is: *C:\Users\Username\AppData\Local\Genetec Inc\Vault*.
- **Automatic cleanup:** When enabled, the retention period in days of exported video and snapshots in the Vault. When disabled, exported video and snapshots in the Vault are never deleted automatically.

3 In the *Export* section, select a **Default file format** for exporting video:

- **G64x:** A file that contains multiple video sequences that can be played back in Security Desk or the Genetec™ Video Player.
- **G64 (compatibility mode):** A Security Center format that can be played back in Security Desk or the Genetec™ Video Player.
- **ASF (Advanced Systems Format):** A Microsoft proprietary data format that can be played back in Windows Media Player.
- **MP4:** A standard format that stores audio and video and can be played back on multiple media players such as Windows Media Player and QuickTime.

4 Click **Advanced** (⊕) and set the following options:

NOTE: The options for G64x format can be overwritten at the time of export.

Option	Description	Applicable to
Add password protection	Turn this option on to protect the exported video files, and enter a password in the **Password** field. Anyone wishing to view the exported video files will have to enter the same password.	G64x
Delete intermediary files	Turn this option on if you want to delete the original files (non-protected files). If you are not protecting the exported video files with a password, this option has no effect. **NOTE:** The password-protected filename is the original filename with the suffix "_1" added.	G64x

Option	Description	Applicable to
Allow the video file to be re-exported	Select this option to allow the person viewing the exported video to *re-export* the video, either in part or in full, in the same or a different format. **NOTE:** Setting a password automatically disables this option.	G64x
Use following profile	Select the compression profile. The bit rate (shown in brackets) indicates the quality of the exported video. The higher the bit rate, the better the quality and the larger the file size. The **Description** under the profile provides useful information to guide your choice.	ASF
Export audio	Turn this option on to include audio information in ASF and MP4 files.	ASF, MP4
Display date and time on video	Turn this option on to have the date and time overlaid on the exported video image.	ASF
Delete intermediary files	Turn this option on if you want to delete the original files after they are converted into ASF or MP4 files.	ASF, MP4

5 Click **Save**.

Related Topics

Video export formats on page 246

Exporting video in G64x format

To create stand-alone G64x video files that you can play without connecting to Security Center, you can export from any task in Security Desk that displays live or playback video.

Before you begin

- Review the available video export formats.
- Configure the default settings for exporting video.
- Ensure that you have the *Export video* privilege.

What you should know

- When you export a G64x video, the system can include additional file information, such as camera name, creation date, and camera coordinates, which can be useful for investigation. To view additional file information, right-click a file in the Vault and select **Show properties**.

  NOTE: The system only includes this additional file information if an administrator enables the feature in your user settings.
- If you have video watermarking enabled, digital signatures and encryption in the video source are excluded from your exported file.

To export video:

1 From the Security Desk home page, open any task that can display live or playback video.

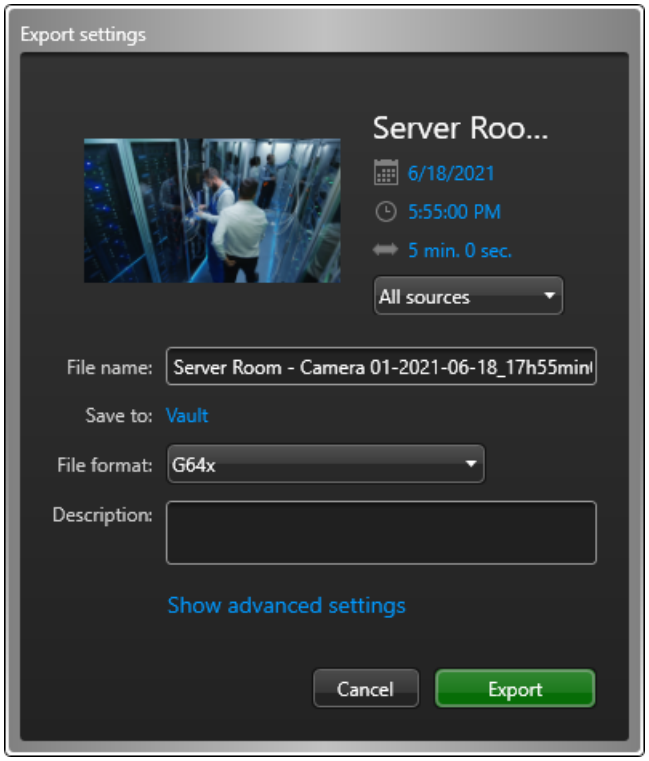
2 Select the video to export.

- After generating a report, select one or more items from the report pane, and click **Export video** ( ).
- Open video in a tile, right-click the tile, and click **Camera** > **Export video**.
- In the *Camera* widget, click **Export video** ( ).

You can export video from the selected tile or from all tiles.

NOTE: Privacy protection is not removed from video streams during export. To export protected streams without blurring or anonymization, users with the *Remove privacy protection* privilege must remove privacy protection from the required streams before they click **Export video**.

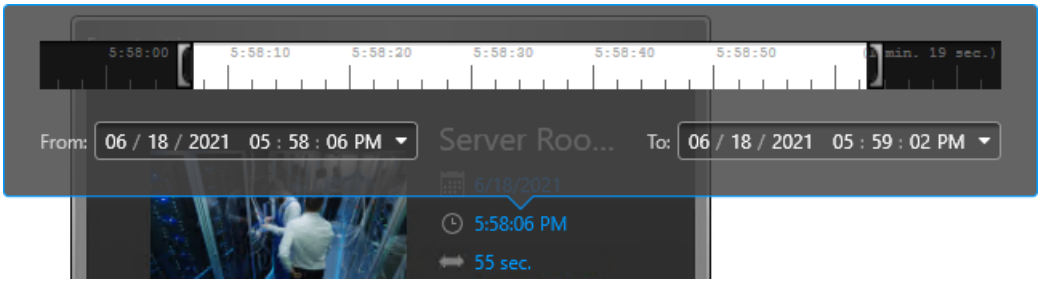
The *Export settings* dialog box opens:



3 Set the date, time, and duration of the selected video sequences:

a) Click the date, time, or duration setting.

b) Enter the date and time for the start and end of the sequence, or drag the time range markers ( ) to the desired length of time.



NOTE: You can set a maximum time range of 24 hours.

4 (Optional) To export a video sequence from a specific source, click **All sources** and select the source to export from.

5 If required, update the name of the video file in the **Filename** field.

By default, the file name includes the camera name, the date, and the duration of the video sequence.

6 (Optional) To save the video file in a specific subfolder of the Vault, click **Vault** and create or select a subfolder.

7 In the **File format** list, select **G64x**.

8 In the **Description** field, enter a description for the exported video if necessary.

The description is shown in the *Audit trails* and file properties in the Vault.

NOTE: A description is mandatory for users without the *Single user export* privilege.

For all other users, the field is only available if the G64x format is selected, and the **Include additional properties on export/snapshot** option is enabled in the user configuration.

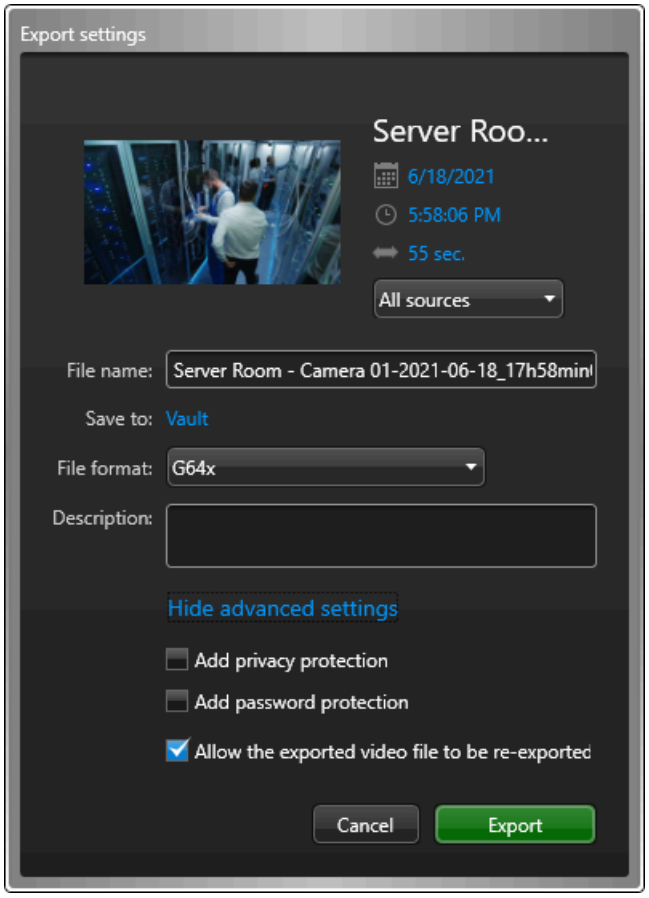
9 If you are exporting video from all tiles, do the following:

a) Select a **Playback mode**.

- **All at once:** Play back the sequences in the same tiles that they were displayed in when exported.
- **Sequential:** Play back the video in-sequence within a single tile.

b) To change the playback order of the video sequences, select a video sequence and use the and buttons.

10 If required, click **Show advanced settings** and configure as needed:



a) If you have a KiwiVision™ Privacy Protector™ license, select **Add privacy protection** to pixelate motion in the exported video. This privacy protection is always applied using default settings.

b) Select **Add password protection** and enter a password to encrypt the video file. The password must be entered to open the exported video.

NOTE: Password protected video files cannot be re-exported.

c) Select **Allow the exported video file to be re-exported** to enable all or part of the exported video to be reexported in the same or a different format.

Video files can be re-exported in Security Desk or the Genetec™ Video Player.

11 Click **Export**.

If you do not have the *Single user export* privilege, the *Authorization* window opens, and a second user with the *Export video* privilege must enter their credentials to authorize the export.

The export progress is shown in the notification tray ( ). To view the current progress or troubleshoot exporting errors, click **More** or **Show details** to open the *Export* dialog box.

If another export process is running, your export is queued and starts when the previous export has finished. When your export is complete, the video files are created in the export folder that you specified, and the files are available in the Vault.

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

Do one of the following:

- Play the exported video files on your local computer.
- Copy the exported video files so that you can share them on another computer.

Related Topics

Video export formats on page 246
Encrypting exported video files on page 274

Exporting video in G64, ASF, and MP4 formats

To create stand-alone G64, ASF, and MP4 video files that you can play without connecting to Security Center, you can export from any task in Security Desk that displays live or playback video.

Before you begin

- Review the available video export formats.
- Configure the default settings for exporting video.
- Ensure that you have the *Export video* privilege.

What you should know

- When you export a G64, ASF, or MP4 video, the system does not include additional file information, such as camera name, creation date, and camera coordinates, which can be useful for investigation. To include additional file information, export the file as G64x.
- If you lack the *Single user export* privilege, a second user with the *Export video* privilege must authorize the export.
- If another export process is running, your export is queued and starts when the current export has finished.

To export video:

1 From the Security Desk home page, open any task that can display live or playback video.

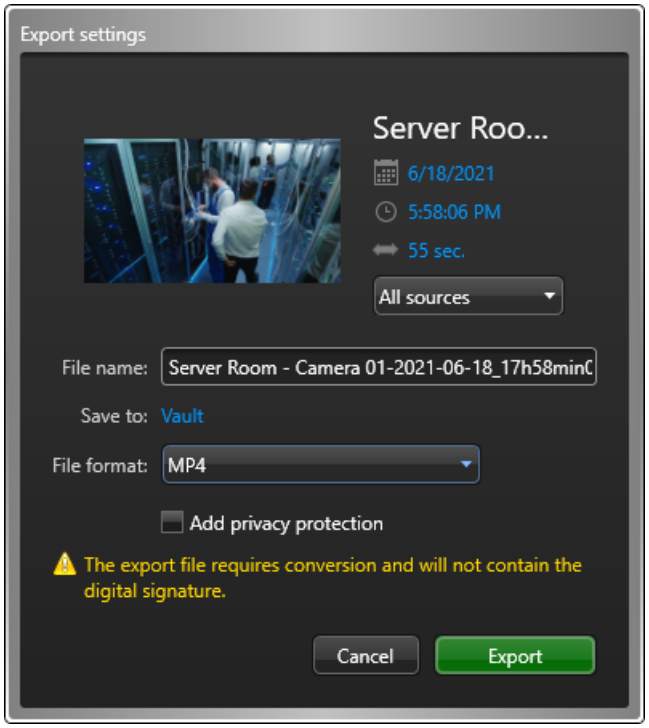
2 Select the video to export.

- After generating a report, select one or more items from the report pane, and click **Export video** ( ).
- Open video in a tile, right-click the tile, and click **Camera** > **Export video**.
- In the *Camera* widget, click **Export video** ( ).

  You can export video from the selected tile or from all tiles.

NOTE: Privacy protection is not removed from video streams during export. To export protected streams without blurring or anonymization, users with the *Remove privacy protection* privilege must remove privacy protection from the required streams before they click **Export video**.

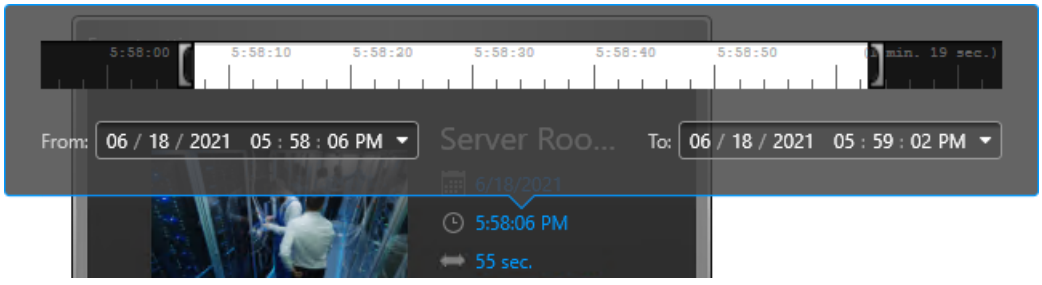
The *Export settings* dialog box opens:



3 Set the date, time, and duration of the selected video sequences:

a) Click the date, time, or duration setting.

b) Enter the date and time for the start and end of the sequence, or drag the time range markers ( ) to the desired length of time.



NOTE: You can set a maximum time range of 24 hours.

4 (Optional) To export a video sequence from a specific source, click **All sources** and select the source to export from.

5 If required, update the name of the video file in the **Filename** field.

By default, the file name includes the camera name, the date, and the duration of the video sequence.

NOTE: Multiple video sequences exported at the same time are each saved as a separate file with a unique file name.

6 (Optional) To save the video file in a specific subfolder of the Vault, click **Vault** and create or select a subfolder.

7 In the **File format** list, select **G64 (compatibility mode)**, **ASF**, or **MP4**.

8 (Optional) If you have a KiwiVision™ Privacy Protector™ license, select **Add privacy protection** to pixelate motion in the exported video. This privacy protection is always applied using default settings.

9 Click **Export**.

If you do not have the *Single user export* privilege, the *Authorization* window opens, and a second user with the *Export video* privilege must enter their credentials to authorize the export.

The export progress is shown in the notification tray ( ). To view the current progress or troubleshoot exporting errors, click **More** or **Show details** to open the *Export* dialog box.

If another export process is running, your export is queued and starts when the previous export has finished. When your export is complete, the video files are created in the export folder that you specified, and the files are available in the Vault.

After you finish

Do one of the following:

- Play the exported video files on your local computer.
- Copy the exported video files so that you can share them on another computer.

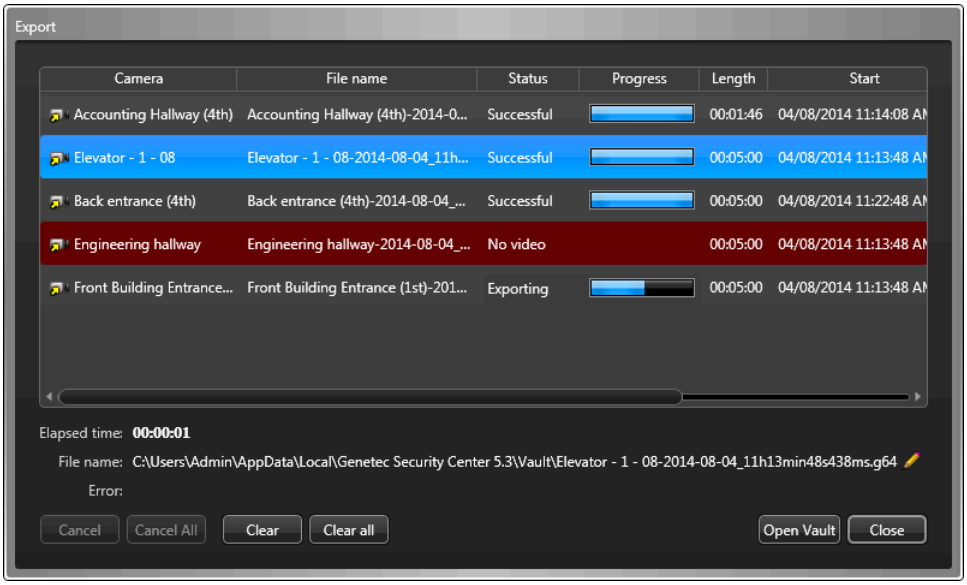
Related Topics

Video export formats on page 246

The Export video dialog box

The *Export* video dialog box opens when you are exporting video from any task in Security Desk that is displaying a playback video sequence in the canvas.

The figure that follows shows the *Export* video dialog box during the exporting video process.



The Export dialog box displays the following information about the export progress:

- **Camera:** Camera name.
- **File name:** Name of the file being exported.
- **Status:** The export status, which can be one of the following:
  - **Queued:** The export operation is queued, but has not started.
  - **Exporting:** The export is in progress. The progress is indicated by the number of bytes transferred.
  - **Converting:** If you chose to encrypt the video file or export in ASF format, this step comes after the **Exporting** step. The progress is indicated by the percentage of work completed.
  - **No video:** There is no recorded video from that camera for the selected time period.
  - **Partial export:** The export has to be aborted due to some unexpected problem. Click on the sequence to see a description of the problem in the Status field found at the bottom of the dialog box. When this happens, the remainder of the video is exported to a separate video file.
  - **Archiver server not running:** The Archiver that manages the selected video sequence is not running.
  - **Canceled:** The export operation has been canceled by the user.
  - **Successful:** The complete video sequence has been exported successfully.
  - **Error occurred:** The export operation failed. Click the sequence to see why the export failed in the Error field found at the bottom of the dialog box.
- **Progress:** The export progress
- **Length:** Total length of the video file.
- **Start:** Start time of the video sequence contained in the file.
- **End:** End time of the video sequence contained in the file.
- **Source:** The archiving source of the video sequence.
- **Elapsed time:** The total elapsed time since the export operation started.
- **File name:** Name of the file being exported. You can click **Rename** (✎) to edit the filename.

- **Error:** The error message explaining why the selected export failed or was aborted (partial export).
- **Cancel:** Interrupt the export before it completes. If the operation already started, the partial sequences that were already exported are saved as video files.
- **Cancel all:** Interrupt the export of all remaining video files. The sequences that were already exported (marked as *Successful*) are saved as video files.

Viewing exported video files

You can use the Vault tool in Security Desk to play back your exported video files on your local computer.

What you should know

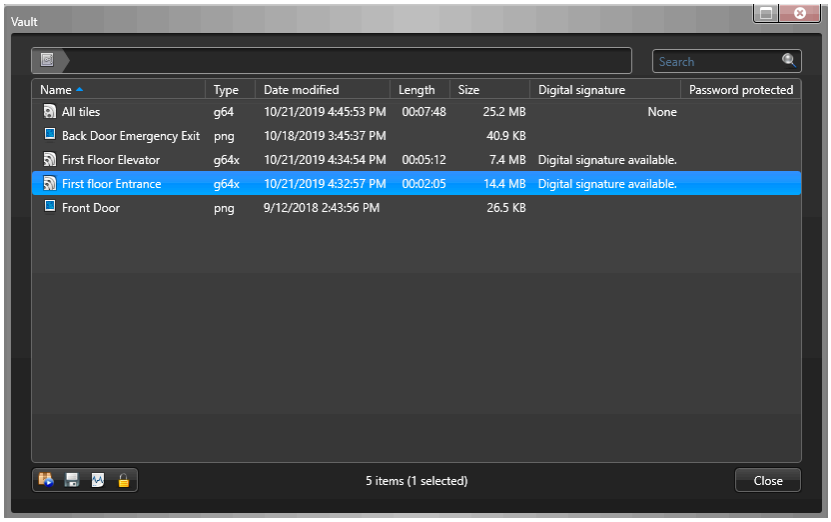
- If you exported multiple video sequences simultaneously as a G64x file, they are either played back in the same tiles that they were displayed in when they were exported, or played back sequentially within a single tile.
- If you changed the save location of exported video files, files that were exported to the original location can no longer be viewed from the Vault. You cannot drag a video file from Windows into the Vault.
- ASF files can only be viewed in Windows Media Player.
- MP4 files can be viewed in many media players such as Windows Media Player and QuickTime.

  NOTE: Some media players require a specific codec to be installed to play the file correctly.
- When you export a G64x video, the system can include additional file information, such as camera name, creation date, and camera coordinates, which can be useful for investigation. To view additional file information, right-click a file in the Vault and select **Show properties**.

  NOTE: The system only includes this additional file information if an administrator enables the feature in your user settings.

To view an exported video file from the Vault:

1 From the home page, click **Tools** > **Vault**.



The Vault displays all exported files.

2 Double-click the file you want to view.

(G64x only) If the file is password-protected, enter the password.

One of the following happens:

- If it is a G64x file, the file opens in Security Desk and plays in the canvas of the *Monitoring* task.
- If it is an ASF or MP4 file, the file opens in the media player you have installed on your system.

To view exported video files from the Genetec™ Video Player:

1 From the home page, click **Tools** > **Genetec™ Video Player** .

2 Click **File** > **Open file**, and then select the video file to view.

The video starts playing. You can control the playback using the commands at the bottom of the window.

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

Camera widget on page 39

Viewing exported files in the Video file explorer

Using the *Video file explorer* task, you can search for and play exported G64 and G64x video files and check if they are authentic.

What you should know

You do not have to be logged on to Security Center to use the *Video file explorer* task. This is helpful if you need to view an important video file but cannot log on.

TIP: Double-clicking an exported file in Windows Explorer automatically opens a new *Video file explorer* task in Security Desk. You can also drag a file from Windows Explorer directly to a tile in Security Desk.

To view an exported video file in the *Video file explorer*:

1 From the home page, open the *Video file explorer* task.

2 In the **Selector**, select a folder.

If the folder contains video files, they are listed in the report pane with the following information:

- **File name:** Name of the video file.
- **Camera:** Name of camera the video was taken from.
- **Start:** Start time of the video sequence contained in the file.
- **End:** End time of the video sequence contained in the file.
- **Time zone:** Time zone of the camera.
- **Length:** Length of the video sequence (**End time** minus **Start time**).
- **File size:** Size of the video file.
- **Digital signature:** Indicates whether or not the video file is digitally signed.
- **Encryption:** Indicates whether the video file is encrypted. If the file is encrypted, you must decrypt it before you can view it.
- **Date modified:** Date the video file was last modified.

3 Double-click or drag a video file from the report pane to the canvas.

The selected sequence starts playing immediately, and the file name and playback timestamp are displayed. The time in the timeline always represents the local time of the recorded video.

NOTE: You cannot switch to live video when you are viewing an exported file, because Security Desk does not know which camera the file is associated with.

Related Topics

Overview of the Video file explorer task on page 584

Sharing exported video files

To share your exported G64 and G64x video files with someone who does not have Security Desk installed, you can package the files with the Genetec™ Video Player, and then copy them to a CD, DVD, or USB.

What you should know

To share ASF or MP4 files, you copy the files onto a CD or DVD.

To share an exported video file:

1. From the home page, click **Tools** > **Vault**.
2. Select the video file, and click **Package with Genetec Video Player** ().
3. In the **Destination** field, select where to save the files and the *Genetec Video Player.exe*.
4. Click **Package**.
5. Navigate to the folder where you saved the files, and then copy all the files onto a CD, DVD or USB.

Example

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

Converting video files to ASF or MP4 format

Security Desk enables you to convert previously exported G64 or G64x video files to ASF or MP4 format so they can be viewed using Windows media players.

Before you begin

Configure your video export settings

What you should know

Video files exported in *ASF* or *MP4* format can be viewed using software such as Windows Media Player. You do not need Security Desk installed. This is helpful if you need to make a copy of a video recording to share with law enforcement, your legal department, or other members of your security team.

To convert a video file to ASF or MP4 format:

1 From the home page, do one of the following:
- Click **Tools** > **Vault**.
- Open the *Video file explorer* task, and select the folder that contains the video file to convert.

2 Select the video file, and click the **Save as** button ( ).

NOTE: To select multiple video files, hold the Ctrl or Shift key.

3 In the **Save as** dialog box, you can type a new **File name**, or leave the existing one.
4 From the **File format** field, choose **ASF** or **MP4**.
5 Click **Save** to start the conversion.

TIP: You can check the progress of the conversion at any time by double-clicking the **Video conversion** ( ) icon in the notification tray.

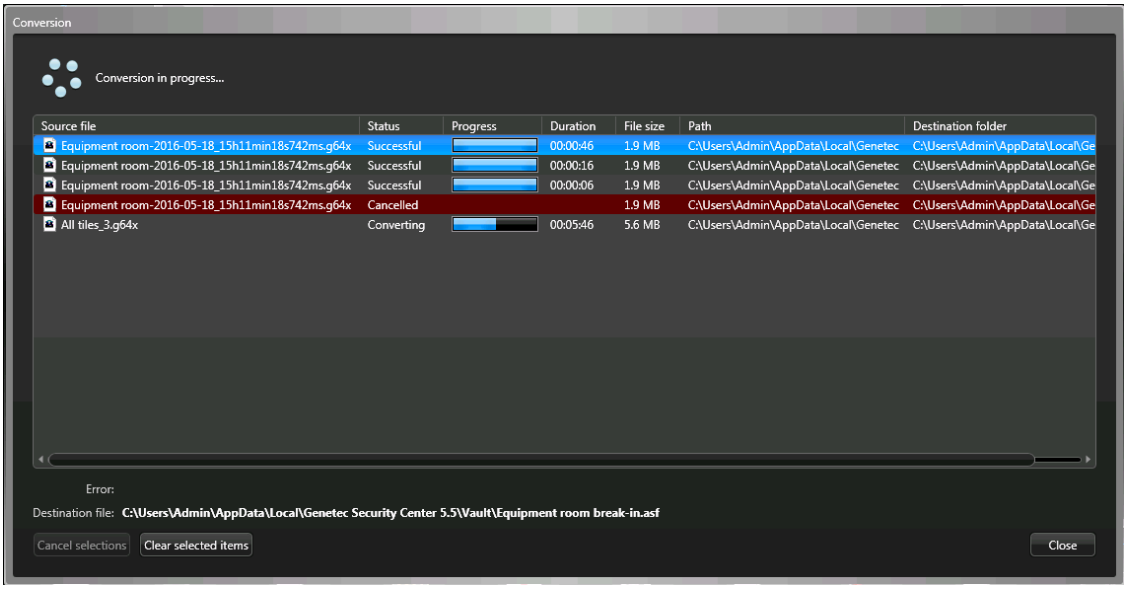
Related Topics

Video export formats on page 246

Conversion dialog box

In Security Desk, you can monitor the conversion status of G64 and G64x video files to ASF or MP4 formats from the *Conversion* dialog box.

You can open the *Conversion* dialog box by double-clicking the **Video conversion** ( ) icon in the notification tray.



The dialog box shows both the conversion queue (files waiting to be converted) and the conversion log (files that have already been converted). Each file is identified by its **File name**, the conversion **Status**, a **Progress** indicator, the **Duration** of the conversion, the original **File size**, the file **Path**, and the **Destination folder** for the converted file. The converted file keeps the name of the original file, but uses the **ASF** extension.

The possible conversion statuses are the following:

- **Queued:** The file is waiting to be converted.
- **Converting:** The conversion is in progress. The progress of the conversion is indicated in the **Progress** column.
- **Successful:** The conversion has been completed successfully. The time the conversion took is indicated in the **Duration** column.
- **Error occurred:** The conversion failed. Select the file to see the reason of the failure in the **Error** field below.
- **Canceled:** The conversion has been canceled by the user. If the conversion was canceled after it started, the conversion time is indicated in the **Duration**.

The action buttons found in the dialog box are the following:

- **Clear selected items:** Deletes the selected items from the conversion log. Only conversions that are *Successful*, *Failed*, and *Canceled* can be removed from the log. The conversion log is lost when you exit Security Desk.
- **Cancel selections:** Cancels the selected items from the conversion queue. Only conversions that are *Queued* or *Converting* can be canceled. When you cancel a conversion that has already started, the portion that has already been converted is saved.
- **Close:** Closes the conversion monitoring dialog box. The conversion process continues in the background. Closing this dialog box allows you to add more files to the conversion.

Re-exporting G64 and G64x video files

G64 and G64x files can be re-exported to create new files in Security Desk or the Genetec™ Video Player. Re-export a file to isolate a video segment, adjust settings, and save the file in a different format.

Before you begin

- Review the available video export formats.
- Configure the default settings for exporting video.
- Ensure that you have the *Export video* privilege.

What you should know

- Only G64 files and 64x files exported with the **Allow the exported video file to be re-exported** option can be re-exported.
- Starting with Security Center 5.8 GA, GEK files are no longer used to store encrypted video. Both encrypted and non-encrypted videos are now saved in G64x files.

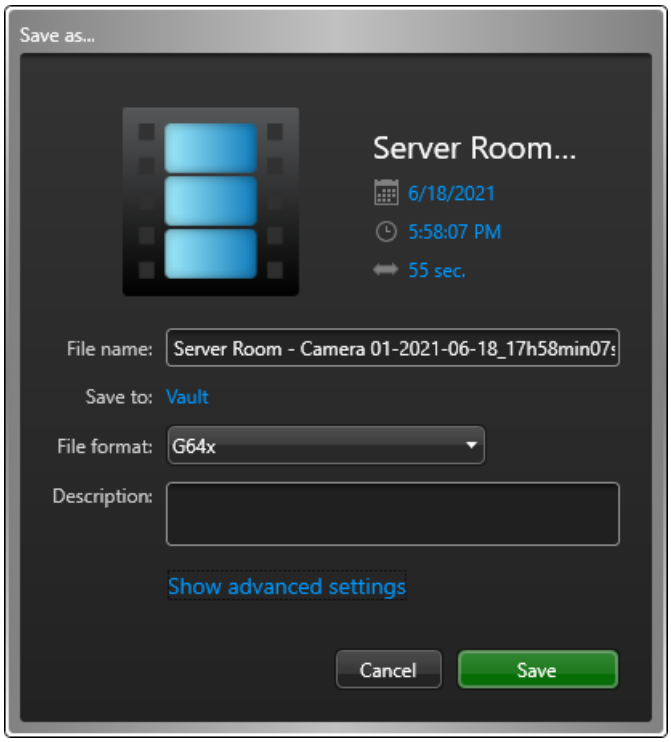
  NOTE: Security Center applications at 5.8 GA and later can read the GEK files created in earlier versions. Earlier versions of the applications cannot read the password-protected G64x files created in 5.8 GA and later.
- If a G64x file includes multiple video sequences, only one sequence can be re-exported at a time.

To re-export a video file:

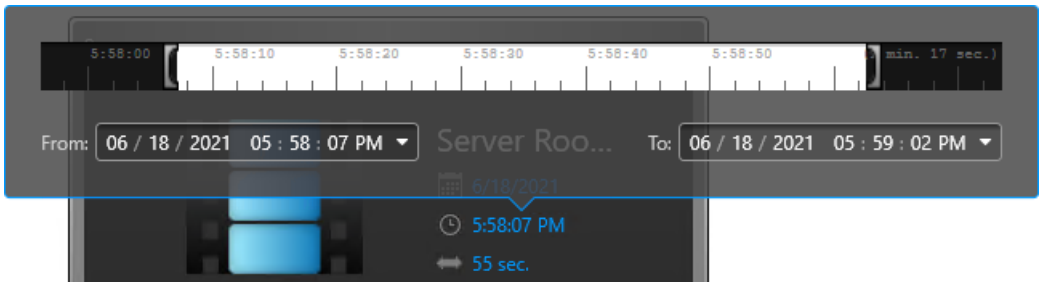
1 If you are re-exporting a video file from Security Desk:
   - Open the file in a tile, right-click the tile, and click **Camera** > **Save as**.
   - In the *Camera* widget, click **Save as** ( ).
   - Navigate to the video file in the *Video file explorer* task, select it from the report pane, and click **Save as** ( ).
2 If you are re-exporting the file from the Vault, select the file and click **Save as** ( ).
3 If you are re-exporting the file from the Genetec™ Video Player, open the file and click **File** > **Save as**.

4 In the **Save as** dialog box, set the date, time, and duration of the video sequence to re-export

a) Click the date, time, or duration.



b) Enter the date and time for the start and end of the sequence, or drag the time range markers ( ) to the desired length of time.



5 If required, update the name of the video file in the **Filename** field.
By default, the file name includes the camera name, the date, and the duration of the video sequence.

6 From the **File format** field, select the required export format.

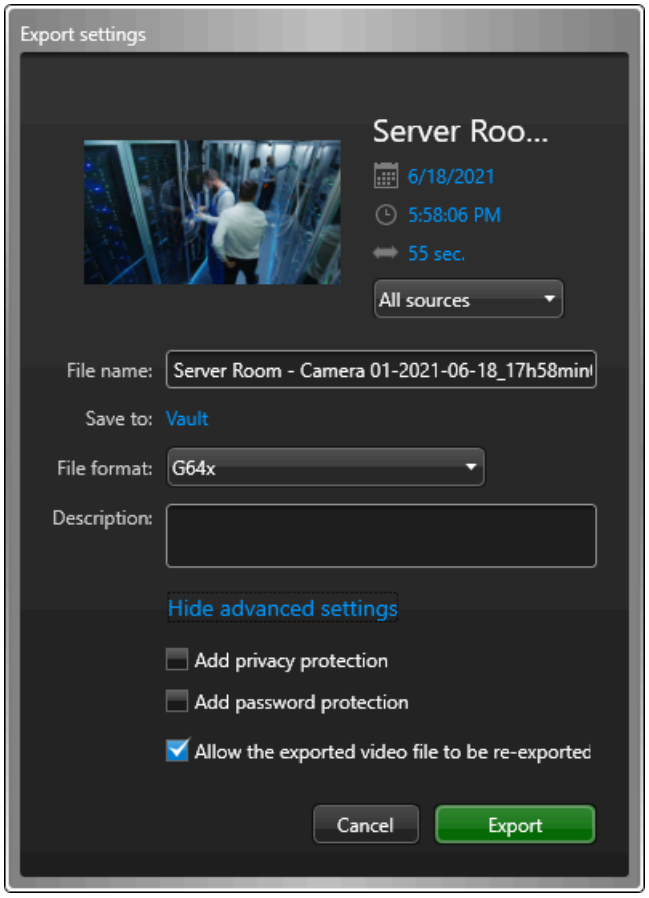
NOTE: G64x files cannot be re-exported to the G64 format.

7 In the **Description** field, enter a description for the exported video if necessary.
The description is shown in the *Audit trails* and file properties in the Vault.

NOTE: A description is mandatory for users without the *Single user export* privilege.

For all other users, the field is only available if the G64x format is selected, and the **Include additional properties on export/snapshot** option is enabled in the user configuration.

8 If you are re-exporting in G64x format, click **Show advanced settings** and configure as needed:



a) If you have a KiwiVision™ Privacy Protector™ license, select **Add privacy protection** to pixelate motion in the exported video. This privacy protection is always applied using default settings.

NOTE: Privacy protection can only be added from Security Desk or the Vault.

b) Select **Add password protection** and enter a password to encrypt the video file. The password must be entered to open the video.

NOTE: Password protected video files cannot be re-exported.

c) Select **Allow the exported video file to be re-exported** to enable all or part of the video to be re-exported again in the same or a different format.

9 (Optional) If you are re-exporting in G64, ASF, or MP4 format and you have a KiwiVision™ Privacy Protector™ license, select **Add privacy protection** to pixelate motion in the exported video. This privacy protection is always applied using default settings.

NOTE: Privacy protection can only be added from Security Desk or the Vault.

10 Click **Save**.

The export progress is shown in the notification tray ( ). To view the current progress or troubleshoot exporting errors, click **More** or **Show details** to open the *Export* dialog box.

If another export process is running, your export is queued and starts when the previous export has finished. When your export is complete, the video files are created in the export folder that you specified, and the files are available in the Vault.

NOTE: Files re-exported from the Genetec™ Video Player are only available in the Vault if they are saved to that folder location.

After you finish

Do one of the following:

- Play the exported video files on your local computer.
- Copy the exported video files so that you can share them on another computer.

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 home page, 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. The range can be defined for a specific period or for global time units, 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 272
Overview of the Archive storage details task on page 586

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.

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. For information about monitoring the disk space available for video files, see the *Security Center Administrator Guide*.

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.

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 information about archive storage, see the *Security Center Administrator Guide*.

- **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.

Encrypting exported video files

To protect your exported video files, you can create password protected versions of the files and then delete the original unprotected files.

What you should know

You can also choose to password protect all exported video as the default behavior or encrypt the file at the time of video export.

To encrypt an exported video file:

1 From the home page, do one of the following:

- Click **Tools** > **Vault**.
- Open the **Video file explorer** task, and select the folder that contains the unencrypted G64x video file.

2 Select the video file, and click **Encrypt files** ( ).

NOTE: To select multiple video files, hold the Ctrl or Shift key.

3 In the *Encryption settings* dialog box, select a **Destination** folder.

4 Enter a strong **Password**, confirm it, and then click **Encrypt**.

An encrypted version of the selected file is created.

5 (Optional) For added security, delete the original unencrypted file.

From the Vault, right-click the original file and click **Delete**.

Related Topics

Configuring settings for exporting video on page 248
Exporting video in G64x format on page 250

15

Video options

This section includes the following topics:

Configuring joysticks

You can configure any joystick (or any game controller supporting at least one axis) attached to your computer, so you can control the camera display in Security Desk.

Before you begin

Connect a joystick to your computer.

BEST PRACTICE: Do not connect two joysticks of the same model. They are listed with the same name, and you might not know which one to select. Furthermore, you can only have one joystick active at a time.

What you should know

You can associate two different Security Desk commands to each button, one for the button down event, and another for the button up event. The *Up command* is optional. The number of buttons you can configure depends on the type of joystick that you have.

The **Joystick dead zone** option value determines the percentage of movement required on the joystick before the PTZ camera starts moving. When you bring the joystick back into the home position, this value determines how close to the home position the joystick needs to be for the PTZ to stop moving.

The joystick settings apply to the local Security Desk workstation for all users.

To configure a joystick:

1. From the home page, click **Options** > **Peripherals**.
2. Click the **Joystick** tab.
3. From the **Active joystick** drop-down list, select the brand and model name of your joystick.

   You can click at any time to refresh the list.

   All axes supported by your joystick are listed below.
4. (Optional) To import a previously saved joystick configuration from a disk, click **Import**.
5. To map the joystick axis commands to the PTZ commands of your choice, do the following:
   a) Select an **Axis** from the list.
   b) From the drop-down list in the **Commands** column, select a PTZ command.
   c) To invert the command, select the option in the **Invert** column.

      Example: If you mapped the *Tilt* command to the Y axis, inverting the commands causes the camera to move up when you pull the joystick towards you, and down when you push the joystick away from you.
   d) To erase the selected command mapping, click **Clear** ().
6. To map the joystick buttons to the Security Desk commands of your choice, do the following:
   a) Select a **Button** in the list.
   b) To associate a command to a button down event, select a command from the drop-down list in the *Down command* column.
   c) To associate a command to a button up event, select a command from the drop-down list in the *Up command* column.
   d) If the selected command requires an argument, such as selecting a PTZ preset, then enter it in the **Args** column field.
7. To erase the selected command mappings and start over, click **Clear** ().
8. To set the threshold for registered movement in relation to the home position (idle zone), select a percentage value in the **Joystick dead zone** option.
9. To save the joystick configuration to disk, click **Export**.
10. Click **Save**.

Configuring CCTV keyboards

You can configure any CCTV keyboard (for example, the Axis T8310 Video Surveillance Control Board) attached to your computer, so you can control the camera display in Security Desk.

Before you begin

Connect a CCTV keyboard to your computer.

What you should know

After you connect to a CCTV keyboard, you can control PTZ monitors, switch between cameras, control playback, and so on, using the keyboard instead of your mouse.

The CCTV keyboard settings apply to the local Security Desk workstation for all users.

To configure a CCTV keyboard:

1. From the home page, click **Options** > **Peripherals** > **Keyboard** .
2. From the **Keyboard protocol** drop-down list, select the make and model of your CCTV keyboard.
3. In the *Serial port* section, configure the characteristics of the serial port where the CCTV keyboard is connected.

   This section is only required for some CCTV keyboards. Follow the specifications of the keyboard manufacturer.
4. To automatically connect to the CCTV keyboard every time Security Desk starts up, select the **Connect to keyboard automatically** option.

   If you clear this option, you'll have to connect the keyboard manually every time you want to use it.
5. Click **Connect**.

   For some CCTV keyboards, the connection status is displayed in the *Keyboard status* section.
6. To disconnect the CCTV keyboard, from the home page, click **Options** > **Peripherals** > **Keyboard** > **Disconnect**.

Customizing video stream options

You can customize video stream options, such as the default video stream for viewing live video in the canvas, the default archiving source for viewing playback video, and when to receive messages about video streams, from the *Options* dialog box.

What you should know

The **Live stream** and **Playback source** options apply to the local Security Desk workstation for all users. The **Display a warning when stream selection is not automatic** option is saved as part of your user profile.

To customize video stream options:

1. From the home page, click **Options** > **Video** > **Default options**.
2. From the **Live stream** drop-down list, select the default video stream for live video.
   - **Live:** Default stream used for viewing live video.
   - **Recording:** Stream recorded by the Archiver for future investigation.
   - **Remote:** Stream used for viewing live 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.
   - **Automatic:** Security Desk uses the *Low resolution* or *High resolution* stream, depending on the size of the tile and the zoom level.
3. From the **Playback source** drop-down list, select the default archiving source to view playback video from.
   - **Any playback source:** Let the system decide which archiving source to use.
   - **Archiver:** Video that was recorded by the Archiver.
   - **Auxiliary Archiver:** Video that was recorded by the Auxiliary Archiver.
   - **Any Federated playback source:** Let the system decide which federated archiving source to use.
   - **Federated Archiver:** Video that was recorded by the federated Archiver.
   - **Federated Auxiliary Archiver:** Video that was recorded by the federated Auxiliary Archiver.
   - **Cloud storage:** Video that was in the Cloud storage performance tier.
   - **Edge playback:** Video that was recorded on an edge recording unit.
4. Click the **User interaction** tab.
5. If you want to receive a warning message when the resolution of a displayed video image is too big for the tile, and the video stream selection is not *Automatic*, select the **Display a warning when stream selection is not automatic** option.

   The message that appears says you should change the video stream to *Automatic*.
6. Click **Save**.

Configuring automatic cleanup of the Vault

You can configure automatic deletion of files that are older than a defined number of days.

Before you begin

Make sure your Windows user account has the privileges to delete files from the Vault folder.

What you should know

- Files in the Vault are only deleted automatically if the **Automatic cleanup** option is enabled.
- Only the following file types can be automatically deleted:
  - Images: *.png*, *.jpg*, *.bmp*, and *.gif*
  - Videos: *.g64*, *.g64x*, *.gek*, *.asf*, *.asx*, and *.mp4*

  Folders are not deleted from the Vault.
- The system checks for files to delete upon Security Desk logon, and then at every subsequent hour. Files cannot be deleted if they are open during a check.

To configure automatic cleanup of the Vault:

1 From the Security Desk home page, click **Options** > **Video**.
2 In the *Vault* section, set the **Automatic cleanup** option to **ON**, and then enter a retention period from 1 - 999 days.
3 Click **Save**.

Video options

After you become familiar with how to work with video in Security Center, you can customize how video is handled by the system from the *Video* tab in the *Options* dialog box.

Seek time options

Select the default values when seeking for live and playback video. These settings are saved as part of your user profile.

- **Playback offset:** When you view an event in a tile, this value determines how many seconds of video is played before the event occurred. The default playback offset value is 15 seconds. You can set the value from 0 to 90 seconds.

  NOTE: If the *Time to record before an event* option in Config Tool has a lower value than the seek time, you might not receive any video. Ask you administrator for the *Time to record before an event* value. For more information, see the *Security Center Administrator Guide*.
- **Playback duration:** When you view an event in a tile, this value determines how many seconds of video is played. If you export the event, this value determines the length of the exported video sequence.
- **Jump backward/forward:** Determines the amount of time that a playback video recording jumps backwards or forwards when you click **Jump backward** ( ) or **Jump forward** ( ) in the camera widget.

Default options

Select the default values when playing video. These settings apply to the local Security Desk workstation for all users.

- **Live stream:** Video stream to request when playing live video.
- **Playback source:** The video source to prioritize when requesting playback video.
- **Show overlays:** Turn this option on to show video overlays by default.

Video cache options

The video cache is used to cache playback video streams received by Security Desk. Playback video is buffered before playback starts so that a sufficient length of video plays. The cache helps to reduce re-transmission of video, allows faster access to playback video, provides smoother reverse playback and additional playback speeds. The cache is emptied when you close Security Desk or log off.

These settings apply to the local Security Desk workstation for all users.

- **Cache location:** Select the location where you want the cache to be stored. You can use the default folder provided by Windows or specify your own.
- **Maximum size:** Set a size for your cache.
- **Live video caching:** Live video streams are cached separately from playback video. When the cache location is unavailable, the live video is not affected.
- **Clear cache at logoff:** Turn this option on to clear the cache when you log off Security Desk.
- **Clear cache now:** Click to clear the cache now.

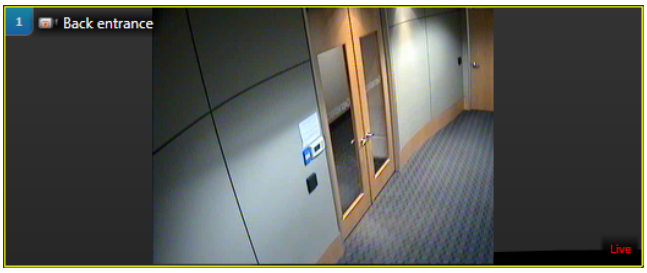
Advanced settings

The advanced video settings apply to the local workstation and affect Security Desk and Config Tool for all users.

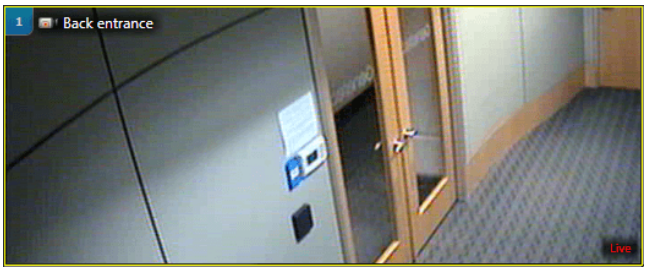
NOTE: After changing the Advanced setting options, you must restart Security Desk.

- **Jitter buffer delay:** The jitter buffer prevents rendering issues with the video stream caused by network latency variations, and provides smoother video in the event of irregular frame transmission from the source. It is recommended that you keep the buffer size at a minimum to avoid side effects such as a time lag in PTZ manipulation or an increased delay when you start to view a video stream.
- **Enable deinterlacing:** Select this option to help reduce the jagged effect around straight lines during movement in interlaced video streams.
- **Enable video quality degradation:** Select this option to prevent Security Desk from using too much CPU on your computer by lowering the frame rate of the video displayed. When the CPU is above 90%, Security Desk lowers the frame rate of the video displayed in the canvas, starting from tile number 1. MJPEG video streams are reduced to 5 fps or lower, while video streams using other types compression are reduced by showing only key frames. The video tiles affected by this option are indicated with a flashing icon ( ). To restore a video to its normal frame rate, clear the tile and restore its content (from the tile widget, click and then).

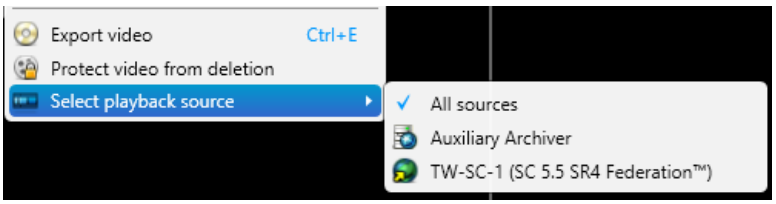
  NOTE: Whenever you change the content displayed in the canvas, Security Desk restarts lowering the video frame rate from tile #1.
- **Camera tile:** Select how cameras are displayed in tiles.
  - **Display full image (boxed):** Black strips might appear around the image if the aspect ratio of the image is not the same as that of the tile.

  - **Fill the tile (cropped):** The video image fills the tile. The image might be cropped if the aspect ratio of the image is not the same as that of the tile.

- **Audio mode:** Select the audio mode.
  - **Full-duplex:** Allows you to talk and listen at the same time.
  - **Half-duplex (push-to-talk):** Requires you to switch between talking and listening. When you click the *Talk* ( ) button in the camera widget, the *Listen* ( ) button is disabled until you release the Talk button. Half-duplex mode is necessary when two units are connected, or when audio must be controlled through digital inputs.
- **Playback filter type (context menu):** Select how Security Desk queries the playback source selected by the user.
  - **Streaming source:** (Default) The user selects the role from which to stream the video. Security Desk only queries the servers hosting the selected role. With this option, the user might see gaps in the video, if parts of the video archive have been transferred (moved) to other roles.



  - **Original archive source:** The user selects the roles that originally recorded the video. Security Desk queries all roles that have a copy of the original video recorded by the selected role. With this option, the user will not see any gaps in the video even if parts of the video archive have been transferred to other roles.
- **Hardware acceleration:** Turn this option on to allow Security Desk to offload video decoding from the main CPU to the video cards. To see what video cards are installed on your computer, click **Show hardware information**. There are also tips about how to achieve the best video decoding performance.
- **Call-up time optimization:** Turn this option on to reduce the call-up time for a group of cameras. After you enable this feature in Security Desk, you must select a sequence of cameras from the **Call-up time camera list**. Security Desk continuously streams live video from the selected cameras and allows faster video access.

  NOTE: Enabling this feature puts a burden on the system, resulting in increased bandwidth consumption on the redirector servers and extra stream request on the Archiver server.
- **Synchronize video for new tasks:** Turn this option on to open any new task with the capability to display synchronized video, such as *Monitoring*, *Archives*, and *Video file explorer*, with the synchronized video mode turned on by default.

Related Topics

Customizing snapshot options on page 207
Configuring settings for exporting video on page 248
Synchronizing video in tiles on page 197

Part III

Introduction to access control in Security Desk

This part includes the following chapters:

16

Access control at a glance

This section includes the following topics:

About Security Center Synergis™

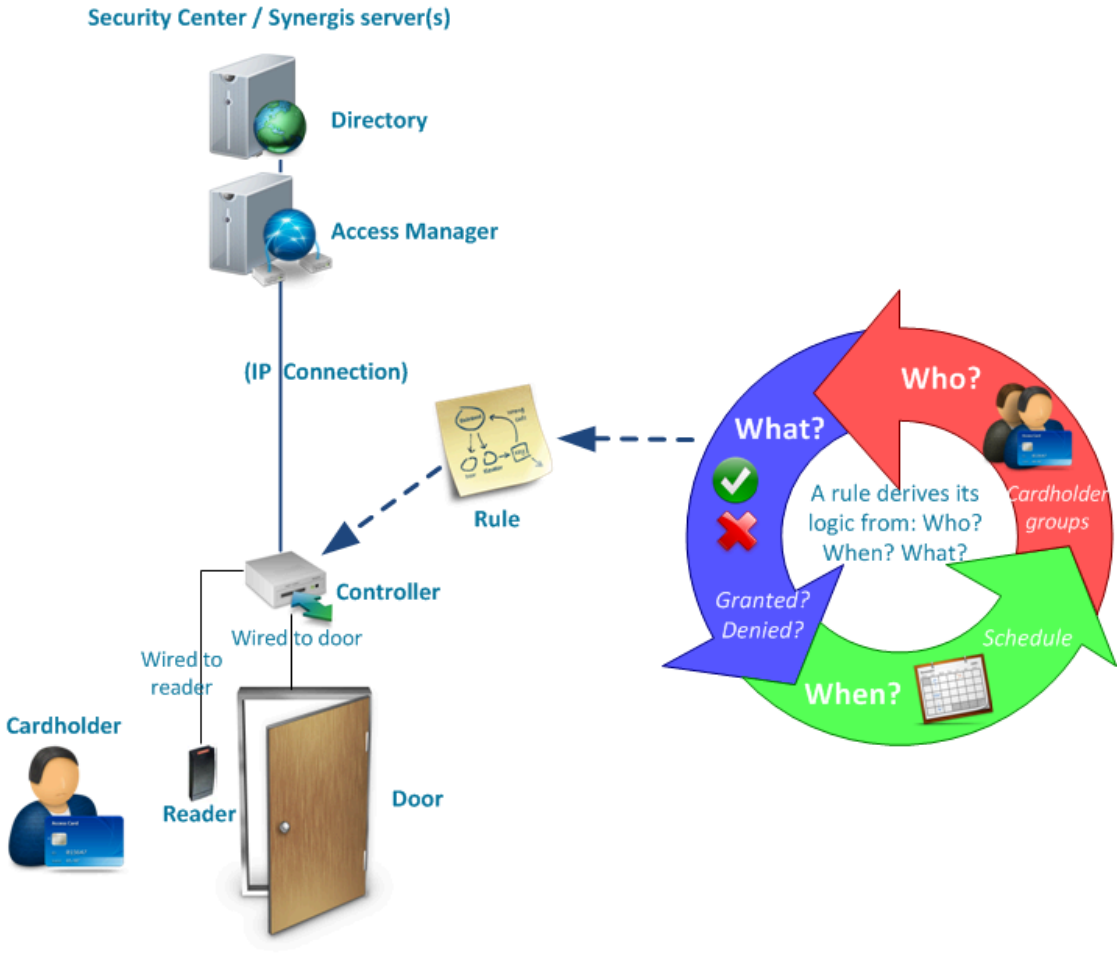
Security Center Synergis™ is the IP access control system (ACS) that heightens your organization's physical security and increases your readiness to respond to threats. Synergis™ supports an ever-growing portfolio of third-party door control hardware and electronic locks. Using Synergis™, you can leverage 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.

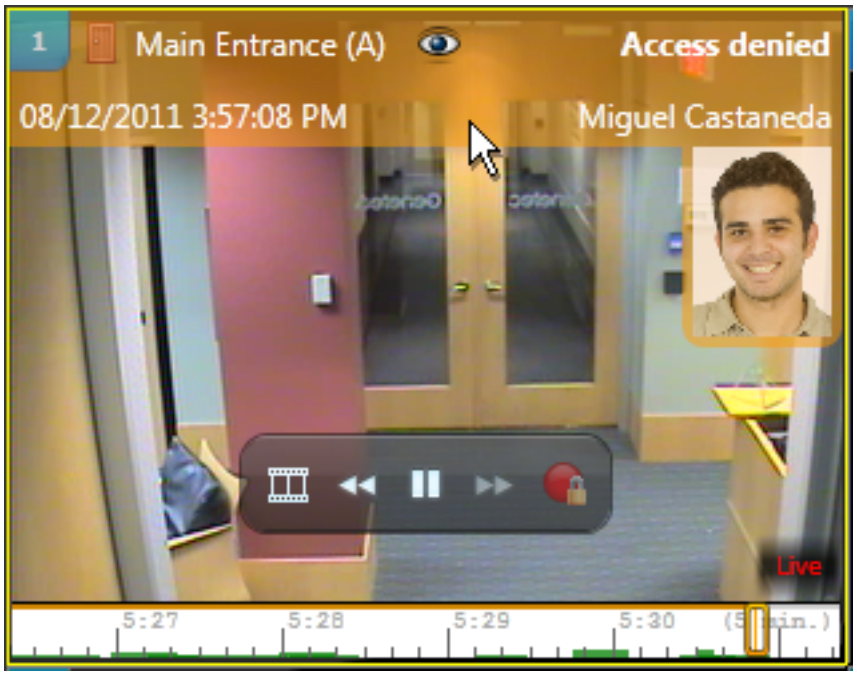
- Access Manager communicates directly with the physical door controllers, called access control units, over TCP/IP.
- Access Manager pushes schedules, cardholder information, and access rules to the door controllers.
- When a cardholder presents their credential to a reader, the controller refers to the access rule to determine whether the user should be granted or denied access.
- Once 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.

How access events are displayed in tiles

An access event (*Access granted* or *Access denied: Invalid PIN*, and so on) is any event involving an *access point*. When an access event occurs on an entity you are monitoring, information about the event is displayed in a tile in the *Monitoring* task.

The following figure is an example of an Access denied event that has occurred. The event description is displayed at the top of the tile as a colored overlay. Additional information, such as the event timestamp and the cardholder name is displayed when you place the cursor over the colored overlay. Also, you can expand the cardholder picture by placing the cursor over the picture. This might be helpful when comparing the cardholder picture to the face you see in the video.



How antipassback works

An *antipassback violation* occurs when a cardholder enters an area that they never exited, or when they exit an area that they never entered. This can occur when an authorized cardholder unlocks a door, and while entering, passes their card back to somebody else.

The Security Center administrator can configure the system to deny access to that cardholder. When this happens, you must click the **Forgive antipassback violation** ( ) button to let the cardholder in or out. For information about applying antipassback to areas, see the *Security Center Administrator Guide*.

17

Cardholders and visitors

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.

How cardholders are displayed in the Security Desk canvas

Cardholders represent people, such as employees, who can enter and exit secured areas using access cards, and whose activities can be tracked.

To view cardholder information in the canvas, drag a cardholder-related event from the report pane in the Cardholder access rights or Cardholder configuration tasks, to a tile.

A	Cardholder name.
B	Displays additional cardholder details.
C	Cardholder picture.
D	Cardholder details.

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

- To add custom information to cardholders, create custom fields in Config Tool. For more information, see the *Security Center Administrator Guide*.
- If you require different groups of cardholders with different access rights, create cardholder groups in Config ToolFor more information, see the *Security Center Administrator Guide*.
- To modify the security clearance of a cardholder, you must be granted the *Change cardholder options* and *Modify security clearance* privileges.

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 In the *Status* section, set the following:

- **Status:** Set their status to *Active* or *Inactive*. 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:** (Only available after a cardholder is deactivated) The date and time that you clicked **New** ( ) to create the cardholder.
  - **Specific date:** Activates on a specific date and time.
- **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.

6 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.

7 Assign the cardholder to a cardholder group.

NOTE: A cardholder can belong to more than one cardholder group.

a) To assign the first cardholder group, click the **Cardholder group** drop-down list and select a cardholder group.

b) To assign additional cardholder groups, click **Advanced** ( ), then click **Add an item** ( ). In the dialog box that opens, select the cardholder groups, and click **OK**.

8 Enter the cardholder's email address.

A valid email address is necessary if you want to assign *mobile credentials* to the cardholder.

9 Enter the cardholder's mobile phone number.

10 (Optional) If custom fields are defined for cardholders, such as department, phone numbers, and so on, enter the additional cardholder information.

11 (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.

To learn more about configuring areas and doors using the extended grant time and antipassback rules, see the *Security Center Administrator Guide*.

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, type 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.

12 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.

Related Topics

Cropping pictures on page 327
Applying transparent backgrounds to pictures on page 328
Overview of the Cardholder management task on page 588

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 in Config Tool (see the *Security Center Administrator Guide*).

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 > **Add** ( ).

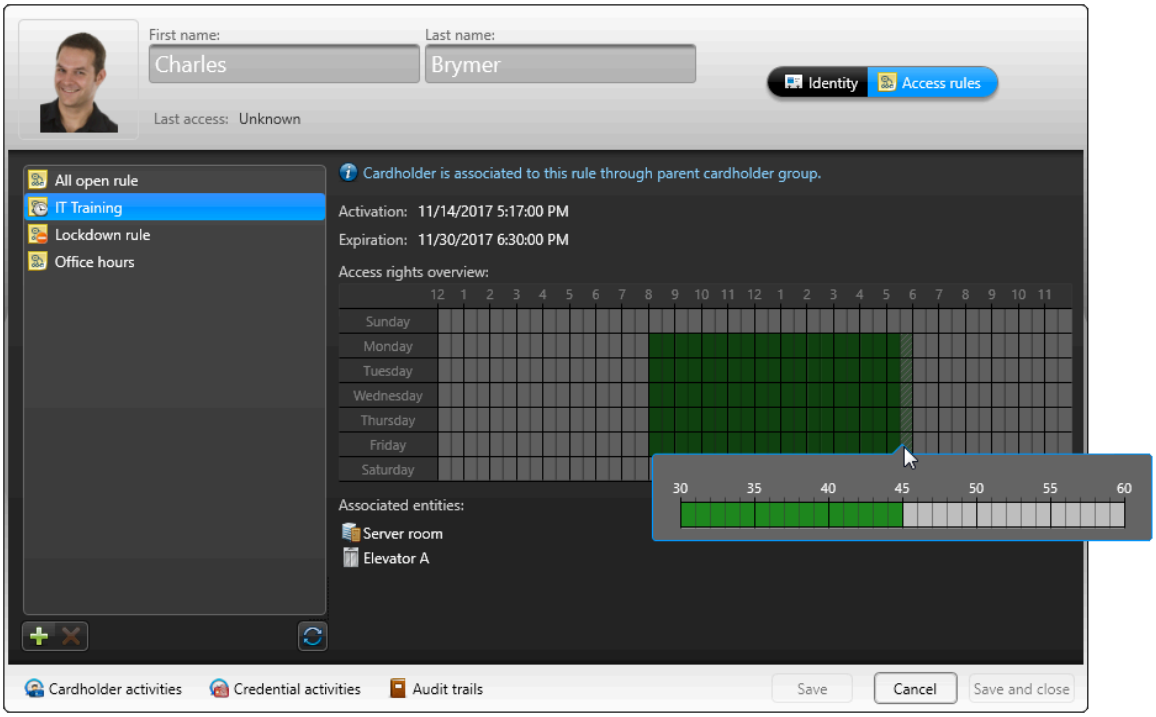
A dialog box listing the access rules that are not yet assigned to this cardholder opens.

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 30 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.



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.

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 > **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**, then select from the **Access rule** drop-down 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.

Checking in new visitors

To ensure that a visitor's activities can be monitored throughout their visit, you must check in visitors, using the *Visitor management* task. You can either pre-register visitors for later check-in, or create a visitor and check them in immediately.

Before you begin

Access rules cannot be directly associated to visitors. Therefore, to grant *access rights* to a visitor, you must create a cardholder group that is reserved for visitors in Config Tool, and assign access rules to the group. For more information about creating cardholder groups, see the *Security Center Administrator Guide*.

To check in a new visitor:

1. From the home page, open the *Visitor management* task.
2. Click **New** ( ).
3. At the top of the dialog box, enter the visitor's first name and last name.
4. To assign a picture to the visitor, 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.
5. 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.
6. In the *Status* section, set the following:

   NOTE: The *Activation* date is the same as the check-in date. You can set the activation date to a date in the future, which allows you to create visitor profiles in advance.

   - **Status:** For a visitor's credentials to work, their status must be *Active*. You can set their status to *Active* immediately by clicking **Check in** ( ), and then **Save**.
   - **Activation:** Set an activation for their profile:
     - **Never:** The default value. Use this option when you plan to check in a visitor manually or you don't know when the visitor will be arriving.
     - **Specific date:** Expires on a specific date and time.
   - **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.
7. Assign a credential to the visitor so that their movement can be tracked in the system.

   NOTE: You can assign a credential now or later.

8 Assign the visitor to a cardholder group.

Cardholder groups define which access rules apply to the visitor.

a) To assign the first cardholder group, click the **Cardholder group** list and select a cardholder group.

NOTE: Only cardholder groups configured for visitors are listed. A visitor can belong to more than one cardholder group.

b) To assign additional cardholder groups, click **Advanced** ( ), then click **Add an item** ( ). In the dialog box that opens, select the cardholder groups, and click **OK**.

9 Enter the visitor's email address.

10 Enter the visitor's mobile phone number.

11 (Optional) Assign one or two hosts (or escorts) to the visitor:

For more information about the visitor escort rule, see the *Security Center Administrator Guide*.

a) Click the **Visitor host** list and select a cardholder as the visitor's host.

A dialog box opens displaying the message *Do you wish to automatically enable the Escort required option?*

b) Click **Yes** to turn on the **Escort required** option.

When the option is on, the visitor is not allowed to access certain areas unless their assigned hosts also present their credentials after them within a certain delay.

c) (Optional) To assign a second host, click **Advanced** ( ), then click **Add an item** ( ). In the dialog box that opens, select a cardholder to assign as host and click **OK**.

NOTE: The order in which the hosts present their credentials is not important.

12 (Optional) Enter a date and time into the **Expected arrival** field.

13 (Optional) If custom fields are defined for visitors, enter the additional visitor information.

14 (Optional) In the *Advanced* section, configure the following visitor properties:

NOTE: Some of these properties can be inherited from the parent cardholder groups. When a specific value is configured for the visitor, 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 visitor has been assigned a credential, grant access privileges to the visitor.

- **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.
- **Bypass antipassback rules:** Exempts them from all antipassback restrictions.

To learn more about configuring areas and doors using the extended grant time and antipassback rules, see the *Security Center Administrator Guide*.

b) In the **Security clearance** field, enter the visitor'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, type a new name for the visitor entity, if you do not want to use the visitor's first and last name.

By default, the **Entity name** uses the **First name** and **Last name** fields.

d) (Optional) In the **Description** field, type a description for the visitor.

e) Assign the visitor 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 visitor.

15 Do one of the following:

- To pre-register a visitor to be checked in later, click **Save**.
- To check in the visitor immediately, click **Save and check in**.

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

Overview of the Visitor management task on page 590

Checking in returning visitors

If a visitor returns to your site, you can check in the visitor without having to re-enter their information, because all checked-out visitors are saved in the database.

What you should know

If the visitor was previously assigned a credential, you must assign a new credential after the visitor is checked in.

To check in a returning visitor:

1 In the *Visitor management* task, click **New** ( ).

2 At the top of the dialog box, enter the visitor's first name or last name.

If a match is found in the visitor database, a green button showing the number of potential matches appears ( ).

3 Click the green button.

A **Visitors** dialog box opens, listing all potential matches found in the database.

4 (Optional) To filter the visitor list, do one of the following:

- Type a visitor's first name or last name, and then click **Search**.
- Select the visitor's check-in, expiration, or expected arrival date, and then click **Search**.
- Click **Click to edit**, select a visitor custom field, click **OK**, and then click **Search**.

5 Select a visitor, and then click **Select**.

The information of the selected visitor is loaded into the visitor dialog box.

6 Modify the visitor information as needed, and then do one of the following:

- To pre-register a visitor to be checked in later, click **Save**.
- To check in the visitor immediately, click **Save and check in** ( ).

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

If the visitor requires a credential, assign one.

Assigning an additional visitor host for areas with turnstiles

You can set a second host for visitor delegations to turnstile-accessible areas. This feature lets you set one host at the head of a delegation and the other to tail the visitors. For a delegation with a set limit, a second host is required if the visitor number exceeds that limit.

What you should know

- This procedure applies to visitor escort for turnstiles in delegation mode.

  NOTE: *Delegation* mode is not to be confused with *single passage enforcement* mode. For more information about this mode, see the *Synergis™ Softwire Single Passage Enforcement Technote*.
- A delegation consists of one or two hosts and one or more visitors.
- If your visitor delegation is at its configured limit for a single host, adding an additional visitor will trigger the warning "Single host visitor limit exceeded. Assign a different host or add a second one," and require you to either start a new delegation or to assign a second host to the expanded delegation.

To add a second host:

1 Click **Advanced** (⊕), then click the **Visitor host** drop-down list.

2 Do one of the following tasks:

- Add a second host to the delegation
  a. From the **Visitor host** list, select a cardholder as the second host.
  b. Select the **Escort required** option.
  c. Click **Save**. In the dialog box that opens, confirm that you want to add a second host to the delegation.

  NOTE: When adding a second host to an existing delegation, the second host is assigned to all cardholders in that delegation.
- Start a new delegation
  a. Delete the assigned host by clicking **Clear selection** at the bottom of the **Visitor hosts** list.
  b. Select a new host from the list.

How visitor escort for turnstiles in delegation mode works

With the visitor escort rule, host and visitor badging at a turnstile follows a strict order.

For visitor escort for turnstiles in delegation mode, the badge-and-entry sequence is as follows:

1. The host badges and enters.
2. The first visitor badges and enters.
3. The next visitor badges and enters. This sequence continues until the last visitor has entered.
4. If there is a second host, the host badges and enters.

If the badging order between host and visitor is not respected, it can trigger any of the following events:

- *Access denied: a valid host is required* is triggered if a visitor badges before the host.
- *Visitor astray*: if the host badges and enters without the visitor(s), then this event is triggered for each visitor, including a *Missing tail host* event if a second host was configured.
  - *Visitor astray* is also triggered if a visitor does not badge after the host enters, or if the tail host badges before the last visitor.
- *Missing tail host* is triggered if the tail host in a two-host delegation does not badge.

NOTE: The badging order of the hosts is not important, as long as one badges and enters before the first visitor, and the other badges and enters last.

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:

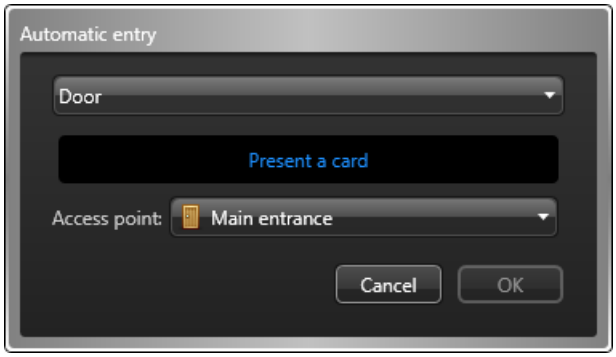
- For cardholders, open the *Cardholder management* task, select a cardholder, and then click **Modify** ( ).
- For visitors, open the *Visitor management* task, select a visitor, and then click **Modify** ( ).

2 In the *Credential* section, click **Add a credential** ( ).

3 Select one of the following options:

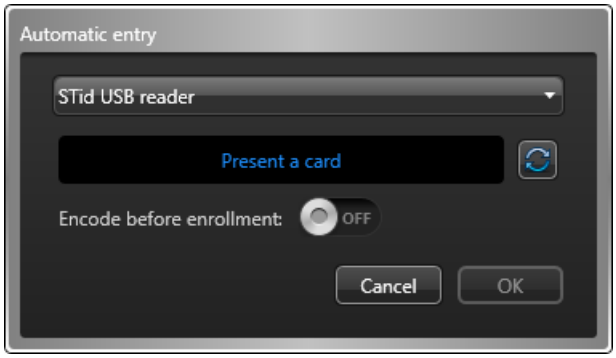
- **Automatic entry:** Present the card at a reader.
- **Manual entry:** Manually enter the card data. Use this method when you do not have a card reader near you.
- **Existing credential:** Select a pre-enrolled, unassigned credential.
- **PIN:** Create a PIN credential.
- **License plate:** Enter a 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**, then select a reader (USB reader or a door) and present the card at the reader.



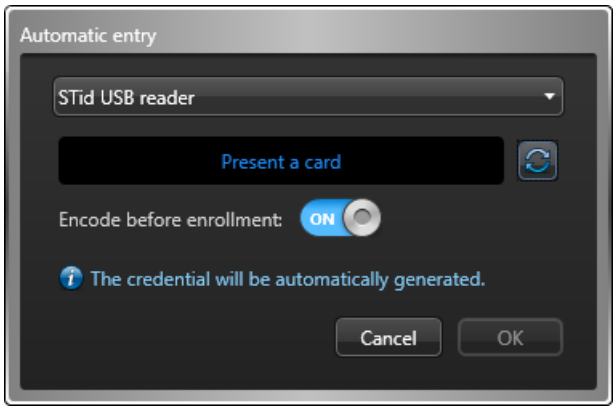
If you have a smart card encoding reader set up, do one of the following:

- To read a pre-encoded card, set the option **Encode before enrollment** to **OFF**. 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.



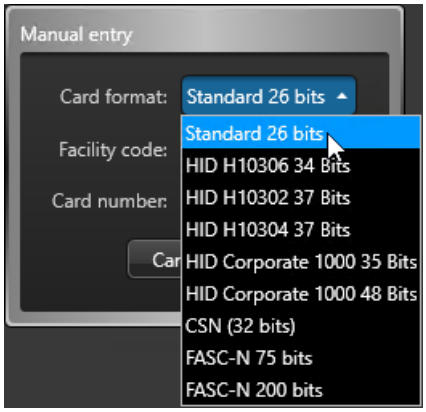
- To generate and encode on your card a random 128-bit MIFARE DESFire credential before enrolling it, set the option **Encode before enrollment** to **ON**. When the reader LED turns red (ready to encode), place the smart card on the reader for approximately 2 seconds. The reader LED turns yellow and 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.



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**.

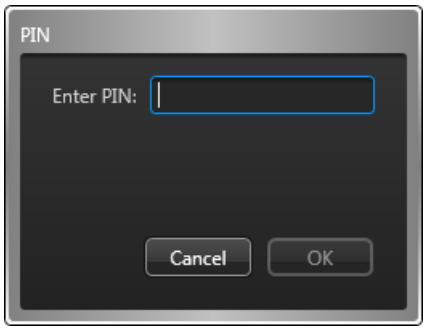


CAUTION: Enter your card data carefully because the system cannot validate whether the data you entered correspond to a physical card or not.

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:

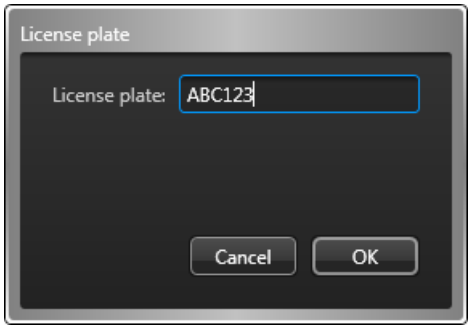


a) Enter the PIN as a numerical value.

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:

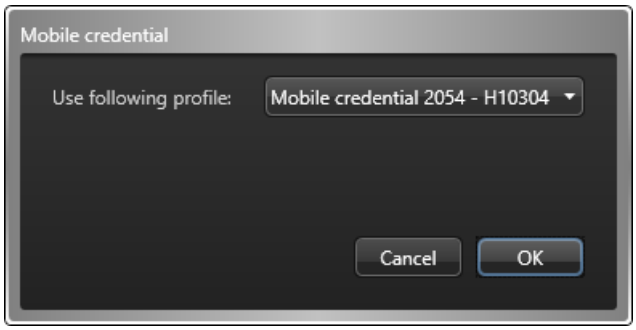


a) Enter the license plate number.

NOTE: You do not need to enter spaces that appear 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:



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**.

Badge templates are created in Config Tool. For more information, see the *Security Center Administrator Guide*.

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.

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.

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** drop-down list, select a badge template.

You only need to select a badge template if you want a badge to be printed. Badge templates are created in Config Tool. For information, see the *Security Center Administrator Guide*.

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

Responding to credential card requests on page 349

Printing credential cards in batches

To save time when printing credential cards, you can print them in batches.

What you should know

All the credentials you select must be associated with a badge template.

For information about creating badge templates, see "Designing badge templates" in the *Security Center Administrator Guide*.

To print credential cards in batches:

1 From the home page, 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.

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.

For information about creating badge templates, see the *Security Center Administrator Guide*.

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**.

Assigning temporary cards

If a cardholder or visitor's card credential is reported as lost or stolen, you can replace it with a temporary card and mark the original card as lost.

Before you begin

Make sure that you have the following:

- A card reader nearby.
- A stack of pre-enrolled spare cards. You can enroll a large quantity of cards at once using the Credential management task.

To assign a temporary card to a cardholder or visitor:

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 **Assign temporary card**.
3 From the drop-down list, select a card reader near you.
   The card reader can be a **USB** connected to your computer, or you can use an **Access point** (door).
4 Present a spare card that is pre-enrolled.
5 Set the number of days the temporary card is to remain active, and click **Assign temporary card**.
6 Click **Save**.

After this operation, the original card is marked as **Lost**, but remains assigned to the cardholder. The temporary card is activated for the specified number of days, and assigned to the same cardholder. The cardholder now has at least two cards. A permanent one that is lost, and a temporary one that is active.

Example

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

Restoring original cards to cardholders and visitors

When a lost card is found, you can restore the original card and remove the temporary card assignment.

Before you begin

Make sure you have a card reader nearby.

What you should know

To restore the original card, the cardholder or visitor must return both the original and the temporary card.

CAUTION: When a cardholder has more than one temporary card, returning the temp card restores the original card to the cardholder. The return temporary card functionality can be used only once per cardholder.

To restore an original card to a cardholder or visitor:

1 In the *Cardholder management* or *Visitor management* task, click **Return card** ( ).

2 From the drop-down list, select a card reader near you.

The card reader can be a **USB Reader** connected to your computer, or you can use an **Access point** (door).

3 Present both the original and the temporary cards; the order is not important.

4 If both cards match the same cardholder, click **Restore original card** to restore the status of the original card to **Active**, and deactivate the temporary card.

The temporary card can now be assigned to someone else.

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.

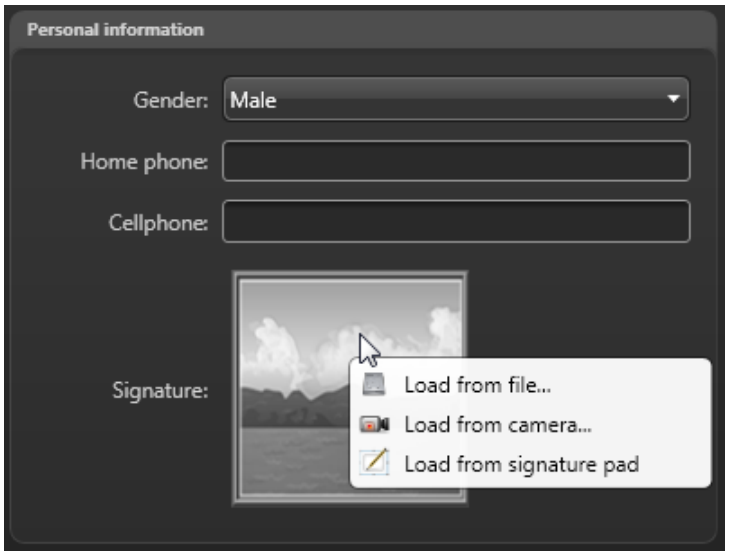
Before you begin

- 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**.



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**.

Checking out visitors

You must check out visitors when they leave.

To check out a visitor:

1 In the *Visitor management* task, select the visitor from the visitor list.

If the visitor list is long, use the search features to find the visitor name.

NOTE: You can check out multiple visitors at the same time by holding down the shift key and selecting the visitors you want to check out.

2 Click **Check-out** ( ).

The checked-out visitor is removed from the visitor list, but remains available for investigation reports. The visitor's information is also saved in the database, and can be used if the visitor returns.

If the visitor was assigned a credential, the credential status switches to *Unassigned,* and can be assigned to another visitor or cardholder. The credential is also removed from all access controllers it was synchronized with. This might take a few seconds.

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

Investigating visitor events on page 312
Overview of the Visitor management task on page 590

Deleting visitors

Pre-registered visitors who have not yet checked in cannot be checked out, but they can be deleted.

To delete a visitor:

1 In the *Visitor management* task, select the visitor from the visitor list.

If the visitor list is long, use the search features to find the visitor name.

NOTE: You can delete multiple visitors at the same time by holding down the shift key and selecting the visitors you want to delete.

2 Click **Delete** ( ).

The deleted visitor is removed from the database.

Investigating cardholder events

You can investigate events related to cardholders (Access denied: Invalid PIN, First person in, Last person out, Antipassback violation, and so on), using the *Cardholder activities* report.

What you should know

For example, if you want to see which areas, doors, and elevators a cardholder has access in the last day or week, you can search for that specific cardholder, and set a time range for your report. If there has been suspicious activity on your site in the last day, you can investigate which cardholders were denied access to an area by selecting the area, and the *Access denied* event.

To investigate cardholder events:

1 From the home page, open the *Cardholder activities* task.

2 Set up the query filters for the report. Choose from one or more of the following filters:

- **Cardholders:** Restrict the search to specific cardholders, cardholder groups, or visitors.

  NOTE: If you only select the *All cardholders* cardholder group, federated cardholders are not included. This is because *All cardholders* is a local cardholder group that only covers local cardholders.
- **Credential:** Restrict the search to specific credentials.
- **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.
- **Doors - Areas - Elevators:** Restrict the search to activities that took place at certain doors, areas, and elevators.
- **Events:** Select the events of interest. The event types available depend on the task you are using.
- **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.

3 Click **Generate report**.

The cardholder events are listed in the report pane.

4 Show the corresponding video of an event in a tile by double-clicking or dragging the item from the report pane to the canvas.

If there is no camera attached to the entity, the door, elevator, or area icon is displayed, depending on the type of cardholder event.

5 Control the tiles using widgets in the *Controls* pane.

Report pane columns for the Cardholder activities 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 activities task.

- **Event:** Event name.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **Location:** Location (area) where the activity took place.
- **Access point:** Access point involved (only applicable to areas, doors, and elevators).
- **Credential:** Credential name used by the cardholder.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door or elevator.
- **Event timestamp:** Date and time that the event occurred.
- **Card format:** Credential card format.

- **Cardholder:** Cardholder entity name.
- **Credential code:** Facility code and card number.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Email address:** Cardholder or visitor's email address.
- **IP address:** IP address of the unit or computer.
- **License plate exact match:** Indicates whether or not the license plate read associated with the cardholder exactly matches a license plate credential in Security Center.
- **Mobile phone number:** Cardholder or visitor's mobile phone number.
- **Occurrence period:** Period when the event occurred.
- **Product type:** Model of the unit.
- **Time zone:** Time zone of the unit.
- **Unit:** Name 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.

Investigating visitor events

You can investigate events related to visitors (access denied, first person in, last person out, antipassback violation, and so on), using the *Visitor activities* report.

What you should know

In Security Desk, you can see all the areas and doors that a visitor accessed during their stay. If you want to check for any critical events that occurred on your site in the last day in relation to visitors, you can set a time range for the report.

To investigate visitor events:

1 From the home page, open the *Visitor activities* task.

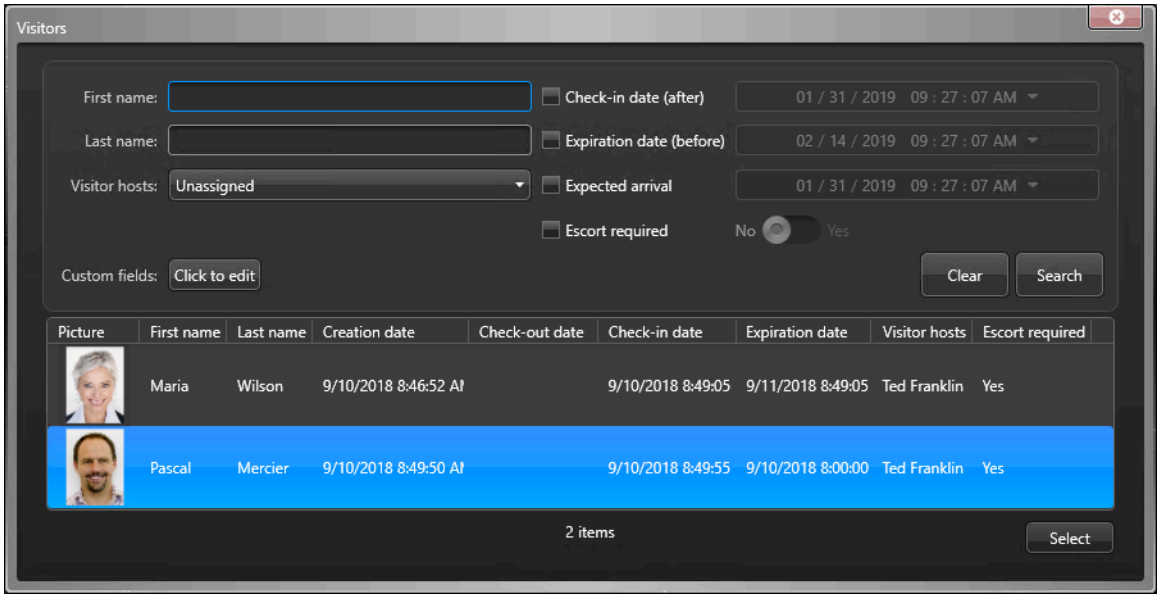
2 In the *Visitor* query filter in the *Filters* tab, click .

3 In the **Visitors** dialog box, filter the visitor list in one of the following ways:

- Type a visitor's first name or last name, and then click **Search**.
- Select the visitor's activation, expiration, or expected arrival date, and then click **Search**.
- Select the visitor's host, and then click **Search**.
- Click **Click to edit**, select a visitor custom field, click **OK**, and then click **Search**.

4 Select a visitor to investigate.

You can only specify one visitor at a time.



5 Click **Select**.

6 Set up the other query filters for your report. Choose one or more of the following filters:

- **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.
- **Doors - Areas - Elevators:** Restrict the search to activities that took place at certain doors, areas, and elevators.
- **Events:** Select the events of interest. The event types available depend on the task you are using.
- **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.

7 Click **Generate report**.

The visitor events are listed in the report pane.

8 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If there is no camera connected to the entity, the door, elevator, or area icons are displayed, depending on the type of visitor event.

9 To control the tiles, use the widgets in the *Controls* pane.

Report pane columns for the Visitor activities task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Visitor activities task.

- **Event:** Event name.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Location:** Location (area) where the activity took place.
- **Access point:** Access point involved (only applicable to areas, doors, and elevators).
- **Event timestamp:** Date and time that the event occurred.
- **Picture:** Cardholder or visitor's picture.
- **Visitor hosts:** Cardholders assigned as visitor escorts.
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Email address:** Cardholder or visitor's email address.
- **IP address:** IP address of the unit or computer.
- **Mobile phone number:** Cardholder or visitor's mobile phone number.
- **Occurrence period:** Period when the event occurred.
- **Product type:** Model of the unit.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door or elevator.
- **Time zone:** Time zone of the unit.
- **Unit:** Name 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.

Counting people

You can view the number of cardholders that are currently in secured areas on your system, using the *People counting* task. This is also useful for removing people from areas of which they are mistakenly listed as occupants.

What you should know

The number of cardholders present in a selected area is updated in real time as people move in and out of the area.

For the report to be accurate, the selected area must be fully secured, meaning that people should not be allowed to enter or exit the area without swiping their card. Readers should be installed on both sides of a door (no *REX's*), and cardholders must pass through the door one by one (no *tailgating*). Turnstiles are often used for this purpose.

To count the number of cardholders in an area:

1 From the home page, open the *People counting* task.

2 In the *Selector*, select an area.

The cardholders present in that area are listed on the right.

3 To launch an investigation report on a selected cardholder, click **Investigate** ( ).

4 To remove a selected cardholder from the area you are viewing, click **Remove from area** ( ).

5 To reset the people count to zero for the selected area, click **Clear all**.

The cardholders that you removed using either the **Remove from area** command or the **Clear all** command, are automatically forgiven one antipassback violation the next time they badge their card. This allows them to re-enter the area they have been removed from.

Example

If you see suspicious activity while monitoring a live video feed, you can use *people counting* to see cardholders that are currently in that area. If there is a fire in your building, you can use *people counting* to see if there is anyone left in an area of the building.

Related Topics

Tracking cardholders present in an area on page 316

Using People counting to track and remove cardholders from areas

If a cardholder tailgates out of an area or is otherwise mistakenly listed as an occupant, you can remove them from that area using the *People counting* task's **Search** field.

What you should know

The cardholder search examines the area name, first name and last name; you can use any name as a search term.

To find a cardholder in an area:

1 From the *People counting* task, enter the cardholder's name in the **Search** field at the top of the canvas. The result autocompletes as you type.

You can also enter partial text. For example, entering "mit" brings up "Smith."

2 Select the cardholder and click **Remove from area**.

The cardholder is removed from the area and forgiven one antipassback violation the next time they badge their card.

Tracking cardholders present in an area

You can see how many cardholders and visitors are currently present in a selected area, and how long they have been there, using the *Area presence* report.

What you should know

For the report to be accurate, the selected area must be fully secured, meaning that people should not be allowed to enter or exit the area without swiping their card. Readers should be installed on both sides of a door (no *REX's*), and cardholders must pass through the door one by one (no *tailgating*). Turnstiles are often used for this purpose.

To track which cardholders are present in an area:

1 From the home page, open the *Area presence* task.

2 Set up the query filters for the report. Choose one or more of the following filters:

- **Areas:** Select the areas to investigate.

  NOTE: You must select a fully secured area.
- **Cardholders:** Restrict the search to specific cardholders, cardholder groups, or visitors.
- **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 cardholders and visitors currently in the selected area are listed in the report pane.

4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If the area is not associated to a URL or a map file through a tile plugin, the area icon is displayed.

5 To control the areas, use the area widget.

Related Topics

Counting people on page 314

Report pane columns for the Area presence task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Area presence task.

- **Area:** Area name.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Last access:** Time the cardholder entered the area.
- **Picture:** Cardholder or visitor's picture.
- **Cardholder:** Cardholder entity name.
- **Email address:** Cardholder or visitor's email address.
- **Mobile phone number:** Cardholder or visitor's mobile phone number.
- **Cardholder groups:** Cardholder groups that the cardholder or visitor belongs to.
- **Visitor hosts:** Cardholders assigned as visitor escorts.
- **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.

Tracking attendance in an area

Find out which cardholders and visitors have been inside a selected area, and the total duration of their stay within a given date range, using the *Time and attendance* report.

What you should know

This report displays the total time spent in the selected area by each selected cardholder and visitor, for each day covered by the date range. For example, if something happened in an area two days ago, you can find out who was in that area during that day by selecting the area and the date range.

For the report to be accurate, the selected area must be fully secured, meaning that people should not be allowed to enter or exit the area without swiping their card. Readers should be installed on both sides of a door (no *REX's*), and cardholders must pass through the door one by one (no *tailgating*). Turnstiles are often used for this purpose.

NOTE: The time zone of the access control unit is used for this report.

To investigate the duration of a cardholder or visitor's stay:

1 From the home page, open the *Time and attendance* task.

2 Set up the query filters for the report. Choose from one or more of the following filters:

- **Areas:** Select the areas to investigate.

  NOTE: You must select a fully secured area.
- **Cardholders:** Restrict the search to specific cardholders, cardholder groups, or visitors.
- **Time range:** The date range for the report.
- **Start of day:** The time you want the day to reset every day. For example, you can set the day to start at 8 pm to account for night shifts that span over two days.
- **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 total time spent in the selected area by each selected cardholder and visitor, for each day covered in the selected date range, are listed in the report pane.

Report pane columns for the Time and attendance task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Time and attendance task.

- **Date:** The date.
- **Weekday:** Weekday corresponding to the date.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **Area:** Area name.
- **Total time:** The amount of time from the first entry to the last exit that the cardholder or visitor spent in the area, minus the time that they were not in the area. For example, if an employee badged out of the area to take a lunch break for an hour, this hour would not be calculated in the **Total time**.
- **First-in time:** The time of the cardholder or visitor's first entry into the area during the day.
- **Last-out time:** The time of the cardholder or visitor's last exit out of the area during the day.
- **Gross total time:** The amount of time from the first entry to the last exit that the cardholder or visitor spent in the area, including the time that they were not in the area.
- **Cardholder groups:** Cardholder groups that the cardholder or visitor belongs to.

- **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.

Tracking the duration of a visitor's stay

You can investigate the stay time of current and past visitors, between check-in and check-out, using the *Visit details* report.

What you should know

If you want to know if a visitor checked out before they left at the end of the day, you can investigate that visitor, and see if the *Check-out date* column in the report pane is completed. You can also see which visitors were added or removed from the system in the last week.

To track the duration of a visitor's stay:

1 From the home page, open the *Visit details* task.

2 Set up the query filters for your report. Choose one or more of the following filters:

- **Check-in date:** The date and time that the visitor profile was activated, which can correspond to the arrival time.
- **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.
- **Escort required:** Specify that a host is required.
- **Expected arrival:** Specify a time range during which the visitor is expected to arrive.
- **Expiration date:** Specify a time range during which the cardholder or visitor profile expires.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Status:** The status of the cardholder or visitor's profile: *Active* or *Archived*.
- **Visitor hosts:** Select the visitor's host.

3 Click **Generate report**.

The visitor events are listed in the report pane.

4 To show a visitor's picture, name, and custom fields in a tile, double-click or drag an item from the report pane to the canvas.

5 To display additional visitor information in a tile, click  .

Report pane columns for the Visit 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 Visit details task.

- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **Check-in date:** Date and time the visitor's profile was activated (can correspond to arrival time).
- **Expiration date:** Date and time the cardholder or visitor profile expires.
- **Creation date:** Date and time that the visitor's profile was created.
- **Check-out date:** Date and time the visitor was checked out (can correspond to the departure time).
- **Visitor hosts:** Cardholders assigned as visitor escorts.
- **Escort required:** Indicates whether a visitor host is required.
- **Expected arrival:** Date and time of the visitor's expected arrival.
- **Visit duration:** The time between check-in and now for a checked-in visitor; the time between check in and check out for a checked-out visitor. For a pre-registered visitor who has not yet checked in, this column entry is blank.

- **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 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.

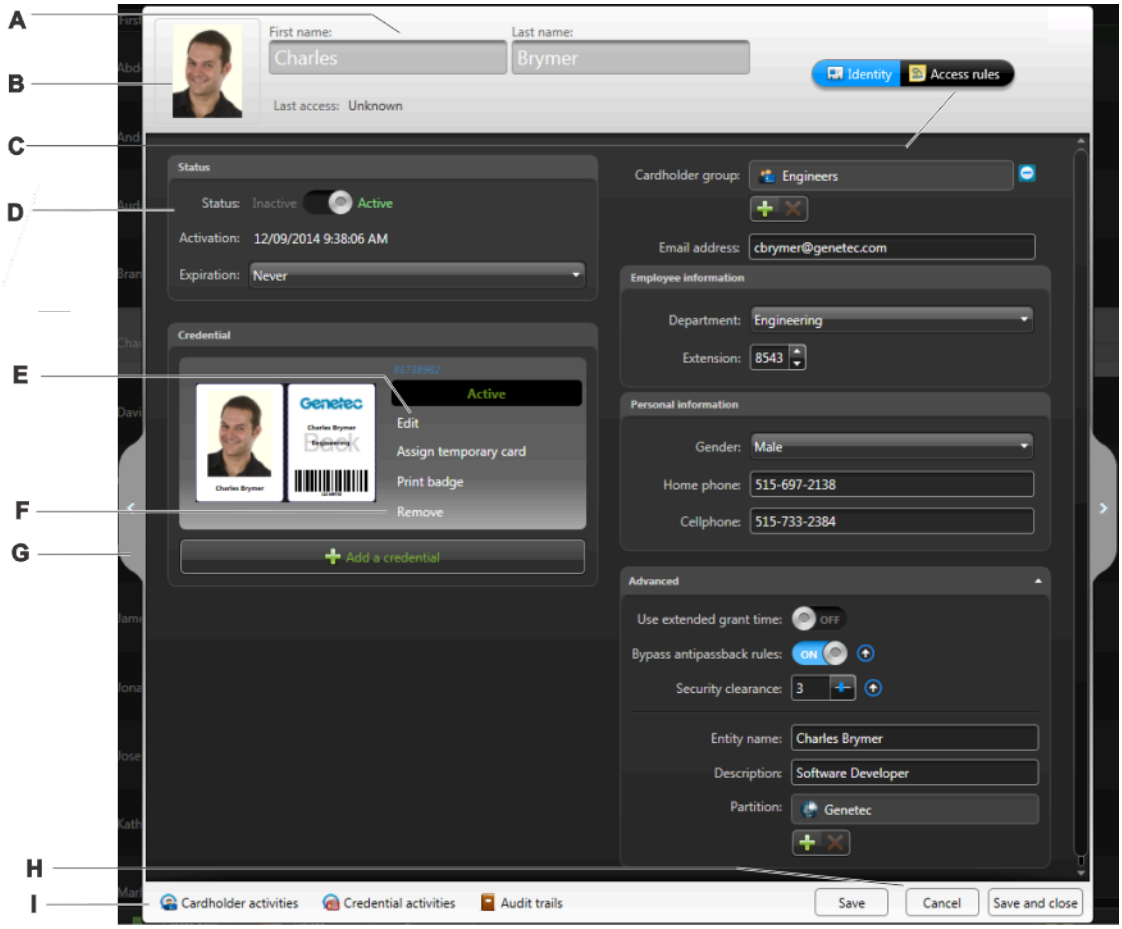
- **Cardholder:** Cardholder entity name.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.

- **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.
- **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.

The modify cardholder dialog box

After creating a cardholder, you can go back and modify their properties, credentials, and access rights by selecting the cardholder in the *Cardholder management* task, and then clicking **Modify** ( ).

The properties you can edit depend on your user privileges. The following figure shows the cardholder modification dialog box.



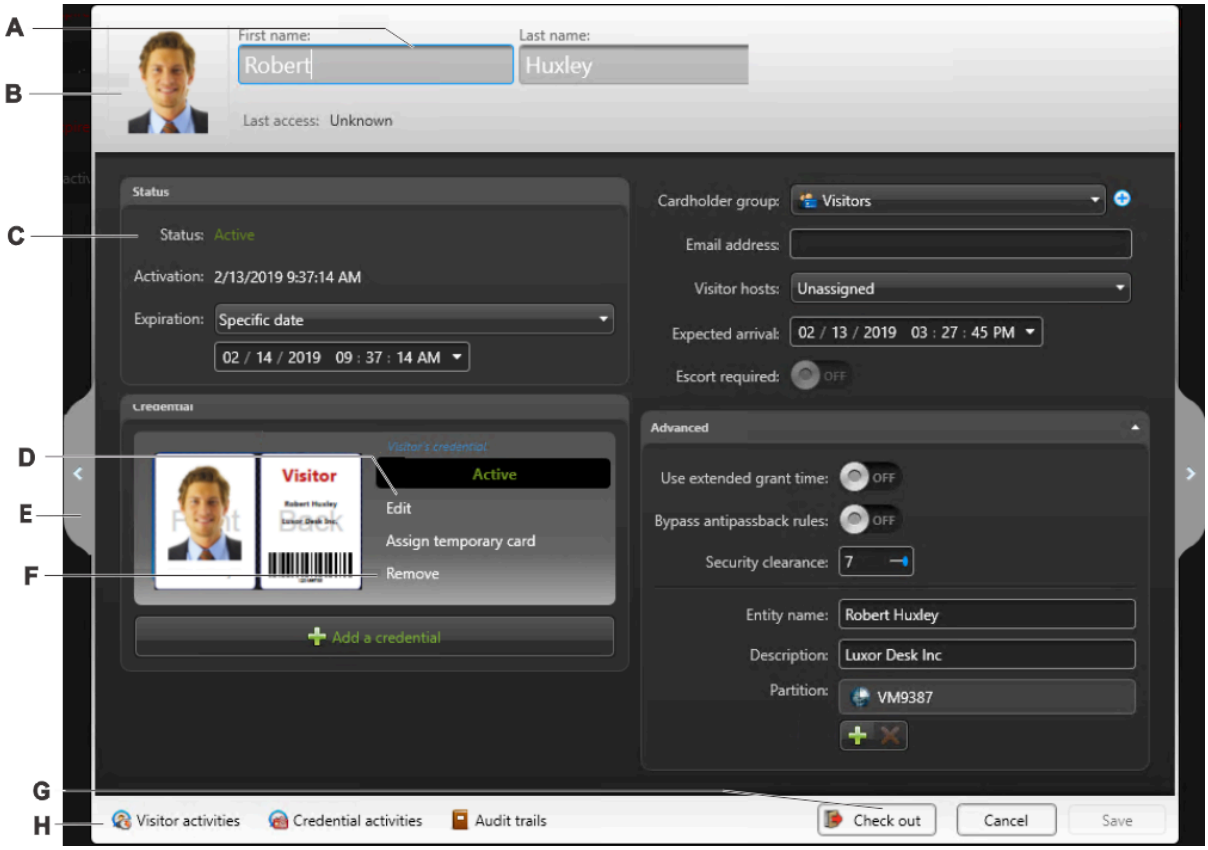
A	Cardholder's basic properties. The cardholder properties are described in Creating cardholders on page 291.
B	Edit the cardholder's picture. See Cropping pictures on page 327 and Applying transparent backgrounds to pictures on page 328. To remove the cardholder's picture, right-click, and then click **Clear the picture**.
C	Assign additional access rights to the cardholder from the *Access rules* page. See Assigning credentials on page 300.
D	Additional cardholder information. The properties are described in Creating cardholders on page 291.
E	Edit the cardholder's credential. The credential properties are described in Assigning credentials on page 300.
F	Remove the cardholder's credential.

G	Switch between cardholders.
H	Save or cancel your changes.
I	•  - Generate reports on the cardholder. See Investigating cardholder events on page 310. •  - Generate reports on the cardholder's credential (see Investigating credential events on page 352). •  - Generate reports on the changes made to the cardholder (see Finding out what changes were made to the system configuration on page 121).

The modify visitor dialog box

After checking in a visitor, you can go back and modify their properties by selecting the visitor in the *Visitor management* task, and then clicking **Modify** ( ).

The properties you can edit depend on your user privileges. The following figure shows the visitor modification dialog box.



A	Visitor's basic properties. The visitor properties are described in Checking in new visitors on page 295.
B	Edit the visitor's picture. See Cropping pictures on page 327 and Applying transparent backgrounds to pictures on page 328. To remove the visitor's picture, right-click it, and then click **Clear the picture**.
C	Additional visitor information. The properties are described in Checking in new visitors on page 295.
D	Edit the visitor's credential. The credential properties are described in Assigning credentials on page 300.
E	Switch between visitors.
F	Remove the visitor's credential.

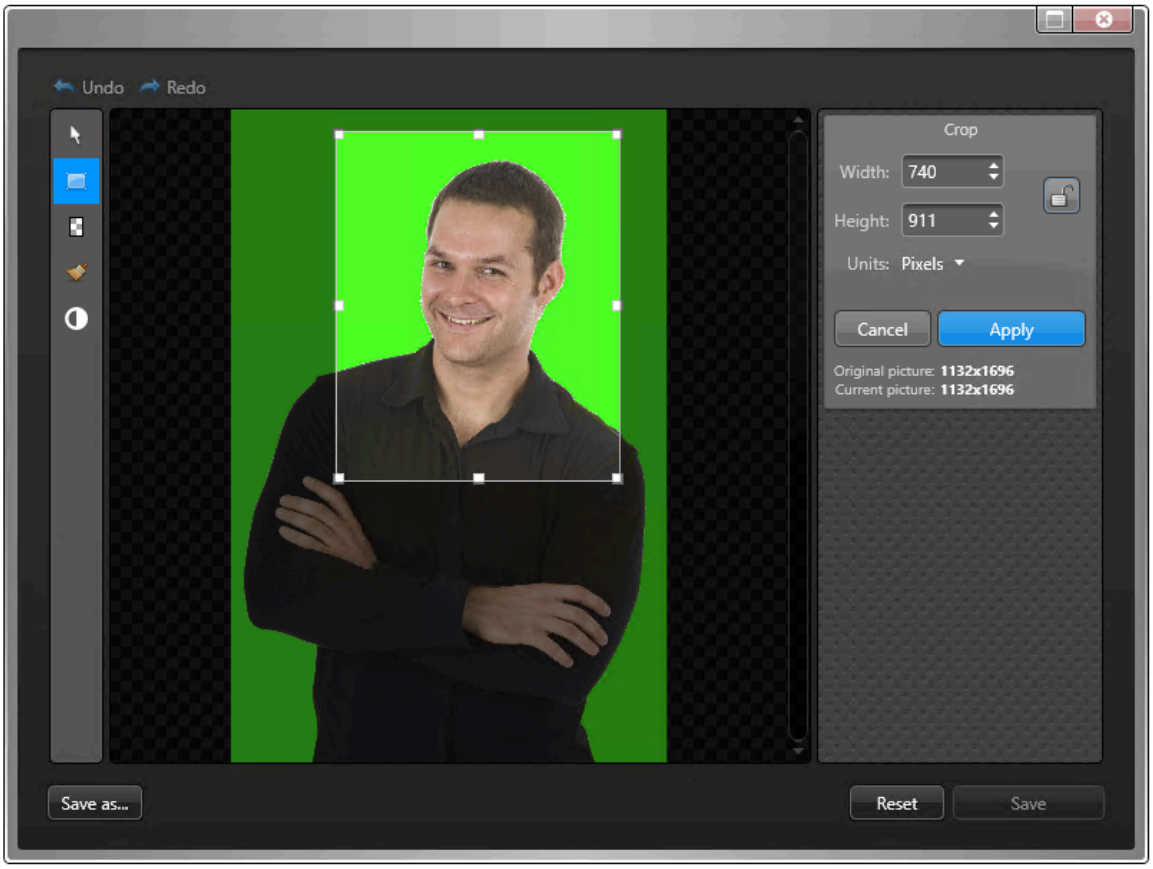
G	Save or cancel your changes, or check out the visitor.
H	• - Report on the visitor. See Investigating visitor events on page 312. • - Report on the visitor's credential. See Investigating credential events on page 352. • - Report on the changes made to the visitor. See Finding out what changes were made to the system configuration on page 121.

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

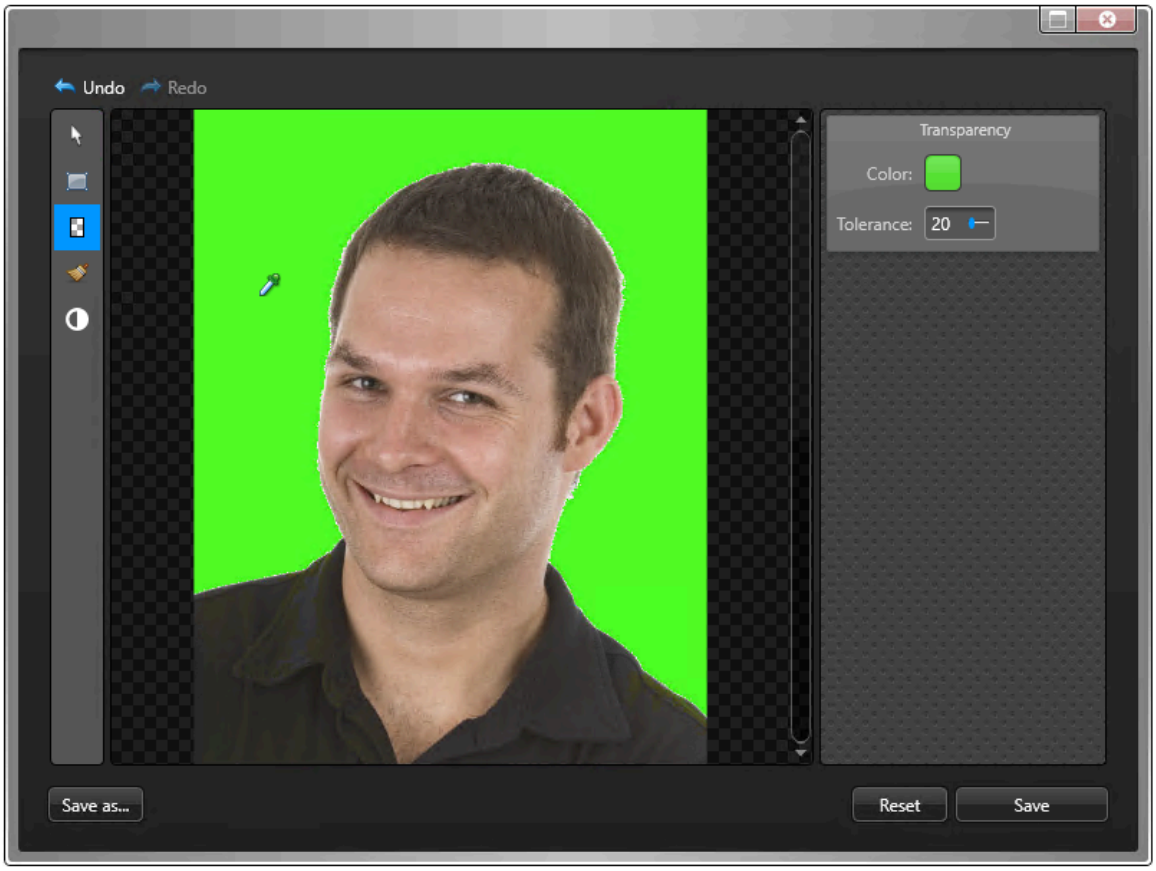
Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

Applying transparent backgrounds to pictures

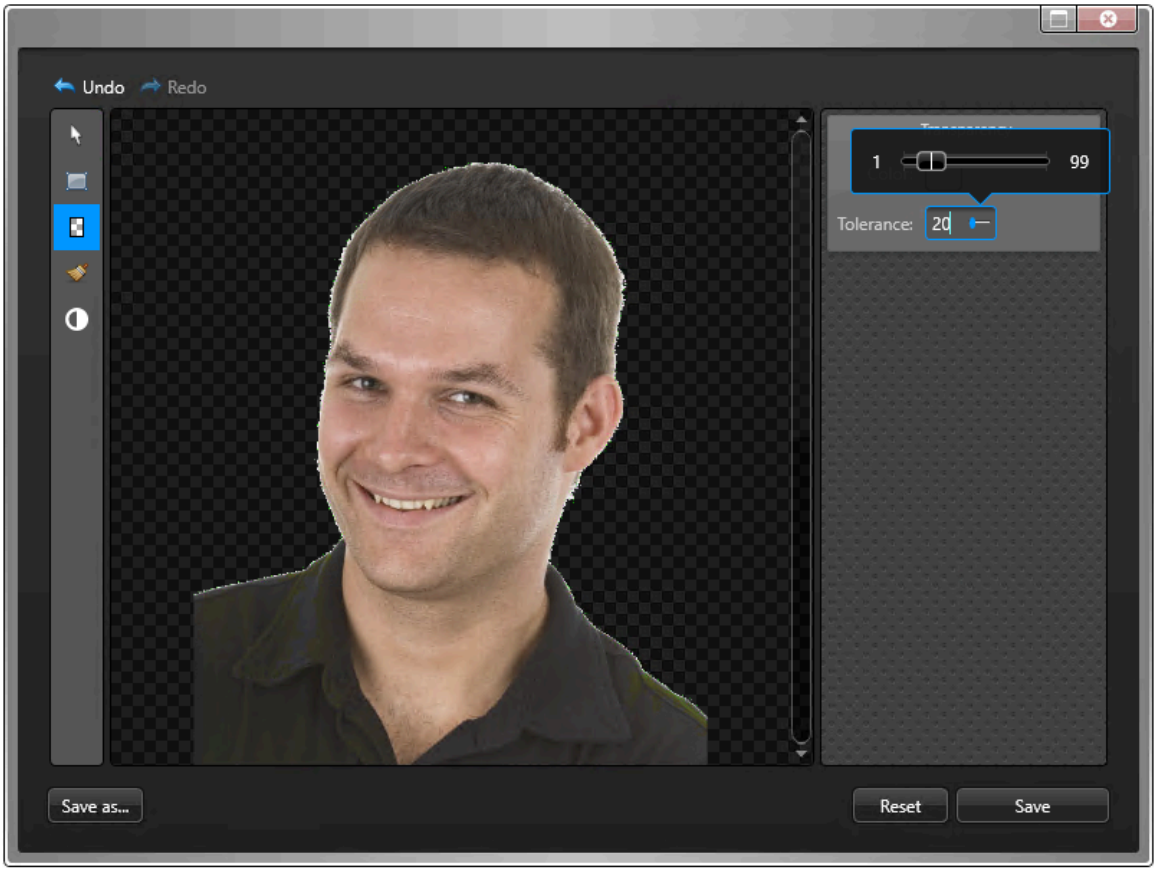
If a cardholder or visitor's picture was taken in front of a chroma key screen, you can make the picture background transparent. This is helpful if you create a badge template that has an image in the background.

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).



5 Using the **Tolerance** slider, adjust the transparency percentage.



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.

Searching for cardholders

If you have a large access control system and cannot find a cardholder, you can search for them by name, or use the advanced search by applying a combination of filters.

To search for a cardholder or visitor:

1 From the home page, open the *Cardholder management* task.

2 To search by an entity name, enter the name in the *Search* ( ) box.

All entities with names that match the text you entered are listed.

3 To search for the entity using the advanced search:

a) In the left pane, click **Advanced search**.

b) Set up the query filters for the report. Not all query filters are available for each task. Choose from one or more of the following, according to your task:

- **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.
- **Cardholder groups:** Restrict the search to specific cardholder groups.
- **Partition:** Partition that the entity is a member of.
- **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.
- **Can escort visitors:** Indicates whether or not the cardholder can act as a visitor host (can be switched on or off).

c) Click **Search**.

The cardholders that match your search criteria are displayed on screen.

Example

In this example, the cardholder you are searching for has a card that was activated less than a week ago. In the **Activation date** filter, enter 7 days in the *During the last* field.

Report pane columns for the Cardholder management 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 management* task.

- **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.
- **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.
- **Mobile phone number:** Cardholder or visitor's mobile phone number.
- **Activation date:** Date and time that the cardholder profile activates.
- **Cardholder:** Cardholder entity name.
- **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.
- **Expiration date:** Date and time the cardholder or visitor 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.

Searching for visitors

If you have a large access control system and cannot find a visitor, you can search for them by name, or use the advanced search by applying a combination of filters.

To search for a visitor:

1 From the home page, open the *Visitor management* task.

2 To search by an entity name, type the name in the **Search** (🔍) box.

All entities with names that match the text you entered are listed.

3 To search for the entity using the advanced search:

a) In the left pane, click **Advanced search**.

b) Set up the query filters for the report. Not all query filters are available for each task. Choose from one or more of the following, according to your task:

- **Check-in date:** The date and time that the visitor profile was activated, which can correspond to the arrival time.
- **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.
- **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.
- **Cardholder groups:** Restrict the search to specific cardholder groups.
- **Partition:** Partition that the entity is a member of.
- **Creation date:** Date and time that the visitor's profile was created.
- **Expected arrival:** Specify a time range during which the visitor is expected to arrive.
- **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.
- **Escort required:** Specify that a host is required.
- **Visitor hosts:** Select the visitor's host.

c) Click **Search**.

The visitors that match your search criteria are displayed on screen.

Report pane columns for the Visitor management task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the *Visitor management* task.

- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.

- **Status:** The visitor profile status.
- **Check-in date:** The date and time that the visitor profile was activated, which can correspond to the arrival time.
- **Expiration date:** Date and time the cardholder or visitor profile expires.
- **Creation date:** Date and time the visitor's credential was activated (can correspond to the arrival time).
- **Visitor hosts:** Cardholders assigned as visitor escorts.
- **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.
- **Expected arrival:** Date and time of the visitor's expected arrival.
- **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.
- **Escort required:** Indicates whether a visitor host is required.
- **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.

Searching for cardholders and visitors using their credential

If you have an unidentifiable card, you can find the cardholder or visitor it belongs to by presenting the card at a USB reader or door.

Before you begin

Make sure that you have a USB reader connected to your computer, or that there is a door you can present the card at.

To search for a cardholder or visitor by using their credential:

1 From the home page, open one of the following tasks:
   - For cardholders, click **Cardholder management**.
   - For visitors, click **Visitor management**.
2 At the top of the task window, click  .
3 From the drop-down list in the search window, select one of the following:
   - **USB Reader:** A USB reader that is connected to your computer.
   - **Door:** An access point close by.
4 Present the card to the device selected in the previous step.

If the card is assigned to a cardholder or visitor, the search dialog box closes and the corresponding person is selected in the cardholder or visitor list. If the card is not assigned to a cardholder or visitor, the reason that the card is rejected is displayed in the search dialog box. You can present another card, or click **Cancel** to stop the operation.

Example

If you found a card in the office or parking lot and it has no name or picture on it, you can identify who it belongs to.

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

18

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 are also supported if they are predefined in your system. To learn about creating custom card formats, see the *Security Center Administrator Guide*.

[2] For information on FASC-N 75 bits and FASC-N 200 bits formats, see How credential card formats work with Active Directory in Security Center in the *Security Center Administrator Guide*.

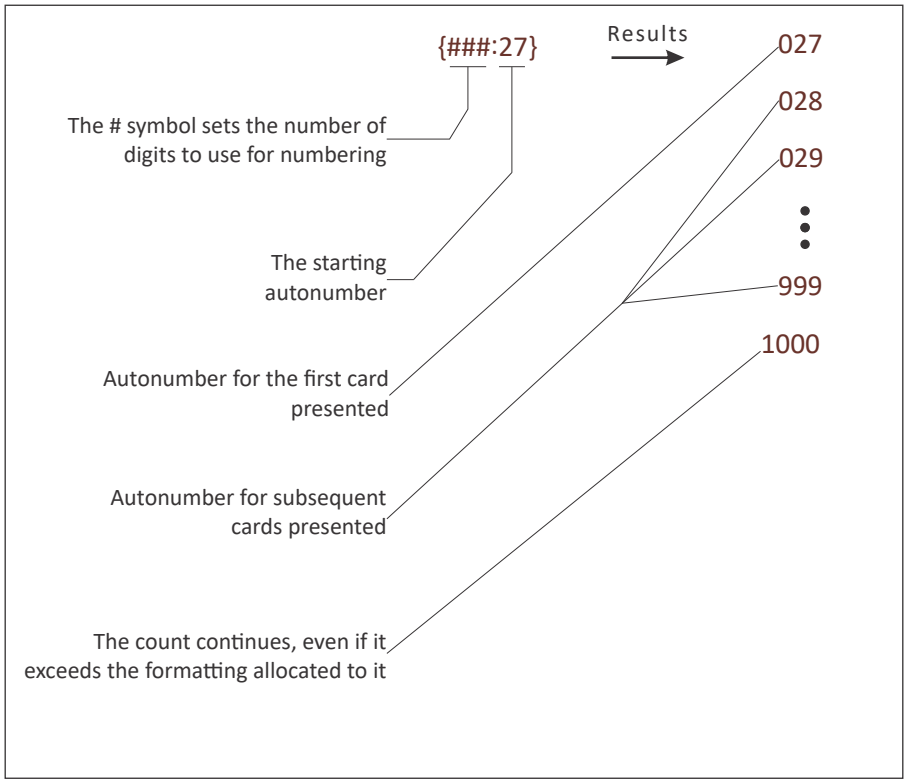
The credential prefix and the counter

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:



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 the FASC-N card format and raw 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.

FASC-N credentials can be created manually in Config Tool or Security Desk using the native **Card format** definition list or by using **Batch enrollment** in the Security Desk *Credential management* task.

You can also import FASC-N and raw-format credentials from a CSV file using the *Import tool* in Config tool, or the Security Center SDK. If you select **Credential raw data** on the *Bindings* page during import, Security Center automatically resolves the credentials and formats.

Non-governmental Personal Identity Verification-Interoperable (PIV-I) and Commercial Identity Verification (CIV) credentials will output the *CHUID.GUID* identifier, which is recognized by Security Center as a raw 128-bit credential; the credential can also be mapped to a custom card format.

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*. For more information about importing credentials using the *Import tool*, see the *Security Center Administrator Guide*.

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 300.

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.
  - **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** ( ).

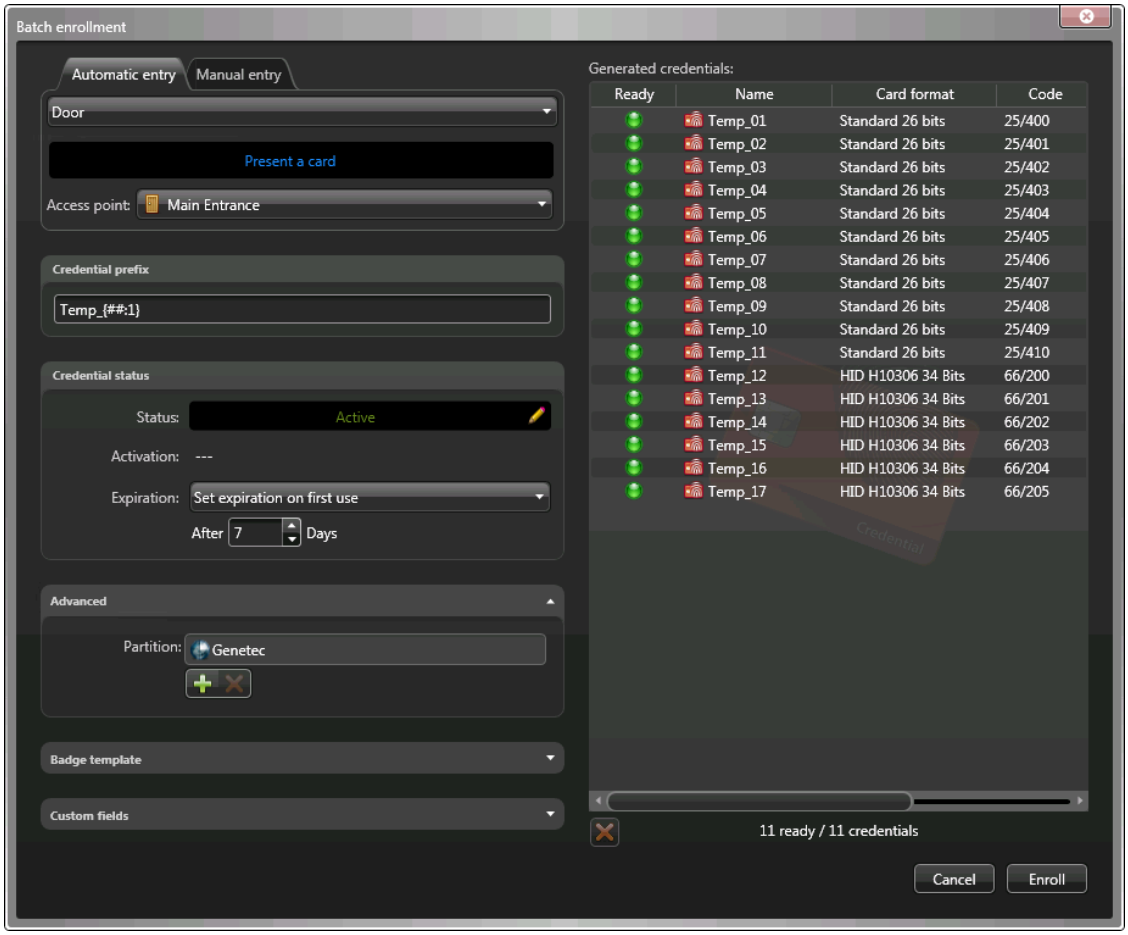
7 From the **Badge template** list, select the default badge template used to represent the credential.

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.



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

About credentials on page 336

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.
  - **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** ().

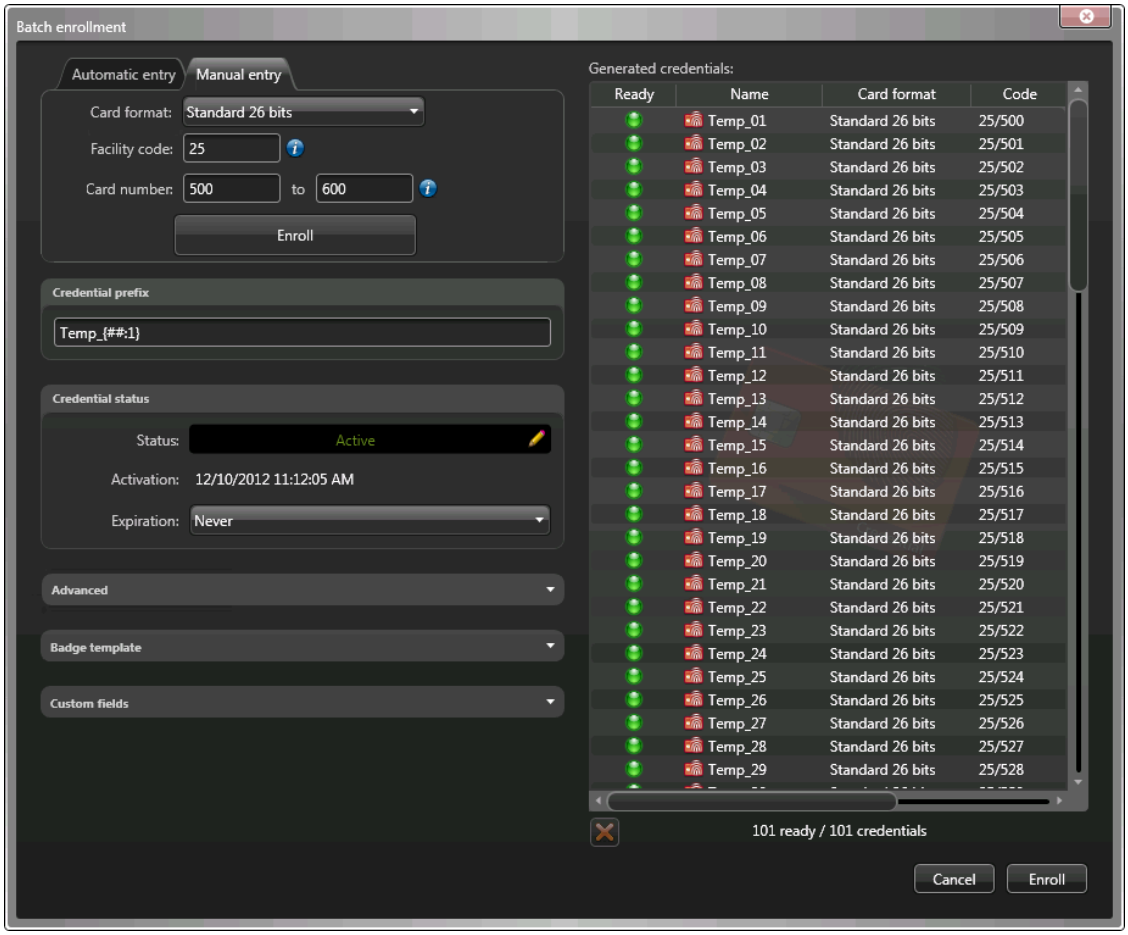
8 From the **Badge template** list, select the default badge template used to represent the credential.

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.



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

About credentials on page 336

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 credentials manually, you can import them from a CSV file, or from your company's Active Directory. For more information, see the *Security Center Administrator Guide*.
- To learn how to create mobile credentials, see "Creating mobile credentials in the Mobile Credential Manager" in the *Security Center Administrator Guide*.

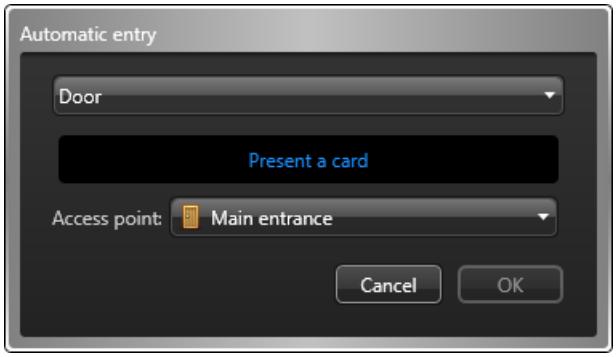
To create a credential:

1 In the *Credential management* task, click **Create new credential** ( ).

2 Select one of the following options:

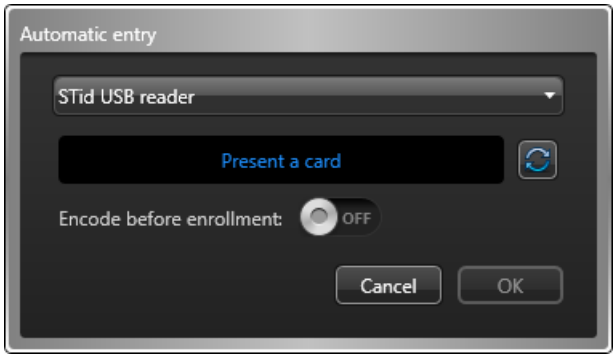
- **Automatic entry:** Present the card at a reader.
- **Manual entry:** Manually enter the card data. Use this method when you do not have a card reader near you.
- **PIN:** Create a PIN credential.
- **License plate:** Enter a cardholder's license plate number. Use this method if a Sharp camera is 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.



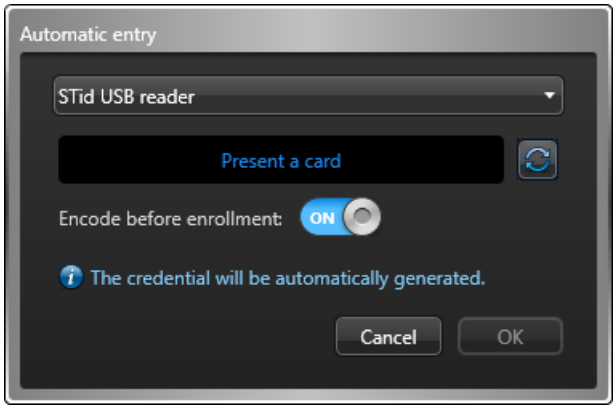
If you have a smart card encoding reader set up, do one of the following:

- To read a pre-encoded card, set the option **Encode before enrollment** to **OFF**. 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.

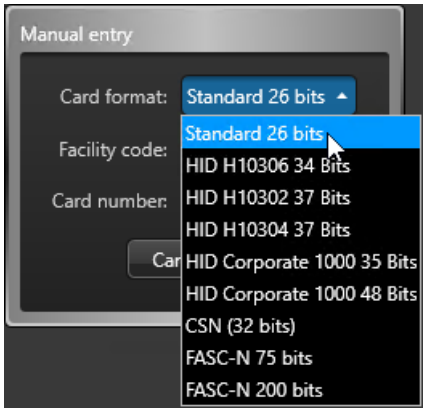


- To generate and encode on your card a random 128-bit MIFARE DESFire credential before enrolling it, set the option **Encode before enrollment** to **ON**. When the reader LED turns red (ready to encode), place the smart card on the reader for approximately 2 seconds. The reader LED turns yellow and 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.

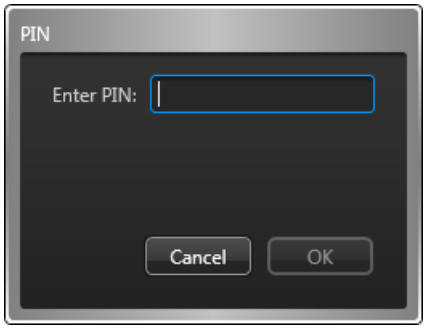


4 If you select **Manual entry**, you must then select a card format, enter the required data fields, and click **OK**.



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:

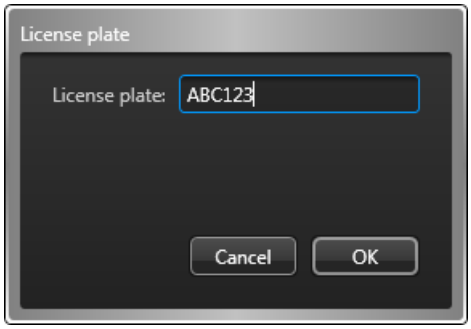


a) Enter the PIN as a numerical value.

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:



a) Enter the license plate number.

NOTE: You do not need to enter spaces that appear 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.

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. For information, see the *Security Center Administrator Guide*.

      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

Assigning credentials on page 300
Requesting credential cards on page 304
Overview of the Credential management task on page 592

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 new 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**, then 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 300.
- To assign a credential manually, click **Manual entry**, then select a card format, enter the required data fields, and click **Enroll**.
  If an eligible card is entered, 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.
  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**, then 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

Creating credentials on page 344
Requesting credential cards on page 304

Investigating request history of credential cards

You can see which users requested, canceled, and printed credential cards, using the *Credential request history* report.

Before you begin

To receive results in the Credential request history report, you must already be monitoring credential request user activities. For information about how to select which activities to monitor and record in the database from the System task in Config Tool, see the *Security Center Administrator Guide*.

What you should know

Credential badges are usually requested if there is no printer located on the site. If you create a report of the badges that were printed in the last month, the report results can be used as billing information.

To investigate the request history of credential badges:

1 From the home page, open the **Credential request history** task.

2 Set up the query filters for your report. Choose one or more of the following filters:

- **Activities:**

  Select which badge printing activities to investigate.

  - **Credential request:** When a user requests a badge printing job.
  - **Credential request canceled:** When a user cancels a badge printing job.
  - **Credential request completed:** When a user prints a badge from the queue.
- **Cardholders:** Restrict the search to specific cardholders, cardholder groups, or visitors.
- **Credential:** Restrict the search to specific credentials.
- **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.
- **Printing users:** Restrict the search to specific users that printed a badge.
- **Requesting users:** Restrict the search to specific users that requested to print a badge.

3 Click **Generate report**.

The credential badge printing events are listed in the report pane.

Related Topics

Requesting credential cards on page 304

Report pane columns for the Credential request 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 Credential request history task.

- **Date/time queued:** The date and time that the badge printing job was requested.
- **Activity name:** Type of activity.
- **Request reason:** Reason why the new credential was requested.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **Credential:** Credential name used by the cardholder.

- **User:** Name of the user who triggered the event. The user name is empty if the event was not triggered from Security Desk.
- **Requester email:** Email address of the user who requested the badge printing job.
- **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 credential events

You can investigate events related to credentials (Access denied: Expired credential, Access denied: Inactive credential, Access denied: Stolen credential, and so on), using the *Credential activities* report.

What you should know

In the *Credential activities*, you can investigate areas a cardholder accessed by selecting the credential, and the time range. You also can search by critical credential events. For example, if an *Access denied: Stolen credential* event occurred, you can see who tried to use the stolen credential by reviewing the video associated with the event.

To investigate credential events:

1. From the home page, open the **Credential activities** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **Credential:** Restrict the search to specific credentials.
   - **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.
   - **Doors - Areas - Elevators:** Restrict the search to activities that took place at certain doors, areas, and elevators.
   - **Events:** Select the events of interest. The event types available depend on the task you are using.
   - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
3. Click **Generate report**.

   The credential events are listed in the report pane.
4. To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

   If there is no camera connected to the entity, the door, elevator, or area icon is displayed, depending on the type of credential event.
5. To control the tiles, use the widgets in the *Controls* pane.

Report pane columns for the Credential activities 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 activities task.

- **Event:** Event name.
- **Credential:** Credential name used by the cardholder.
- **Location:** Location (area) where the activity took place.
- **Access point:** Access point involved (only applicable to areas, doors, and elevators).
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **Event timestamp:** Date and time that the event occurred.
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential code:** Facility code and card number.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Email address:** Cardholder or visitor's email address.
- **IP address:** IP address of the unit or computer.

- **Mobile phone number:** Cardholder or visitor's mobile phone number.
- **Occurrence period:** Period when the event occurred.
- **Product type:** Model of the unit.
- **Time zone:** Time zone of the unit.
- **Unit:** Name 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.

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.

Searching for credentials

If you have a large access control system and cannot find a credential, you can search for it by name, or use the advanced search by applying a combination of filters.

To search for a credential:

1 From the home page, open the *Credential management* task.

2 To search by an entity name, type the name in the *Search* (🔍) box.

All entities with names that match the text you entered are listed.

3 To search for the entity using the advanced search:

a) In the left pane, click **Advanced search**.

b) Set up the query filters for the report. Choose from one or more of the following filters:

- **Description:** Restrict the search to entries that contain this text string.
- **Partition:** Partition that the entity is a member of.
- **Status:** The status of the cardholder or visitor's profile: *Active*, *Expired*, *Inactive*, *Lost*, *Stolen*.
- **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.
- **Expiration date:** Specify a time range during which the credential expires.
- **Credential information:** Restrict the search to specific card formats, facility codes, card numbers, or license plates.

c) Click **Search**.

The credentials that match your search criteria are displayed on screen.

Report pane columns for the Credential management 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 management 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.
- **Last access grant:** Time the cardholder entered the area.
- **Cardholder:** Cardholder entity 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.
- **Cardholder status:** The cardholder's profile status.
- **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.
- **Email address:** Cardholder or visitor's email address.
- **First name:** Cardholder or visitor's first name.
- **Is a mobile credential:** Indicates whether the credential is a mobile credential.

- **Last name:** Cardholder or visitor’s last name.
- **Mobile credential status:** The status of the credential if it is a mobile credential.
- **Mobile phone number:** Cardholder or visitor's mobile phone number.
- **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.

19

Areas, doors, and elevators

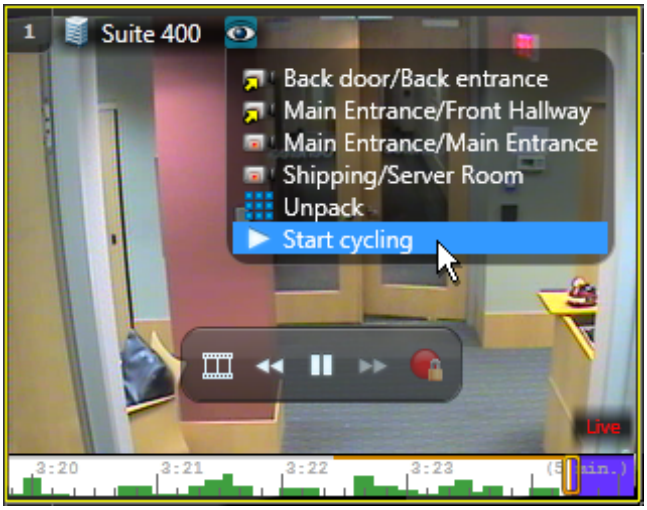
This section includes the following topics:

How areas are displayed in the canvas

When you display an *area* ( ) or a secured area ( ) in a canvas tile, the area widget appears in the *Controls* pane so you can control the area.

Areas usually have multiple cameras attached to them. When you view an area, the first camera associated to that area is displayed.

By clicking the eye ( ) icon in the tile toolbar, you can select which attached entity to view, or you can *unpack* the area, which displays all the attached entities in separate tiles. You can also start *entity cycling*, which rotates the entities displayed in the tile.

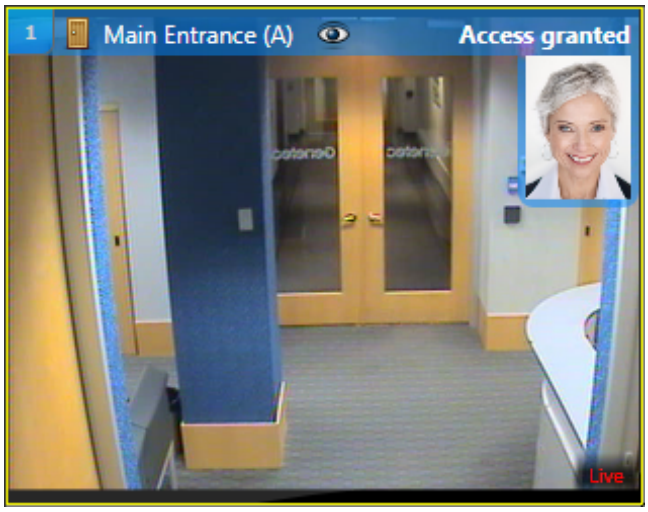


If no camera is associated to the area, only the area icon is shown.

How doors are displayed in the Security Desk canvas

When you display a *door* ( ) in a canvas tile, the door widget appears in the *Controls* pane so you can control the door.

If the door is linked to a camera, then the video stream of the camera is shown in the tile.



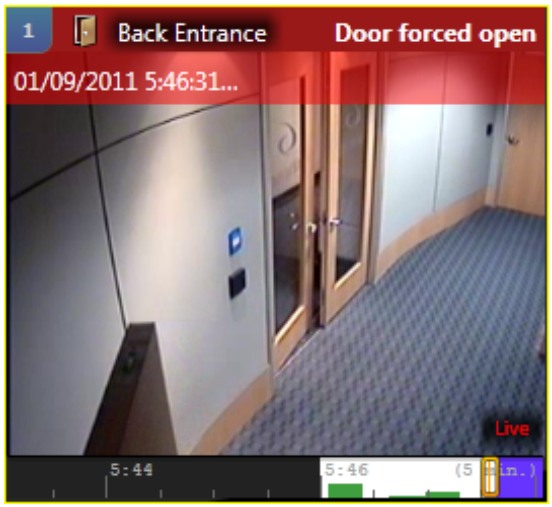
If the door is not linked to a camera, only the door icon is shown. The door image is static. It always remains open.

Allowing access through doors

To unlock a door or override locking and unlocking schedules, you can use the *Door* widget to control access through doors. The door widget is enabled when a door entity is displayed in the selected canvas tile.

What you should know

- For the **Override unlock schedules** button in the *Door* widget to be enabled, you must have the *Modify door properties* privilege.
- Access controlled doors are locked by default, unless an unlock schedule is being used. Only cardholders with the correct credentials can open them. When a door is displayed in a canvas tile, the door entity icon in the tile toolbar changes in real time to reflect whether the door is physically open ( ) or closed ( ).
- If no camera is associated with the door, a static open door image is displayed in the canvas tile. The following figure shows an open door and its corresponding door icon:



To allow access through a door:

1 From the *Monitoring* task, select a tile that is displaying a door.

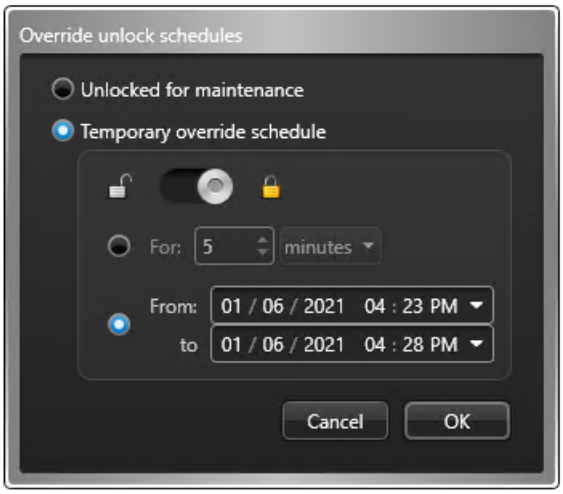
The *Door* widget is displayed in the *Controls* pane.

2 In the door widget, do one of the following:

- To unlock the door and temporarily grant access, click **Unlock** ( ).

  The duration of the grant time is configured by the system administrator. The widget shows that the door is open and unlocked.

- To override the door's unlock schedule, click **Override unlock schedules** ( ), and select one the following:



  - **Unlocked for maintenance:** Unlock the door indefinitely for maintenance purposes. To cancel this override, click in the door widget.
  - **Temporarily override unlock schedule:** Lock ( ) or unlock ( ) the door for a specified period of time, either immediately or in the future. With this option, the door returns to its normal state after the time expires.

3 Click **OK**.

Example

When setting unlock schedules for a door, a Security Center administrator can program a door to grant access to everyone during certain hours of the day, such as when a receptionist is on duty. If you have the rights, you can override these unlock schedules by locking the door when it is scheduled to be unlocked, or by unlocking the door when it is scheduled to be locked.

Preventing access through doors

To temporarily prevent all access through a door, you can deactivate (or shunt) the reader on the side of the door you don't want people to access.

What you should know

Not all readers can be disabled from Security Desk. The ability to shunt a reader depends on your access control equipment. Shunting a reader is equivalent to cutting the power to the reader. For this reason, a cardholder presenting a valid credential at the door would no longer be able to unlock the door. This however does not prevent someone from unlocking the door with a key.

TIP: You can also shunt a defective reader to prevent it from beeping or generating any events.

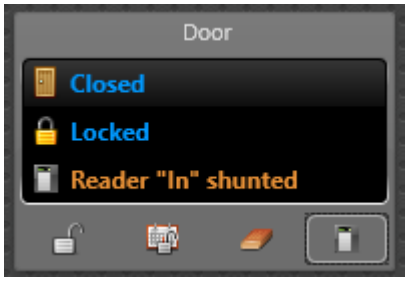
To prevent access through a door:

1 From the *Monitoring* task, select a tile that is displaying a door.

The *Door* widget is displayed in the *Controls* pane.

2 In the door widget, click the **Reader** ( ) button, and select the reader you want to shunt.

The reader that is shunted is indicated in the door widget.



To re-activate a reader:

1 Click again the **Reader** ( ) button and select the reader you want to activate.

Controlling access to elevator floors

To temporarily allow or prevent access to elevator floors, you can use the *Elevator* widget to either override the elevator schedule or to deactivate (shunt) the elevator cabin reader. The elevator widget is enabled when an elevator entity is displayed in the selected canvas tile.

What you should know

Not all elevators can be controlled from Security Desk, and not all readers can be deactivated from the widget. The ability to shunt a reader depends on your access control equipment. Shunting a reader is equivalent to cutting the power to the reader. For this reason, a cardholder presenting a valid credential inside the elevator cabin would no longer be able to operate the elevator by pressing a floor button.

TIP: You can also shunt a defective reader to prevent it from beeping or generating any events.

The following user privileges are required:

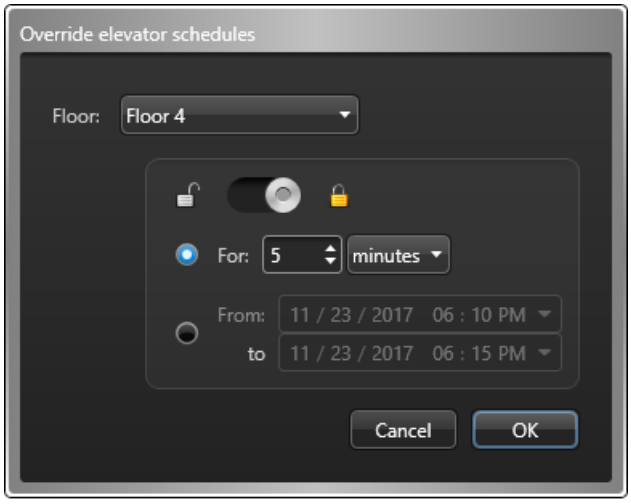
- **Override elevator schedules:** Required to override elevator schedules.
- **Action privileges > Access control > Doors > Override unlock schedules > Maintenance mode:** Required to control elevator reader shunting.

To control the access to an elevator floor:

1 From the *Monitoring* task, select a tile that is displaying an elevator ( ).

2 In the elevator widget, click **Override elevator schedules** ( ).

The *Override elevator schedules* dialog box opens.



3 In the **Floor** drop-down list, select the floors for which you want the schedules to be overridden.

4 Lock ( ) or unlock ( ) the selected floors for a specified period of time.

- Click the first choice and enter a duration for the override to start immediately.
- Click the second choice and enter the specific time period you want the override to start and last.

5 Click **OK**.

To prevent access to all elevator floors:

1 In the elevator widget, click the **Reader** ( ) button, and click **Shunt**.
The reader status is indicated in the elevator widget.

TIP: To read the full status description, point at the **Reader** ( ) button.

To re-activate the elevator cabin reader:

1 Click again the **Reader** ( ) button and select **Activate**.

Related Topics

Elevator widget on page 44

Investigating area events

You can investigate events related to *areas* (Access granted, First person in, Antipassback violation, and so on), using the *Area activities* report.

To investigate area events:

1 From the home page, open the *Area activities* task.

2 Set up the query filters for the report. Choose from one or more of the following filters:

- **Areas:** Select the areas to investigate.
- **Cardholders:** Restrict the search to specific cardholders, cardholder groups, or visitors.
- **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.
- **Events:** Select the events of interest. The event types available depend on the task you are using.
- **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.

3 Click **Generate report**.

The area events are listed in the report pane.

4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If the area is not associated to a URL or a map file through a tile plugin, the area icon is displayed.

5 To control the areas, use the area widget.

Example

If you want to see all the activity that went on in a particular area during the weekend, or since the last time you logged on, you can select a specific area and time range for the report. You can search for critical events that happened in an area (such as *Access granted* or *Access denied: Stolen credential* events), and then review the video associated with that event to see what happened during that time, and to find evidence.

Related Topics

Area widget on page 37

Report pane columns for the Area activities task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Area activities task.

- **Event:** Event name.
- **Area:** Area name.
- **Side - Direction:** Entrance or exit.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **Credential:** Credential name used by the cardholder.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door or elevator.
- **Event timestamp:** Date and time that the event occurred.
- **Security clearance:** The cardholder's security clearance level.
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.

- **Credential code:** Facility code and card number.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Email address:** Cardholder or visitor’s email address.
- **IP address:** IP address of the unit or computer.
- **Mobile phone number:** Cardholder or visitor's mobile phone number.
- **Occurrence period:** Period when the event occurred.
- **Product type:** Model of the unit.
- **Time zone:** Time zone of the unit.
- **Unit:** Name 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.

Investigating door events

You can investigate events related to *doors* (Door forced open, Door open too long, Hardware tamper, and so on), using the *Door activities* report.

To investigate door events:

1 From the home page, open the *Door activities* task.

2 Set up the query filters for your report. Choose one or more of the following filters:

- **Cardholders:** Restrict the search to specific cardholders, cardholder groups, or visitors.
- **Credential:** Restrict the search to specific credentials.
- **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.
- **Doors:** Select the doors to investigate.
- **Events:** Select the events of interest. The event types available depend on the task you are using.
- **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.

3 Click **Generate report**.

The door events are listed in the report pane.

4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If there is no camera attached to the door, the door icon is displayed.

5 To control the doors, use the door widget.

Example

Using the *Door Activities* report, you can see how many access denied events have occurred in the last week, or since your last shift. You can also search for other critical events, such as *Door forced open*. If you see suspicious cardholder activity while monitoring live video, you can investigate what other doors the cardholder accessed in the last day. If you want to verify that maintenance staff has completed work at a particular door, you can investigate on that door by selecting the *Door maintenance completed* event.

Related Topics

Door widget on page 43

Report pane columns for the Door activities 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 activities task.

NOTE: If you generated the Door activities report using Web Client, not all of the report columns are available.

- **Event:** Event name.
- **Door:** Door name.
- **Side:** Door side name.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **Credential:** Credential name used by the cardholder.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door or elevator.
- **Event timestamp:** Date and time that the event occurred.

- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential code:** Facility code and card number.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Email address:** Cardholder or visitor’s email address.
- **IP address:** IP address of the unit or computer.
- **Mobile phone number:** Cardholder or visitor's mobile phone number.
- **Occurrence period:** Period when the event occurred.
- **Product type:** Model of the unit.
- **Time zone:** Time zone of the unit.
- **Unit:** Name 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.

Investigating elevator events

You can investigate events related to elevators (Floor accessed, Elevator offline: Device is offline, Hardware tamper, and so on), using the *Elevator activities* report.

What you should know

Using the *Elevator activities*, you can see which cardholders or credentials accessed which elevators and floors, for a given time period. You also can search for access denied events at an elevator, to see who tried to access a floor they did not have permission to enter.

To investigate elevator events:

1. From the home page, open the *Elevator activities* task.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **Cardholders:** Restrict the search to specific cardholders, cardholder groups, or visitors.
   - **Credential:** Restrict the search to specific credentials.
   - **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.
   - **Elevators:** Select the elevators to investigate.
   - **Events:** Select the events of interest. The event types available depend on the task you are using.
   - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
3. Click **Generate report**.

   The elevator events are listed in the report pane.
4. To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

   If the elevator is not associated to a URL or a map file through a tile plugin, the elevator icon is displayed.
5. To control the tiles, use the widgets in the *Controls* pane.

Report pane columns for the Elevator activities task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Elevator activities task.

- **Event:** Event name.
- **Elevator:** Elevator name.
- **Floor:** Elevator floor name.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **Credential:** Credential name used by the cardholder.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door or elevator.
- **Event timestamp:** Date and time that the event occurred.
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential code:** Facility code and card number.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Email address:** Cardholder or visitor's email address.

- **IP address:** IP address of the unit or computer.
- **Mobile phone number:** Cardholder or visitor's mobile phone number.
- **Occurrence period:** Period when the event occurred.
- **Product type:** Model of the unit.
- **Time zone:** Time zone of the unit.
- **Unit:** Name 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.

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 home page, 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.

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.

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.

For information about modifying the properties of doors or elevators, see the *Security Center Administrator Guide*.

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 home page, 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** drop-down 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.

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 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.

For information about modifying the members of an access rule, see the *Security Center Administrator Guide*.

To identify which entities are affected by an access rule:

1. 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.
   - **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. In the **Expand cardholder groups** option, select **Enable** to list the members of the affected cardholder groups in the report instead of the cardholder groups themselves.
4. In the **Include perimeter entities** option, select **Enable** to include the perimeter entities of the affected areas in the report.
5. Click **Generate report**.

   The entities and access points affected by this access rule are listed in the report pane.

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's profile status.
- **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.

20

Access control units

This section includes the following topics:

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 home page, 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. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
- **Events:** Select the events of interest. The event types available depend on the task you are using.

3 Click **Generate report**.

The access control unit events are listed in the report pane.

NOTE: If you have Access Managers that are offline when you launch the query, you get an error message for each Access Manager, even though they are not related to the selected access control units. This is because the system has no way of knowing whether the selected units were managed by one of them in the past or not.

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.
- **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.

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 a 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 control units:** Select the access control units 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.
- **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 127

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, IO module, Strike relay, etc.).
- **IP address:** IP address of the unit or computer.
- **Manufacturer:** Manufacturer of the unit.
- **Physical name:** Device name.
- **Unit:** Name of the unit.
- **Unit type:** Type of unit (Access control, Intrusion detection, ALPR, or Video).

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 home page, click **Options** > **External devices**.
2. Next to each external device, set the option **ON** or **OFF**.
3. Click **Save**.
4. Restart your application.

Part IV

Introduction to license plate recognition in Security Desk

This part includes the following chapters:

21

LPR 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.

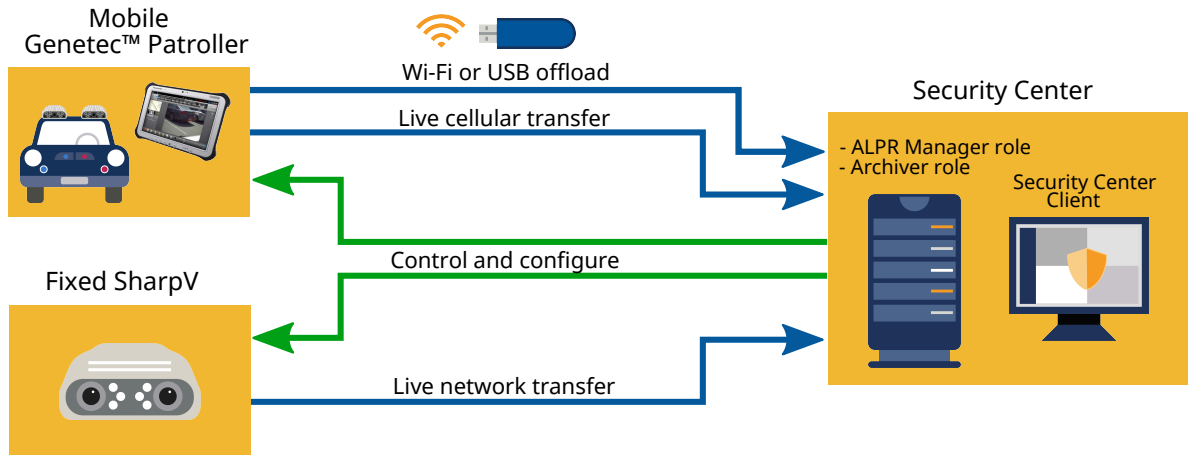
You can use AutoVu™ for the following:

- 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.

22

LPR events

This section includes the following topics:

How ALPR events are viewed in Security Desk

ALPR events are license plate reads and hits that are generated by ALPR entities, such as Genetec Patroller™ installations and ALPR units. You can track ALPR events in real time, using the *Monitoring* task.

When an ALPR event occurs, you can view the event information in the event list, including the plate and context images, the GPS position of the Genetec Patroller™ vehicle or Sharp camera that recorded the event, the reason a hit was rejected, and so on. In fixed Sharp configurations with video (Omnicast), you can stream live video from the Sharp context camera, and other cameras located with the Sharp. You can also print hit events, and use them as proof of violation. You can choose to view ALPR events in the canvas in Tile mode (individual tiles) or Map mode (a road map).

The GPS position of recorded reads and hits is the GPS position of the Genetec Patroller™ or Sharp camera that recorded the event.

CAUTION: For events to be kept in the database and available for reporting, they must be offloaded from Genetec Patroller™. You can monitor live events from the *Monitoring* task and receive live data in some reports without offloading from Genetec Patroller™.

Customizing which ALPR information to display in Security Desk

You can choose what kind of ALPR information you want to display in Monitoring task tiles for reads and hits. This ensures that Security Desk operators see only the information that is required for your ALPR deployment scenario.

Before you begin

Close Security Desk.

What you should know

This feature works by adding different XML attributes and parameters to a specific Security Desk configuration file found on the Security Desk client machine. Each XML attribute corresponds to different ALPR information.

To customize which ALPR information to display in Security Desk:

1 On the Security Desk client computer, go to *C:\Program Files (x86)\Genetec Security Center 5.10\ConfigurationFiles.*

2 Find the following tag in App.SecurityDesk.config: `<Presentation IgnoreSizeConstraints="False" EnableRatioViewbox="True" DisplayResourcesIds="False" SearchFormState="" AutoLoadHighResImages="True" WebBrowserType="InternetExplorer" DisplayFederationArrow="false" />`.

You can add additional XML attributes anywhere between the opening bracket and the closing slash and bracket.

3 To customize the display of read-related information in a tile, add the `"ReadDescription="` attribute, followed by any of the following parameters:

NOTE: Add the character `&#13;` if you want to force a carriage return in the Security Desk tile.

- **{Read.Address}:** The address of the plate read.
- **{Read.Confidence Score}:** The Confidence Score analytic information of the plate read (read accuracy). If the Sharp camera is not configured to send this analytic information, the XML tag will be displayed in the Security Desk tile.
- **{Read.Vehicle Type}:** The Vehicle Type analytic information of the plate read. If the Sharp camera is not configured to send this analytic information, the XML tag will be displayed in the Security Desk tile.
- **{Read.Relative Motion}:** The Relative Motion analytic information of the plate read. If the Sharp camera is not configured to send this analytic information, the XML tag will be displayed in the Security Desk tile.
- **{Read.Plate}:** The license plate characters as read by the ALPR matcher.
- **{Read.PlateState}:** The license plate's issuing state, province, or country.
- **{Read.Timestamp}:** The date and time of the plate read.
- **{Read.User}:** The name of the Genetec Patroller™ unit that read the plate.

Example: Here is what the config file looks like with all the read attributes included: `<Presentation IgnoreSizeConstraints="False" EnableRatioViewbox="True" DisplayResourcesIds="False" SearchFormState="" AutoLoadHighResImages="True" WebBrowserType="InternetExplorer" DisplayFederationArrow="false" ReadDescription="{Read.Plate}, {Read.Confidence Score}%, {Read.PlateState}, {Read.Timestamp}{Read.Address}, User: {Read.User}"/>`

4 To customize the display of hit-related information in a tile, add the "HitDescription=" attribute, followed by any of the following parameters.

NOTE: Add the character
 if you want to force a carriage return in the Security Desk tile.

- **{Hit.Category}:** The “category” attribute of the hotlist or permit list.
- **{Hit.Id}:** The GUID of the hit.
- **{Hit.MatchPlate}:** The plate number that was matched by the ALPR matcher.
- **{Hit.Rule}:** The name of the hotlist or permit list entity in Security Center.
- **{Hit.Timestamp}:** The date and time of the hit.
- **{Hit.Type}:** The type if hit (hotlist, permit, overtime, MLPI).
- **{Hit.User}:** The name of the patrol vehicle that raised the hit.
- **{Hit.Watermark}:** The digital signature of the hit.

Example: Here is what the config file looks like with all the read and hit attributes included: <Presentation IgnoreSizeConstraints="False" EnableRatioViewbox="True" DisplayResourcesIds="False" SearchFormState="" AutoLoadHighResImages="True" WebBrowserType="InternetExplorer" DisplayFederationArrow="false" ReadDescription="{Read.Plate}, ={Read.Confidence Score}%, {Read.PlateState}, {Read.Timestamp}
{Read.Address}, User: {Read.User}" HitDescription="{Read.Plate}, {Read.ConfidenceScore}%, {Read.PlateState}, {Read.Timestamp}, {Read.Address}
{Hit.Type}, {Hit.Rule} / {Hit.MatchPlate}, {Hit.Timestamp}
Category: {Hit.Category}, User: {Hit.User}
{Hit.Id}"/>

NOTE: You can add read information to a hit description because all hits are linked to at least one read. For example, you may want both the read and hit timestamps in the hit description because there may be a delay in the hit being processed.

5 Save and close Notepad.

6 Start Security Desk.

The Monitoring task tiles will now display the ALPR information you added to the config file.

After you finish

Repeat these steps on any Security Desk client machine that requires specific ALPR information in Monitoring task tiles.

Customizing ALPR image quality displayed in report pane columns

You can choose what quality of ALPR images you want to view in the report pane columns for reads and hits. This helps Security Desk operators scan through multiple high quality images to perform a quick investigation.

To customize the quality of ALPR images displayed in report pane columns:

1 From the home page, click **Options** > **Performance**.
2 In the *Car plates* section, select the **Enable high-resolution report images** check box.
3 Click **Save**.

To view high resolution images in report pane columns:

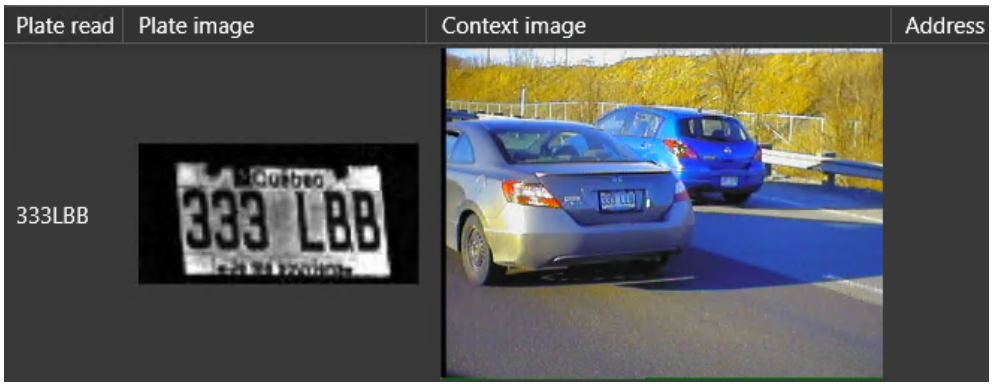
1 From the Security Desk homepage, open the required report task.
Example: If you want to generate a Hits report, open the *Hits* task.
2 Set up the query filters as required.
3 Click **Generate report**.
4 Expand the column width for *Plate image* and *Context image* columns to view high resolution images.

Example

The following examples illustrate how images are displayed in the reports:

1. If the **Enable high-resolution report images** check box is deselected:

2. If the **Enable high-resolution report images** check box is selected:



After you finish

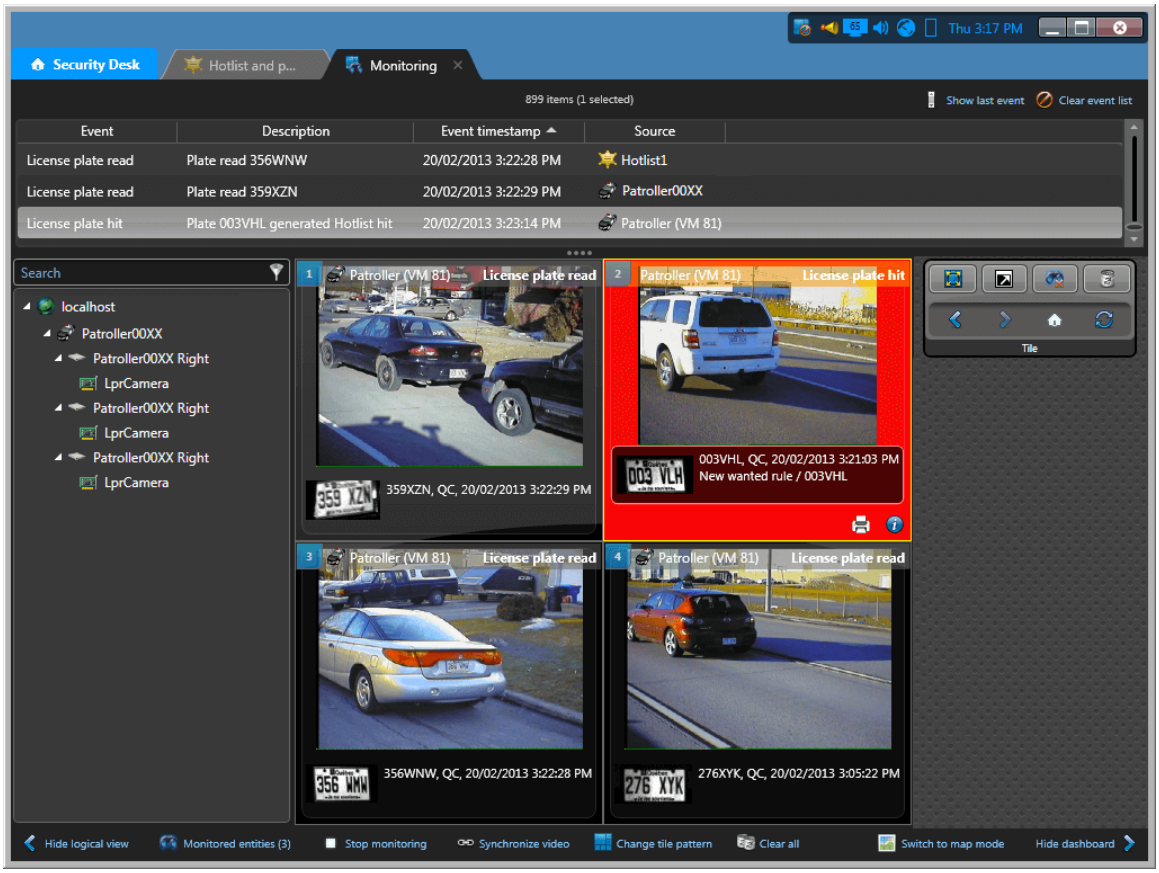
Repeat these steps on any Security Desk client machine that requires high resolution images to be displayed in the report pane columns.

Monitoring ALPR events in tile mode

By default, ALPR events are displayed in the canvas in tile mode, which allows you to view information about the read or hit, view the plate images from the events in high resolution, print hits, and so on, in individual tiles.

To monitor ALPR events in tile mode:

1 In the **Monitoring** task, select an ALPR event in a tile, or double-click an event from the event list.



The following information about the ALPR event is displayed in the tile by default:

- **Entity name:** Name of the entity you are monitoring, shown in the tile toolbar.
- **ALPR event name:** Event type (License plate read, License plate hit, and so on), shown in the tile toolbar.
- **Tile background color:**
  - *Black* (Default). Plate read event.
  - *Red* (Default). Hotlist hit event.
  - *Green* (Default). Permit hit event.
  - *Blue* (Default). Shared permit hit and overtime hit event.

NOTE: You can change the default colors of ALPR events from *hotlists*, *overtime rules*, and *permit restrictions* in Config Tool. For more information, see the *Security Center Administrator Guide*.

- **Context image:** Wide-angled image of the vehicle that was read by the *ALPR unit* context camera.
- **Plate image:** Image captured by the ALPR camera and the OCR interpretation from the event.
- **Plate number:** License plate number.
- **Plate state:** Origin of the license plate.
- **Date and time:** Date and time of the plate capture assigned to the hit rule that matched the plate.
- **Address:** Location of the unit when the plate image was captured.

  NOTE: The address is only shown if the *geocoder* module is enabled in Config Tool. If Genetec Patroller™ is not equipped with maps, then the address is only shown if the geocoder is enabled to resolve the GPS position.
- **(Hits only) Hit rule:** Hit rule that produced the hit.
- **(Overtime hits only) Tire/Overview image:** Wheel image captured by the *wheel-imaging* camera that is mounted at the back of the Genetec Patroller™ vehicle. Wheel images are only shown if the hit was captured by a Genetec Patroller™ that supports wheel imaging.

2 To check the digital signature of the ALPR event, right-click inside the tile, and then click **Verify digital signature**.

A valid digital signature confirms that an ALPR event has not been tampered with. Security Center adds a digital signature to all reads and hits recorded by fixed Sharps, and Genetec Patroller™ adds a digital signature to Sharps installed on the vehicle. A digital signature can have one of the following statuses:

- Valid ( ).
- Invalid ( ).
- If no icon is displayed, the digital signature has been tampered with.

3 (Hits only) To view more information about the hit, such as its hotlist attributes, click in the tile (user, accept or reject reason, plate state, and so on).

4 (Hits only) To print the event data as proof of the violation, click in the tile.

Related Topics

Printing hit reports on page 401

Monitoring ALPR events in map mode

You can use *map mode* in the *Monitoring* task to view all the ALPR events on a map.

What you should know

In map mode, the canvas displays a road map. The map opens centered on the location you zoomed in to, the last time you switched to map mode. You can use your mouse to pan or zoom on the map.

NOTE: The map mode can only be used to display static ALPR events. To show Genetec Patroller™ positions on a map, use the *Patrol vehicle tracking* task. To work with a general purpose map, display a map ( ) in a tile, or use the *Maps* task.

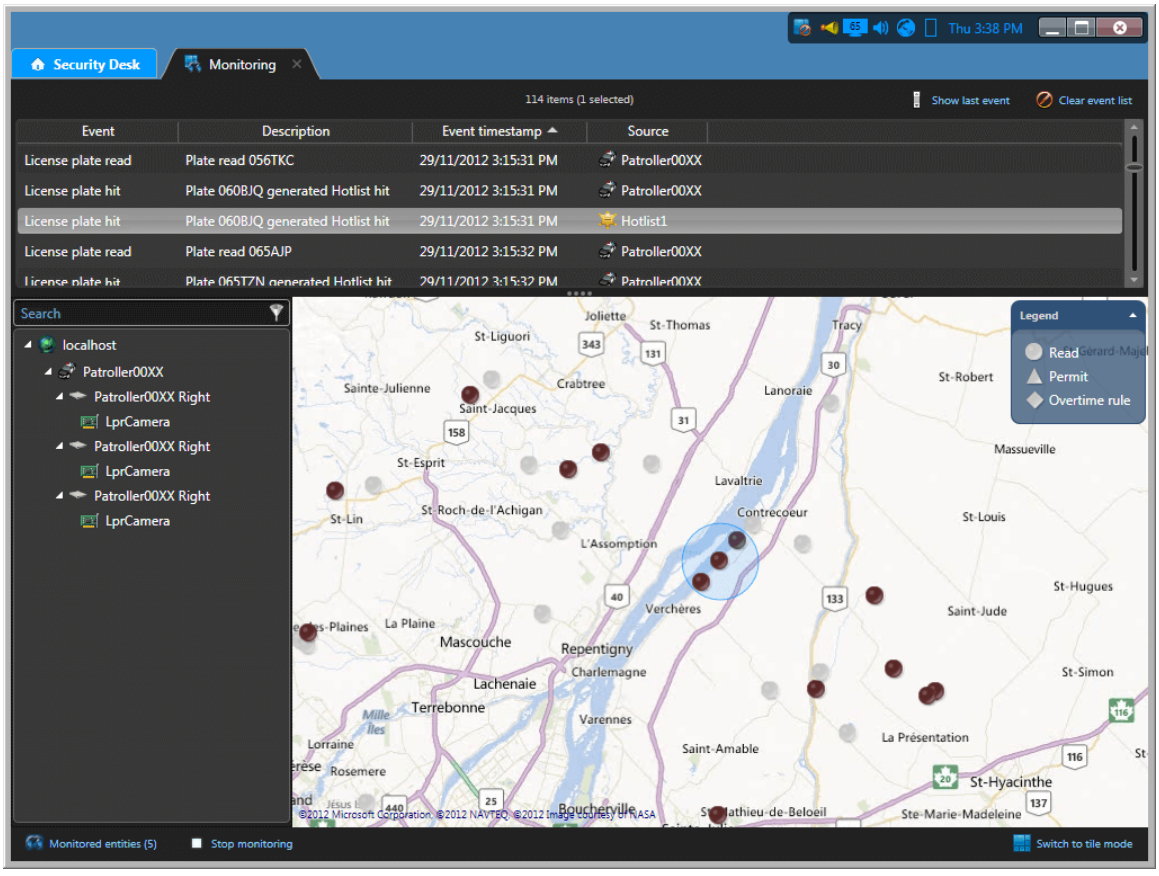
The following symbols represent each ALPR event type on the map:

- **Circle:** Reads and hotlist hits.
- **Triangle:** Permit reads and hits.
- **Diamond:** Overtime reads and hits.

You can change the default colors of ALPR events from *hotlist*, *overtime rule*, and *permit restriction* in Config Tool. For more information, see the *Security Center Administrator Guide*.

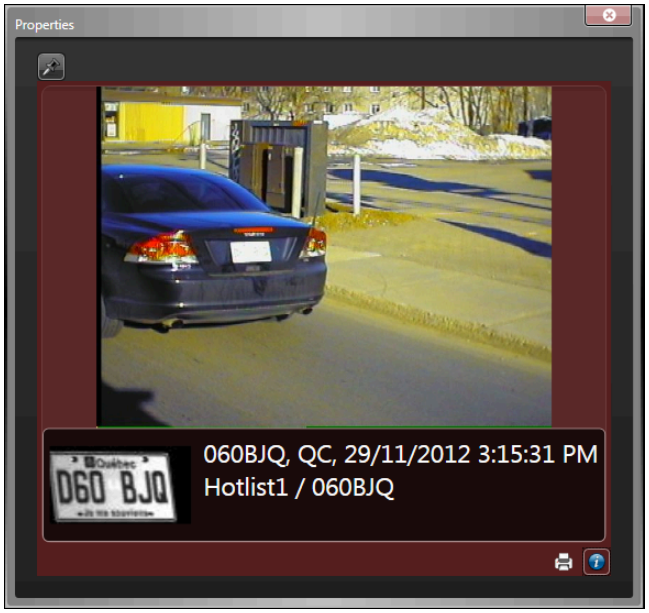
To monitor ALPR events in Map mode:

1 In the *Monitoring* task, click **Switch to map mode** ( ).



2 To find an event on the map, double-click the event in the event list.
The event location is displayed on the map and the event is circled.

3 To view information about the event, click the event on the map.



The *Properties* window opens. The event properties and commands shown in the *Properties* window are similar those available in *tile mode*.

4 To keep the *Properties* window open, click **Push pin** ( ).

Related Topics

Replaying patrol vehicle routes on page 444

23

Reads, hits, hotlists, and permits

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.

About permits

A permit is an entity that defines a single parking permit holder list. 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

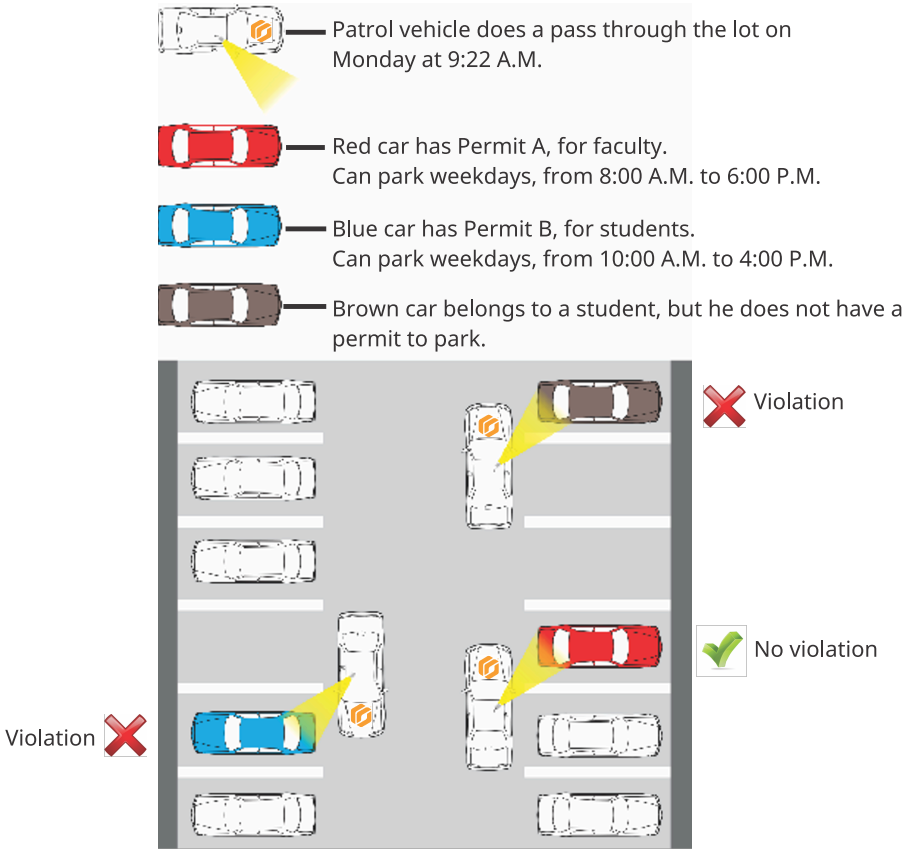
In City Parking Enforcement, you create the permit list and configure its basic properties, but you do not need to define a parking lot or permit restriction. It is the city or municipality that decides when and where the permit is applicable. The patrol vehicle operator chooses which permit to enforce in Genetec 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 Genetec 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.



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. Genetec 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 AutoVu™ Free-Flow on page 427.

Editing hotlists and permit lists

You can edit a *hotlist* or *permit* list using the *Hotlist and permit editor* task.

Before you begin

The hotlist or permit list must be created in Config Tool, the *Enable editor support* option in the entity's Properties tab must be selected, and the user or user groups editing the lists must be granted the required privileges. The changes you can make to a hotlist or permit list might be limited, depending on which privileges you have.

What you should know

Using the *Hotlist and permit editor*, you can add, edit, or delete items from existing lists that were created in *Config Tool*. When you edit a hotlist or permit list, the text file is updated and your patrol vehicles or Sharp cameras receive the new information.

The following conditions apply:

- Only the first 100,000 rows of a hotlist are loaded in Security Desk.
- If an error occurs while the hotlist is being loaded, the load stops and an error message is shown. However, you can still edit the lists that were loaded before the error occurred.

To edit a hotlist or permit list:

1 From the home page, open the **Hotlist and permit editor** task.
The available hotlists and permit lists are displayed in the column on the left.
2 Select the hotlist or permit list that you want to edit.
3 From the drop-down list, select an ALPR Manager, and click **Load**.
4 To find a specific row in the list, type the license plate number in the *Search* box.
5 Do one of the following:
   - To add a row to your list, click **Add** ().
   - To delete a row, select a row from your list, and then click **Remove** ().
   - To edit a row, click an individual item on your list.
6 Click **Save**.

The source file of the hotlist or permit list is updated with the changes.

Example

A hotlist of stolen vehicles is downloaded from the ministry of justice each night at midnight. Every morning, when the officers begin their shift, they load the latest hotlist into a Genetec Patroller™. During the day, some vehicles on the list are found, and new vehicles are stolen. You can remove the vehicles that were found from the list, and add the newly stolen vehicles, so that all the patrol vehicles have the updated hotlist.

Related Topics

Overview of the Hotlist and permit editor task on page 594

Hotlist annotation fields

Hit annotation fields are properties of a hit that are not displayed by default in Security Desk (for example, the vehicle's VIN or serial number). They can be fields that are extracted from the hotlist the plate was matched with, or they can be other fields, such as *UserEditedPlate*, custom fields, and so on.

Custom annotation fields are only available if they have been created in Config Tool. For information about adding annotation fields, see the *Security Center Administrator Guide*.

The following are examples of hotlist annotation fields:

- **{Category}:** For hotlist hits, the *Category* is the reason a license plate is of interest (for example, *Amber alert*, *Wanted felon*, *Stolen*, and so on). For *permit hits*, the *Category* is the type of permit (for example, *Zone 35*, *Zone 50*, and so on).

  NOTE: This is a mandatory field for hotlists and *permits*. The category is taken from the hotlist or permit list that the license plate is matched against. For a *new wanted* license plate, the category is defined in the ALPR settings *new wanted* categories and downloaded to a Genetec Patroller™. When a *new wanted* license plate is entered manually in Genetec Patroller™, the user selects the appropriate *Category* from the downloaded list.
- **{MatchPlate}:** The plate number as it appears in the hotlist.
- **{PlateState}:** The plate state/province as it appears in the hotlist.
- **{EffectiveDate}:** The hotlist is effective from this date.
- **{ExpiryDate}:** The hotlist expires on this date.
- **{UserEditedPlate}:** The license plate was edited manually.

Investigating reported hits

You can investigate *hits* reported within a time range and geographic area, using the *Hits* report.

Before you begin

To view your query results in the canvas, you must know how to monitor ALPR events in Security Desk in map mode.

What you should know

If you must report on all the hits that occurred in a specific region at a certain time, you can select the region, and the time range. If you want to see how many hits one Genetec Patroller™ got during their shift, you can search for that Genetec Patroller™, and set a time range. If you want to see if a Genetec Patroller™ got a hit on a specific license plate, you can search for that license plate.

To investigate reported hits:

1 From the home page, open the **Hits** task.

2 To restrict your search to one or more specific areas, draw one or more regions in your map as follows:
   a) In the *Filters* tab, click the **Region** filter.
   b) Click **Switch to map mode**.
   c) In the **Region** filter, click **Draw region**.
   d) Drag your mouse pointer to create a box.
      A numbered **Region** box is created.
   e) To resize the region, drag the box handles.
   f) To move the region, hold down the mouse button and drag the box to a new location.
   g) Create other regions as required.
   h) Select the regions of interest.
      To view all the regions you created, click  in the *Filters* tab.

3 Set up the query filters for your report:

- **Accept reasons:** Reason selected by the Genetec Patroller™ user when enforcing a hit. Accept reasons are created and customized in Config Tool.
- **Action taken:** Genetec Patroller™ hit actions (Accepted, Rejected, Not enforced) selected by the Genetec Patroller™ user. For fixed Sharps, a hit raised by the Hit Matcher module is always automatically Accepted and Enforced.
- **Annotation fields:** Genetec Patroller™ hit annotations used by the Genetec Patroller™ user.
- **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. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
- **Hit rules:** Select the hit rules to include in the report.
- **Hit type:** Select the type of hits to include in the report: *Permit*, *Shared permit*, *Overtime*, and *Hotlist*.
- **License plate:** Enter a full or partial license plate number. To enter multiple license plates, see Filtering a report with multiple license plates on page 417
- **ALPR units - Patrollers:** Restrict the search to Genetec Patroller™ units (including all their fitted ALPR units) and ALPR units representing fixed Sharp cameras on the Genetec Patroller™ unit.
- **Offload timestamp:** The date and time that the Genetec Patroller™ offloaded the reads/hits to Security Center.
- **Protection status:** Restrict the search to protected or unprotected hit events.
- **Reject reason:** Reason selected by the Genetec Patroller™ user when rejecting a hit. Reject reasons are created and customized in Config Tool. This filter only affects the value in the *Rejected hits* column.
- **Users:** Select the Patroller user name, or the Patrollers' parent user groups.

4 Click **Generate report**.

The hits are listed in the report pane.

5 (Optional) To view high resolution images in the *Plate image* and *Context image* columns, expand the corresponding column width. For more information, see Customizing ALPR image quality displayed in report pane columns on page 386

6 View your query results in the canvas, in one of the following modes:

- **tile mode:** To show the ALPR event in a tile, double-click or drag the item from the report pane to the canvas.
- **map mode:** To locate an ALPR event on the map, double-click the item in the report pane.

After you finish

Print a hit for proof of violation if required.

Related Topics

About license plate filters on page 415

Report pane columns for the *Hits* task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Hits task.

- **Accept reasons:** Reason selected by the Genetec Patroller™ user when enforcing a hit. Accept reasons are created and configured in Config Tool.
- **Address:** Location of the ALPR read.
- **Annotation fields:** Any annotation field defined in **System** > **ALPR Settings** in the Config Tool. Shown in brackets.
- **Context image:** Wide angle color image of the vehicle that was captured by the context camera.
- **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, IO module, Strike relay, etc.).
- **Event timestamp:** Date and time that the event occurred.
- **Latitude:** The coordinates of where the ALPR event occurred.
- **Longitude:** The coordinates of where the ALPR event occurred.
- **Offload timestamp:** The date and time that the patrol vehicle offloaded the reads and hits to Security Center.
- **Patroller entity:** Patroller entity name. The patroller entity name field is not populated for fixed SharpV cameras.
- **Plate image:** The license plate image captured by the ALPR camera.
- **Plate origin:** State that issued the license plate.
- **Plate read:** The license plate read generated by the Sharp unit.
- **Protected:** Indicates that the record will not be deleted from the database when the retention period (for this type of record) expires.
- **Protection expiration:** Indicates when protection for the hit expires.
- **Reject reason:** Reason selected by the Genetec Patroller™ user when rejecting a hit.
- **Rule:** Hit rule that matched the plate read.
- **ALPR Unit:** The ALPR unit that read the plate and populated for a patrol vehicle (for example, Patroller - Left, Patroller - Right, etc.), and for a fixed Sharp.
- **User:** The Genetec Patroller™ user name. Not available at a Security Center Federation™ host for federated Genetec Patroller™ entities.
- **Wheel image:** Image of the vehicle wheels. Used for virtual tire-chalking.

Investigating reported hit statistics

You can quickly investigate hit statistics within a time range and geographic area, using the hits statistics report.

What you should know

To view your query results in the canvas, you must know how to monitor ALPR events in Security Desk.

To investigate reported hit statistics:

1 From the home page, open the *Hits* task.

2 To restrict your search to one or more specific areas, draw one or more regions in your map as follows:

a) In the *Filters* tab, click the **Region** filter.

b) Click **Switch to map mode**.

c) In the **Region** filter, click **Draw region**.

d) Drag your mouse pointer to create a box.

A numbered **Region** box is created.

e) To resize the region, drag the box handles.

f) To move the region, hold down the mouse button and drag the box to a new location.

g) Create other regions as required.

h) Select the regions of interest.

To view all the regions you created, click  in the *Filters* tab.

3 Set up the other query filters for your report. Choose one or more of the following filters:

- **Accept reasons:** Reason selected by the Genetec Patroller™ user when enforcing a hit. Accept reasons are created and customized in Config Tool.
- **Action taken:** Genetec Patroller™ hit actions (Accepted, Rejected, Not enforced) selected by the Genetec Patroller™ user. For fixed Sharps, a hit raised by the Hit Matcher module is always automatically Accepted and Enforced.
- **Annotation fields:** Genetec Patroller™ hit annotations used by the Genetec Patroller™ user.
- **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. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
- **Hit rules:** Select the hit rules to include in the report.
- **Hit type:** Select the type of hits to include in the report: *Permit*, *Shared permit*, *Overtime*, and *Hotlist*.
- **License plate:** Enter a full or partial license plate number. To enter multiple license plates, see Filtering a report with multiple license plates on page 417
- **ALPR units - Patrollers:** Restrict the search to Genetec Patroller™ units (including all their fitted ALPR units) and ALPR units representing fixed Sharp cameras on the Genetec Patroller™ unit.
- **Offload timestamp:** The date and time that the Genetec Patroller™ offloaded the reads/hits to Security Center.
- **Reject reason:** Reason selected by the Genetec Patroller™ user when rejecting a hit. Reject reasons are created and customized in Config Tool. This filter only affects the value in the *Rejected hits* column.
- **Users:** Select the Patroller user name, or the Patrollers' parent user groups.

4 Expand the options under the **Generate report** button and select **Generate report statistics**.

The hits are listed in the report pane.

Example

If you must quickly report how many hits occurred in a specific region at a certain time, you can select the region, and the time range.

Printing hit reports

You can print a *Hits-Photo evidence* report for License plate hit events from the Monitoring task and other ALPR tasks.

What you should know

The printed report includes the current date, hit information (plate number, GPS coordinates, address, hit date, hit type, and so on), the ALPR image, the context image, wheel images (if applicable), and the map context.

To print a hit report:

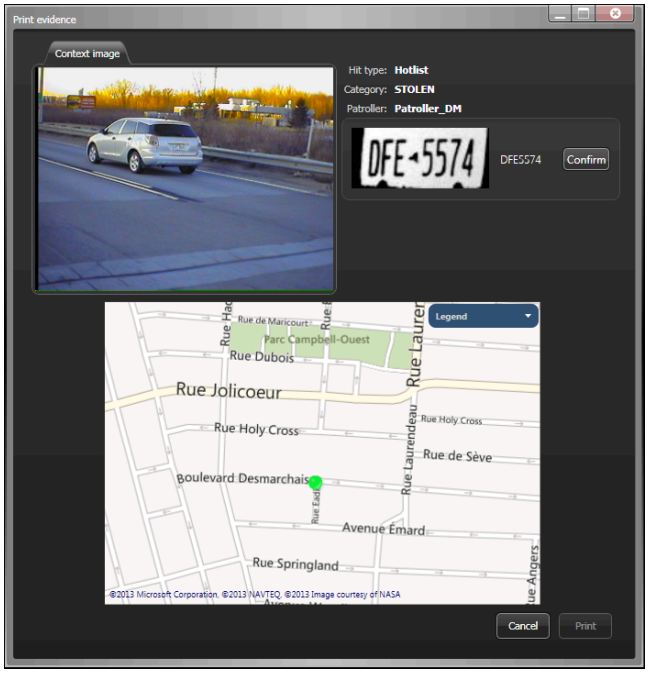
1 From the home page, open the Monitoring task or an ALPR task.

2 If needed, generate your report.

3 Select a hit event in a tile or on the map.

4 In the tile or *Properties* window, click .

5 In the *Print evidence* dialog box, confirm the license plate number so you do not print a false read.

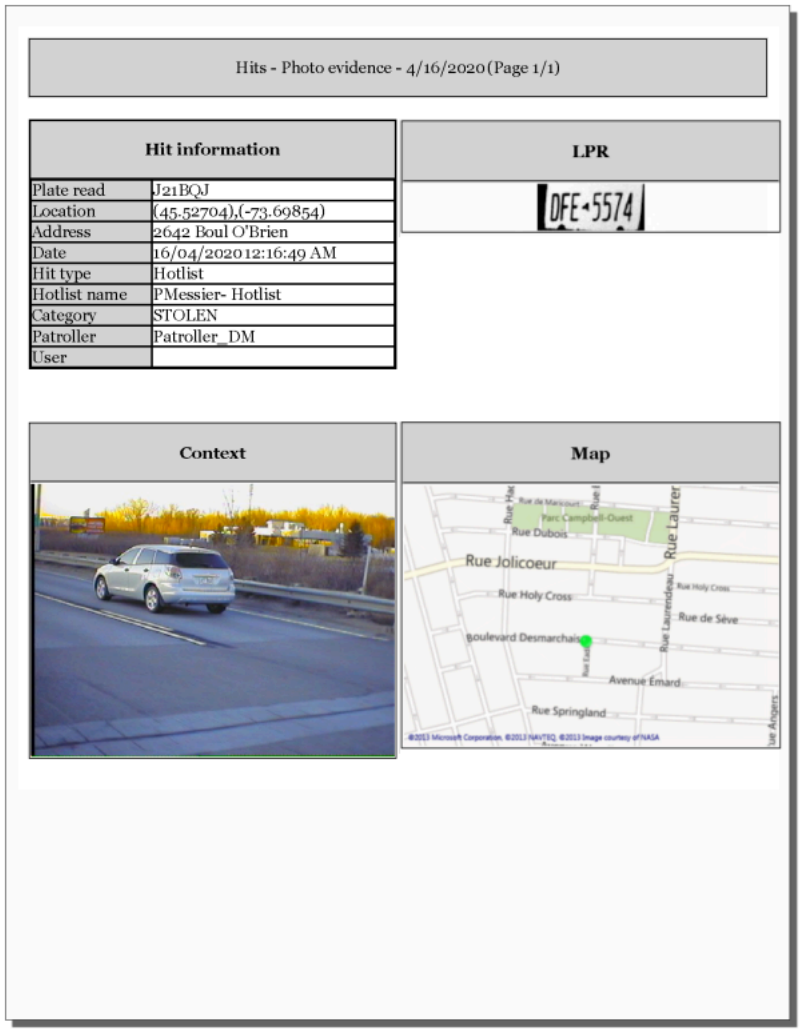


6 Confirm that the OCR interpretation matches the ALPR image.

7 In the text box, type the license plate number, and then click **Confirm**.

8 Click **Print**, select a printer, and then click **Print**.

The *Hits-Photo evidence* report is printed.



Hits - Photo evidence - 4/16/2020 (Page 1/1)

Hit information	
Plate read	J21BQJ
Location	(45.52704),(-73.69854)
Address	2642 Boul O'Brien
Date	16/04/2020 12:16:49 AM
Hit type	Hotlist
Hotlist name	PMessier- Hotlist
Category	STOLEN
Patroller	Patroller_DM
User	

LPR

Context

Map

Editing license plate reads

In certain situations, you may need to modify a plate read in Security Desk. This may be necessary if you notice that the system has incorrectly captured a plate read, or if the system prompts you to verify a plate read that is unclear (low confidence score).

What you should know

- Depending on your user privileges, you can modify plate reads that are displayed in tiles. You can edit plate reads in *Reads* reports, *Reads (Multi-region)* reports, monitoring tiles, and in alarms triggered by license plate read events.
- You cannot edit a plate read if the read is protected, a hit, or if the read is from a federated system or an MLPI inventory.
- When a plate read is edited, if there is a confidence score associated with the plate read, the confidence score is changed to 100%.
- The details of the plate read edit appear in the *Activity trails* report.
- If you are editing plate reads in an AutoVu™ Free-Flow system, see Editing license plate reads in a parking zone on page 434.

To edit a plate read:

1 From the license plate read tile, click **Modify** ( ).

NOTE: If you are trying to modify a plate read in a *Reads* report, you must first double-click the read to display it in a tile.

2 In the *Edit read* window, manually modify the **Plate** and **State** information as required.

3 Click **Save**.

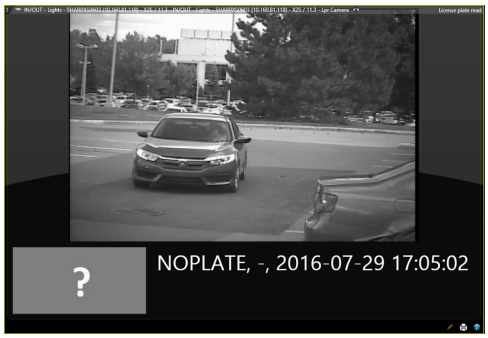
In *Reads* reports, the **Edited** column shows you if the plate read has been edited. For more information on displaying columns, refer to the Reporting task workspace overview.

Investigating NOPLATE reads

If a Sharp camera fails to capture a plate when it is configured to use the **Continuous with virtual loop** or **Single read on trigger** reading mode, no ALPR image is associated with the read, and the plate number appears as *NOPLATE*.

What you should know

- If the camera fails to capture a plate, no ALPR image is associated with the read and the plate number *NOPLATE* is associated with the read. This reading mode is appropriate for maintaining higher vehicle count accuracy in parking lots when recording occupancy, particularly in areas or in seasons that might have a higher rate of no read events (for example, in muddy or snowy weather conditions). For more information, see Editing license plate reads on page 403.



- You cannot edit a plate read if the read is protected, or if the read is from a federated system or an MLPI inventory.
- When a plate read is edited, if there is a confidence score associated with the plate read, the confidence score is changed to 100%.
- The details of the plate read edit appear in the *Activity trails* report.
- If the system generates too many NOPLATE reads (one car generates multiple NOPLATE reads, or a vehicle is detected but does not appear in the image) or too few NOPLATE reads (vehicles that pass the camera are not detected), you can recalibrate the Sharp camera's virtual loop feature. For more information refer to the administrator guide for your Sharp camera.

To investigate *NOPLATE* reads:

1. From the home page, open the *Reads* task.
2. From the **ALPR units - Patrollers** list, select the camera to investigate.
3. Select the **License plate** filter and enter `NOPLATE`.
4. Click **Generate report**.

   Reads with no associated plate number are listed in the report pane.
5. If the vehicle's plate is visible in the context image, you can edit the plate read to include the correct plate number.
   a) Double-click the read to display it in a tile.
   b) From the license plate read tile, click **Modify** ( ).
   c) In the *Edit read* window, manually modify the plate information as required.
   d) Click **Save**.

Investigating reported license plate reads

Using the *Reads* report, you can find license plate reads that were reported within a time range and geographic area. You can also perform vehicle analytics reporting for attributes such as vehicle color and vehicle type.

Before you begin

To view your query results in the canvas, you must know how to monitor ALPR events in Security Desk in map mode.

What you should know

If you must report on all the reads that occurred in a specific region at a certain time, you can select the region, and the time range. If you want to see how many reads a Genetec Patroller™ got during their shift, you can search for that Genetec Patroller™, and set a time range. If you want to see if a Genetec Patroller™ got a read on a specific license plate, you can search for that license plate.

To investigate reported license plate reads:

1 From the home page, open the *Reads* task.

2 To restrict your search to one or more specific areas, draw one or more regions in your map as follows:
   a) In the *Filters* tab, click the **Region** filter.
   b) Click **Switch to map mode**.
   c) In the **Region** filter, click **Draw region**.
   d) Drag your mouse pointer to create a box.
      A numbered **Region** box is created.
   e) To resize the region, drag the box handles.
   f) To move the region, hold down the mouse button and drag the box to a new location.
   g) Create other regions as required.
   h) Select the regions of interest.
      To view all the regions you created, click  in the *Filters* tab.

3 Set up the other query filters for your report. Choose one or more of the following filters:
   - **Annotation fields:** Add one or more filters to refine the search results in the *Reads* report:

- **{State Name}:** Select the plate state/province to investigate.
- **{Confidence Score}:** Specify the desired accuracy percentage for the reads.
- **{Relative Motion}:** Select whether the vehicle is moving away from or approaching the camera.
- **{Speed}:** Specify a speed limit you want to investigate.
- **{Character Height}:** Specify the desired pixel value.
- **{Context}:** Select the LPR context you want to investigate.

- **Generated a hit:** Include reads that generated a hit in the report.
- **Hit rules:** Select the hit rules to include in the report.
- **License plate:** Enter a full or partial license plate number. To enter multiple license plates, see Filtering a report with multiple license plates on page 417
- **ALPR units - Patrollers:** Restrict the search to Genetec Patroller™ units (including all their fitted ALPR units) and ALPR units representing fixed Sharp cameras on the Genetec Patroller™ unit.
- **Offload timestamp:** The date and time that the Genetec Patroller™ offloaded the reads/hits to Security Center.
- **Protection status:** Restrict the search to protected or unprotected read events.
- **Rule:** Hit rule that matched the plate read.
- **Users:** Select the Patroller user name, or the Patrollers' parent user groups.
- **Vehicle color:** Enter a vehicle color. To investigate multiple vehicle colors, choose from one of the following methods:
  - Enter values separated by a semi-colon (;) or a comma (,)
  - Enter the first character and select values from the auto-complete suggestions in the drop-down menu
- **Vehicle make:** Enter a vehicle make, for example, 'Toyota'. To investigate multiple vehicle makes, choose from one of the following methods:
  - Enter values separated by a semi-colon (;) or a comma (,)
  - Enter the first character and select values from the auto-complete suggestions in the drop-down menu
- **Vehicle type:** Enter a vehicle type, for example, 'Truck'. To investigate multiple vehicle types, choose from one of the following methods:
  - Enter values separated by a semi-colon (;) or a comma (,)
  - Enter the first character and select values from the auto-complete suggestions in the drop-down menu

4 Click **Generate report**.

The reads are listed in the report pane.

5 (Optional) To view high resolution images in the *Plate image* and *Context image* columns, expand the corresponding column width. For more information, see Customizing ALPR image quality displayed in report pane columns on page 386

6 View your query results in the canvas, in one of the following modes:

- **tile mode:** To show the ALPR event in a tile, double-click or drag the item from the report pane to the canvas.
- **map mode:** To locate an ALPR event on the map, double-click the item in the report pane.

Related Topics

About license plate filters on page 415

Report pane columns for the Reads task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Reads task.

- **Address:** Location of the ALPR read.

- **Context image:** Wide angle color image of the vehicle that was captured by the context camera.
- **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, IO module, Strike relay, etc.).
- **Event timestamp:** Date and time that the event occurred.
- **Generated a hit:** Indicates if the read generated a hit with a check mark.
- **Latitude:** The coordinates of where the ALPR event occurred.
- **Longitude:** The coordinates of where the ALPR event occurred.
- **Lot:** Parking zone where a given parking regulation is in force.
- **Manual capture:** Displays the plate number entered manually by the Genetec Patroller™ user.
- **Offload timestamp:** The date and time that the patrol vehicle offloaded the reads and hits to Security Center.
- **Patroller entity:** Patroller entity name. The patroller entity name field is not populated for fixed SharpV cameras.
- **Permit name:** Name of the permit list under the permit restriction.
- **Plate image:** The license plate image captured by the ALPR camera.
- **Plate origin:** State that issued the license plate.
- **Plate read:** The license plate read generated by the Sharp unit.
- **Protected:** Indicates that the record will not be deleted from the database when the retention period (for this type of record) expires.
- **Protection expiration:** Indicates when protection for the read expires.
- **Rule:** Hit rule that matched the plate read.
- **ALPR Unit:** The ALPR unit that read the plate and populated for a patrol vehicle (for example, Patroller - Left, Patroller - Right, etc.), and for a fixed Sharp.
- **Vehicle color:** Color of the vehicle captured in the read.
- **Vehicle make:** Make of the vehicle captured in the read.
- **Vehicle type:** Type of vehicle captured in the read.
- **Wheel image:** Image of the vehicle wheels. Used for virtual tire-chalking.

Investigating reported read statistics

You can quickly investigate read statistics within a time range and geographic area, using the reads statistics report.

What you should know

To view your query results in the canvas, you must know how to monitor ALPR events in Security Desk.

To investigate reported read statistics:

1 From the home page, open the *Reads* task.

2 To restrict your search to one or more specific areas, draw one or more regions in your map as follows:

a) In the *Filters* tab, click the **Region** filter.

b) Click **Switch to map mode**.

c) In the **Region** filter, click **Draw region**.

d) Drag your mouse pointer to create a box.

A numbered **Region** box is created.

e) To resize the region, drag the box handles.

f) To move the region, hold down the mouse button and drag the box to a new location.

g) Create other regions as required.

h) Select the regions of interest.

To view all the regions you created, click in the *Filters* tab.

3 Set up the other query filters for your report. Choose one or more of the following filters:

- **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.
- **Generated a hit:** Include reads that generated a hit in the report.
- **Hit rules:** Select the hit rules to include in the report.
- **License plate:** Enter a full or partial license plate number. To enter multiple license plates, see Filtering a report with multiple license plates on page 417
- **ALPR units - Patrollers:** Restrict the search to Genetec Patroller™ units (including all their fitted ALPR units) and ALPR units representing fixed Sharp cameras on the Genetec Patroller™ unit.
- **Offload timestamp:** The date and time that the Genetec Patroller™ offloaded the reads/hits to Security Center.
- **Rule:** Hit rule that matched the plate read.
- **Users:** Select the Patroller user name, or the Patrollers' parent user groups.

4 Click the small arrow on the right of the **Generate report** button and select **Generate report statistics**.

The read count is listed in the report pane.

Example

If you must quickly report how many reads occurred in a specific region at a certain time, you can select the region, and the time range.

Investigating reported reads (Multi-region)

You can view the number of reads common to multiple regions of interest for a specific time period, using the *Reads (Multi-region)* report.

What you should know

To view your query results in the canvas, you must know how to monitor ALPR events in Security Desk.

To investigate the reads for multiple regions:

1 From the home page, open the **Reads (Multi-region)** task.

2 To restrict your search to one or more specific areas, draw one or more regions in your map as follows:

a) In the *Filters* tab, click the **Region** filter.
b) Click **Switch to map mode**.
c) In the **Region** filter, click **Draw region**.
d) Drag your mouse pointer to create a box.
A numbered **Region** box is created.
e) To resize the region, drag the box handles.
f) To move the region, hold down the mouse button and drag the box to a new location.
g) Create other regions as required.
h) Select the regions of interest.
To view all the regions you created, click  in the *Filters* tab.

3 Set up the other query filter for your report. Choose one or more of the following filters:

- **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. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
- **Hit rules:** Select the hit rules to include in the report.
- **License plate:** Enter a full or partial license plate number. To enter multiple license plates, see Filtering a report with multiple license plates on page 417
- **ALPR units - Patrollers:** Restrict the search to Genetec Patroller™ units (including all their fitted ALPR units) and ALPR units representing fixed Sharp cameras on the Genetec Patroller™ unit.
- **Protection status:** Restrict the search to protected or unprotected read events.

4 Click **Generate report**.
The reads that are common to all regions you have defined are listed in the report pane.

5 (Optional) To view high resolution images in the *Plate image* and *Context image* columns, expand the corresponding column width. For more information, see Customizing ALPR image quality displayed in report pane columns on page 386

6 View your query results in the canvas, in one of the following modes:

- **Tile mode:** To show the ALPR event in a tile, double-click or drag the item from the report pane to the canvas.
- **Map mode:** To locate an ALPR event on the map, double-click the item in the report pane.

Example

If you must report on all the reads that occurred in multiple regions for a specific time period, you can create multiple regions, and specify the time range.

Related Topics

About license plate filters on page 415

Report pane columns for the Reads (Multi-region) task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Reads (Multi-region) task.

- **Address:** Location of the ALPR read.
- **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.
- **Event timestamp:** Date and time that the event occurred.
- **ALPR Unit:** The ALPR unit that read the plate and populated for a patrol vehicle (for example, Patroller - Left, Patroller - Right, etc.), and for a fixed Sharp.
- **Manual capture:** Displays the plate number entered manually by the Genetec Patroller™ user.
- **Patroller entity:** Patroller entity name. The patroller entity name field is not populated for fixed SharpV cameras.
- **Plate read:** The license plate read generated by the Sharp unit.
- **Protected:** Indicates that the record will not be deleted from the database when the retention period (for this type of record) expires.
- **Protection expiration:** Indicates when protection for the read expires.
- **Rule:** Hit rule that matched the plate read.

Investigating reported hits (Multi-region)

You can view the number of hits common to multiple regions of interest for a specific time period, using the *Hits (Multi-region)* report.

What you should know

To view your query results in the canvas, you must know how to monitor ALPR events in Security Desk.

To investigate the hits for multiple regions:

1 From the home page, open the **Hits (Multi-region)** task.

2 To restrict your search to one or more specific areas, draw one or more regions in your map as follows:

a) In the *Filters* tab, click the **Region** filter.
b) Click **Switch to map mode**.
c) In the **Region** filter, click **Draw region**.
d) Drag your mouse pointer to create a box.
A numbered **Region** box is created.
e) To resize the region, drag the box handles.
f) To move the region, hold down the mouse button and drag the box to a new location.
g) Create other regions as required.
h) Select the regions of interest.
To view all the regions you created, click  in the *Filters* tab.

3 Set up the other query filter for your report. Choose one or more of the following filters:

- **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. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
- **Hit rules:** Select the hit rules to include in the report.
- **License plate:** Enter a full or partial license plate number. To enter multiple license plates, see Filtering a report with multiple license plates on page 417
- **ALPR units - Patrollers:** Restrict the search to Genetec Patroller™ units (including all their fitted ALPR units) and ALPR units representing fixed Sharp cameras on the Genetec Patroller™ unit.
- **Protection status:** Restrict the search to protected or unprotected hit events.

4 Click **Generate report**.
The reads that are common to all regions you have defined are listed in the report pane.

5 (Optional) To view high resolution images in the *Plate image* and *Context image* columns, expand the corresponding column width. For more information, see Customizing ALPR image quality displayed in report pane columns on page 386

6 View your query results in the canvas, in one of the following modes:

- **Tile mode:** To show the ALPR event in a tile, double-click or drag the item from the report pane to the canvas.
- **Map mode:** To locate an ALPR event on the map, double-click the item in the report pane.

Example

If you must report on all the hits that occurred in multiple regions for a specific time period, you can create multiple regions, and specify the time range.

Related Topics

About license plate filters on page 415

Report pane columns for the Hits (Multi-region) task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Hits (Multi-region) task.

- **Accept reasons:** Reason selected by the Genetec Patroller™ user when enforcing a hit. Accept reasons are created and configured in Config Tool.
- **Address:** Location of the ALPR read.
- **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.
- **Event timestamp:** Date and time that the event occurred.
- **ALPR Unit:** The ALPR unit that read the plate and populated for a patrol vehicle (for example, Patroller - Left, Patroller - Right, etc.), and for a fixed Sharp.
- **Patroller entity:** Patroller entity name. The patroller entity name field is not populated for fixed SharpV cameras.
- **Plate read:** The license plate read generated by the Sharp unit.
- **Protected:** Indicates that the record will not be deleted from the database when the retention period (for this type of record) expires.
- **Protection expiration:** Indicates when protection for the hit expires.
- **Rule:** Hit rule that matched the plate read.
- **User:** The Genetec Patroller™ user name. Not available at a Security Center Federation™ host for federated Genetec Patroller™ entities.

Investigating reported reads and hits per day

You can view the number of reads and hits per day for a specific date range, using the *Reads/hits per day* report.

What you should know

The statistics in this report helps you to assess the performance of Genetec Patroller™ installations and fixed Sharp cameras in the field. For example, if you want to see how efficient the location of a mounted fixed Sharp is, you can search for that Sharp, and set a time range of a week.

To investigate the reads/hits reported on a particular day:

1 From the home page, open the **Reads/hits per day** task.

2 Set up the query filter for your report. Choose one or more of the following filters:

- **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.
- **Hit rules:** Select the hit rules to include in the report.
- **Hit type:** Select the type of hits to include in the report: *Permit*, *Shared permit*, *Overtime*, and *Hotlist*.
- **ALPR units - Patrollers:** Restrict the search to Genetec Patroller™ units (including all their fitted ALPR units) and ALPR units representing fixed Sharp cameras on the Genetec Patroller™ unit.
- **Reject reason:** Reason selected by the Genetec Patroller™ user when rejecting a hit. Reject reasons are created and customized in Config Tool. This filter only affects the value in the *Rejected hits* column.
- **Time range:** The time range for the report.
- **Users:** Select the Patroller user name, or the Patrollers' parent user groups.

3 Click **Generate report**.

The read and hit events are listed in the report pane.

4 View the statistics on the total number of reads, hits, and hit actions taken during the selected time range in the *Statistics* section.

Report pane columns for the Reads/hits per day task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Reads/hits per day 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.
- **Enforced hits:** Number of enforced hits.
- **Hits:**

  Number of hits.

  NOTE: If the *Hit rules* and *Hit type* query filters are used, this value might not be the total number of hits in the day.
- **Not enforced hits:** Number of hits that were not enforced.
- **Reads:** Number of license plate reads.
- **Rejected hits:** Number of hits that were rejected.

Investigating reported reads and hits per parking zone

You can view the number of reads and hits per *parking zone* for a specific date range, using the *Reads/hits per zone* report.

What you should know

By viewing the activity within a parking zone, you can assess the performance of Genetec Patroller™ installations and fixed Sharp cameras in the field. For example, if you want to see how efficient the location of a mounted fixed Sharp is, you can search for that Sharp, and set a time range of a week.

To investigate the reads/hits reported in a parking zone:

1 From the home page, open the **Reads/hits per zone** task.

2 Set up the query filter for your report. Choose one or more of the following filters:

- **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.
- **Hit rules:** Select the hit rules to include in the report.
- **Hit type:** Select the type of hits to include in the report: *Permit*, *Shared permit*, *Overtime*, and *Hotlist*.
- **ALPR units - Patrollers:** Restrict the search to Genetec Patroller™ units (including all their fitted ALPR units) and ALPR units representing fixed Sharp cameras on the Genetec Patroller™ unit.
- **Reject reason:** Reason selected by the Genetec Patroller™ user when rejecting a hit. Reject reasons are created and customized in Config Tool. This filter only affects the value in the *Rejected hits* column.
- **Time range:** The time range for the report.
- **Users:** Select the Patroller user name, or the Patrollers' parent user groups.

3 Click **Generate report**.

The read and hit events are listed in the report pane.

4 View the statistics on the total number of reads, hits, and hit actions taken during the selected time range in the *Statistics* section.

Report pane columns for the Reads/hits per zone task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Reads/hits per zone 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.
- **Enforced hits:** Number of enforced hits.
- **Hits:**

  Number of hits.

  NOTE: If the *Hit rules* and *Hit type* query filters are used, this value might not be the total number of hits in the day.
- **Not enforced hits:** Number of hits that were not enforced.
- **Reads:** Number of license plate reads.
- **Rejected hits:** Number of hits that were rejected.
- **Time zone:** Time zone of the unit.

About license plate filters

When you generate a report that includes license plates captured by an ALPR camera, if you do not know the full license plate number, you can use asterisks (*) and question marks (?) to replace unknown characters.

The following Security Desk reports include the **License plate** filter which lets you include full or partial license plates:

- Hits report
- Hits (Multi-region) report
- Reads report
- Reads (Multi-region) report
- Inventory report
- Parking sessions report
- Parking zones report

Full

When you select **Full**, you can enter the full license plate. You can also enter the wildcard characters * and ? to represent unknown characters.

- **Asterisks (*):** You can enter one or more asterisks to represent one character, multiple characters, or no characters. For example, You know the plate starts with "A" and ends with "123", but you are not sure what is in the middle. Filtering for **A*123** would include the following plates in the report:

Plate number	Report results	Reason
AB 123	Included	One character appears between "A" and "123".
A**BC** 123	Included	Multiple characters appear between "A" and "123".

Plate number	Report results	Reason
A 123	Included	No characters appear between "A" and "123".
AB**C** 123**4**	Excluded	The plate does not end with "123".

- **Question mark (?):** You can enter one or more question marks to represent any single character. For example, if you can't remember the first or last character in the license plate, filtering for **?BC 12?** would include the following plates in the report:

Plate number	Report results	Reason
ABC 12**3**	Included	There is one character before and after "BC 12".
5BC 12**L**	Included	There is one character before and after "BC 12".
AABC 12**3**	Excluded	Each "?" can only represent one character.

- **Combination:** You can enter a combination of asterisks and question marks. For example, filtering for **A?C 1*** would include the following plates in the report:

Plate number	Report results	Reason
A**B**C 1**23**	Included	The "?" is replaced by "B" and there are characters after the "1".
A**2**C 1	Included	The "?" is replaced by "2" and there are no characters after the "1".
A**BB**C 1**23**	Excluded	Each "?" can only represent one character.

Partial

Select **Partial** if you do not know the beginning or end of the plate number. For example, the plate read ABC 123 would only be returned with the first two plate number examples below.

NOTE: You cannot use asterisks and question marks for partial license plates.

Partial plate search	Report results	Reason
123	ABC 123 is included	The missing characters come before "123".
C12	ABC 123 is included	The missing characters come before and after "C12".
ABC 23	ABC 123 is NOT included	The missing character is in the middle of "ABC23".

Multi-plate read and hit reports

If you want to investigate multiple license plates simultaneously, you can enter the desired license plate numbers using a delimiter. This feature is applicable for both full and partial license plate filter. For more information on how to enter multiple license plate numbers, see Filtering a report with multiple license plates on page 417

Filtering a report with multiple license plates

To investigate multiple license plates simultaneously in a report, you can enter the list of license plates using a delimiter in the license plate filter.

Before you begin

Ensure that you are familiar with the different combinations involving full and partial license plate numbers. For more details, see About license plate filters on page 415

What you should know

You can use one of the following delimiters to enter multiple license plate numbers in the filter:

- Semi-colon (;)
- Comma (,)
- Carriage Return Line Feed (\r\n)

Limitation: You might experience slow search speeds in the following conditions:

- You use a combination of wildcards on every license plate number entered.
- You have a huge volume of records to scan through for the selected time range. For example, you have selected a six month time period and the database has nearly half a million records that correspond to that time period.

To search for multiple license plates simultaneously:

1. From the home page, open the desired report task.

   Example: If you want to generate a Hits report, open the Hits task.

   NOTE: For the complete list of reports that use license plate filter, see About license plate filters on page 415

2. In the *Filters* tab, click the **License plate** filter.
3. Enter the desired license plate numbers separated by one of the following delimiters:
   - Semi-colon (;)
   - Comma (,)
   - Carriage Return Line Feed (\r\n)

   NOTE: These delimiters can be mixed and matched as desired.

4. Set up the following query filters for your report:
   - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
   - **ALPR units - Patrollers:** Restrict the search to Genetec Patroller™ units (including all their fitted ALPR units) and ALPR units representing fixed Sharp cameras on the Genetec Patroller™ unit.

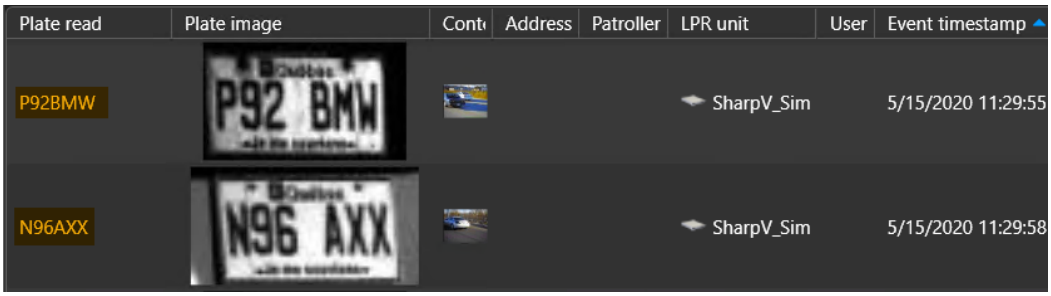
   NOTE: Additionally, you can set up the other query filters.

5. Click **Generate report**.

Example

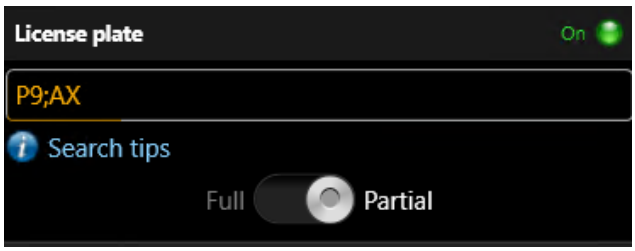
Following examples illustrate various ways to filter a report with multiple license plates:

1. Full license plate: In this example, a comma delimiter separates multiple complete license plate numbers.



2. Full plate with wildcard: In this example, the license plate numbers have wildcards and are separated with a carriage return line feed delimiter.

3. Partial plate: In this example, a semi colon delimiter separates multiple partial license plate numbers.


License plate
On
P9;AX
Search tips
Full
Partial

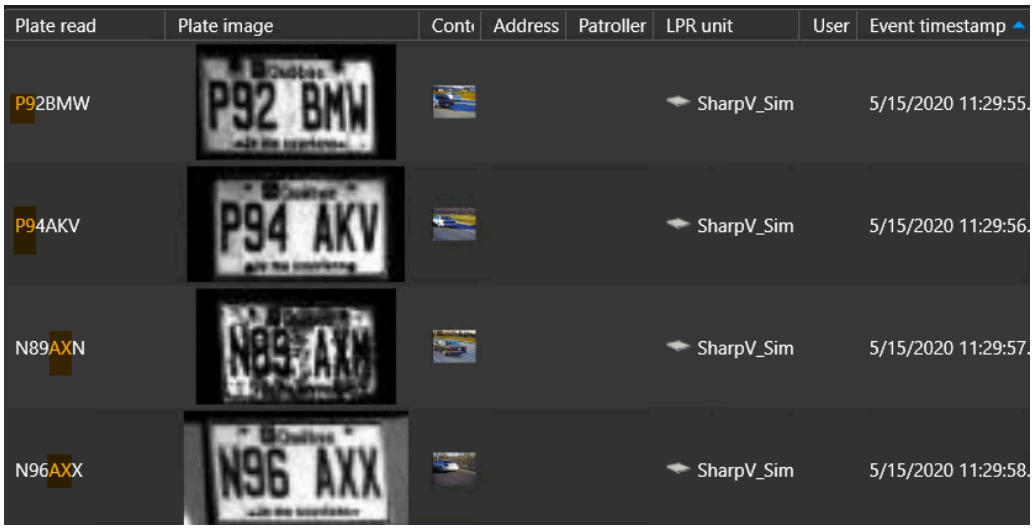


Plate read
Plate image
Conte
Address
Patroller
LPR unit
User
Event timestamp
P92BMW
SharpV_Sim
5/15/2020 11:29:55.
P94AKV
SharpV_Sim
5/15/2020 11:29:56.
N89AXN
SharpV_Sim
5/15/2020 11:29:57.
N96AXX
SharpV_Sim
5/15/2020 11:29:58.

Protecting reads and hits from being deleted

A Security Desk operator can protect an important read or hit from being deleted from the ALPR Manager database. This means that the read or hit is not deleted even after its configured retention period has ended.

Before you begin

In order to protect and unprotect reads and hits, the *Protect/Unprotect ALPR reads/hits* privilege is required.

What you should know

- You can protect reads and hits in the following tasks:
  - Hits
  - Hits (Multi-region)
  - Reads
  - Reads (Multi-region)
- You can use the **Protection status** filter to search for protected reads and hits in reports.
- You can see which users protected and unprotected reads and hits in the *Activity trails* task.

To protect a read or hit:

1 Open a Hits or Reads task.

2 Generate your report.

The hits or reads are listed in the report pane.

3 From the report pane, select the hit or read that you want to protect, and then click **Protect** ( ).

To select multiple events, hold the Ctrl or Shift keys.

4 In the *Protect selected results* dialog box, set how long to protect the read or hit.

- **Indefinitely:** No end date. You must remove the protection status manually by selecting the read or hit in the report pane, and then clicking **Unprotect** ( ).

  NOTE: When you unprotect a read or hit that exceeds the configured retention period, it is deleted and does not appear in reports.
- **During the next x days:** The read or hit is protected for the number of days that you select.
- **Until:** The read or hit is protected until the end of the date that you select.

  Example: If you protect the read or hit until 11/20/2016, it is deleted from the ALPR database on 11/21/2016 at 12:00 am.

5 Click **Protect**.

The read or hit is protected.

After you finish

Add the **Protected** and **Protection expiration** columns to your report so that you can see if hits and reads are protected, and when the protection expires. See Generating and saving reports on page 79

24

AutoVu™ Free-Flow

This section includes the following topics:

Parking zone management

Using the AutoVu™ Free-Flow feature in Security Desk, you can monitor the number of parked vehicles that are in violation in each parking zone. This lets you make decisions based on up-to-date information on parking zone inventory and capacity.

Sharp cameras can detect the license plates of passing vehicles. When Sharp cameras are installed at the entrances and exits of a parking zone, the system can track how long vehicles stay in the parking lot. When the rules of the parking lot are defined (for example, "free parking for one hour"), the system can show you which vehicles are in violation and must be issued a ticket.

About parking sessions

The AutoVu™ Free-Flow feature in Security Center uses parking sessions to track each vehicle's stay in a parking zone.

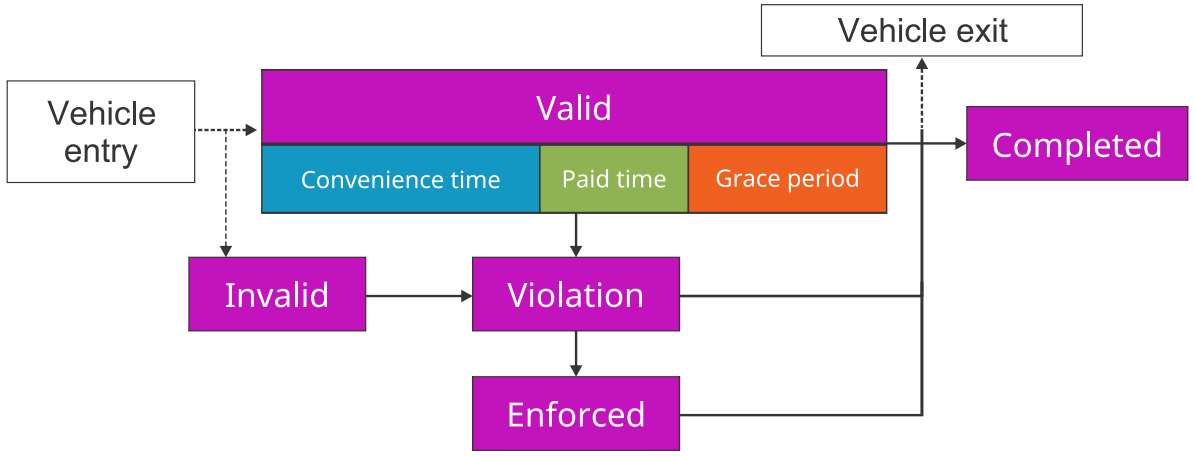
The following terms are important when setting up AutoVu™ Free-Flow parking zones:

- **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.

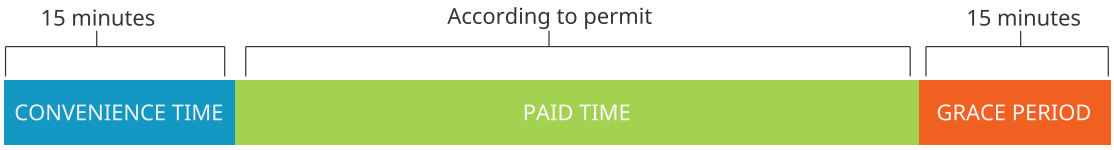
Common parking scenarios for AutoVu™ Free-Flow

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 AutoVu™ 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.

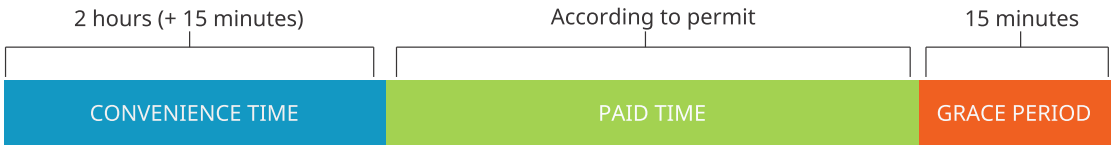


About this scenario:

- 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.

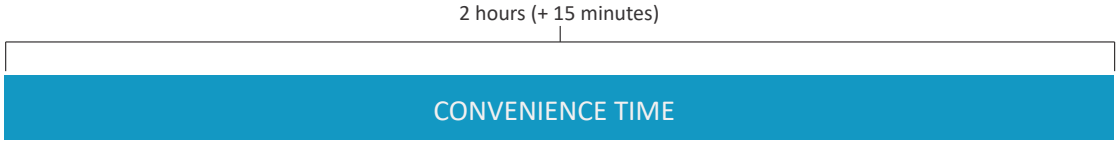


About this scenario:

- 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.

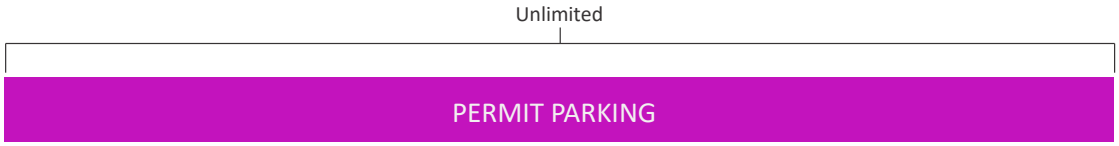


About this scenario:

- 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

About shared permits in AutoVu™ 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.

Monitoring parking zones

You can monitor parking zones from the *Monitoring* task. The *Monitoring* task tiles can display the parking zone occupancy and the number of violations. If additional surveillance cameras are linked to the parking zone, the tiles can also display their video feeds.

To monitor a parking zone in Security Desk:

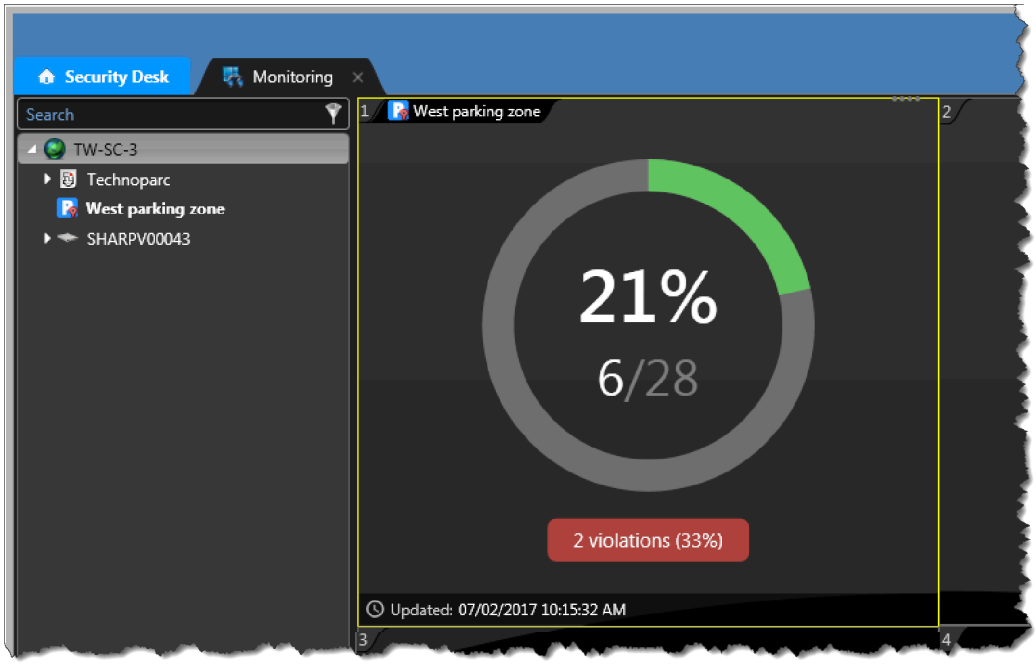
1 Open the *Monitoring* task.

2 Double click a parking zone from the area view, or drag a parking zone to a monitoring tile.

If no additional video cameras are linked to the parking zone, the following information is displayed in the tile:

- Parking zone name
- Current parking zone occupancy displayed as a ratio, a percentage, and a circle graph

  NOTE: The occupancy graph changes from green to orange when the parking zone reaches 70% occupancy. When the parking zone reaches 90% occupancy, the occupancy graph changes from orange to red and starts to flash.
- Current violations, expressed as both a number and a percentage of active parking sessions
- Time and date at which the tile information was updated

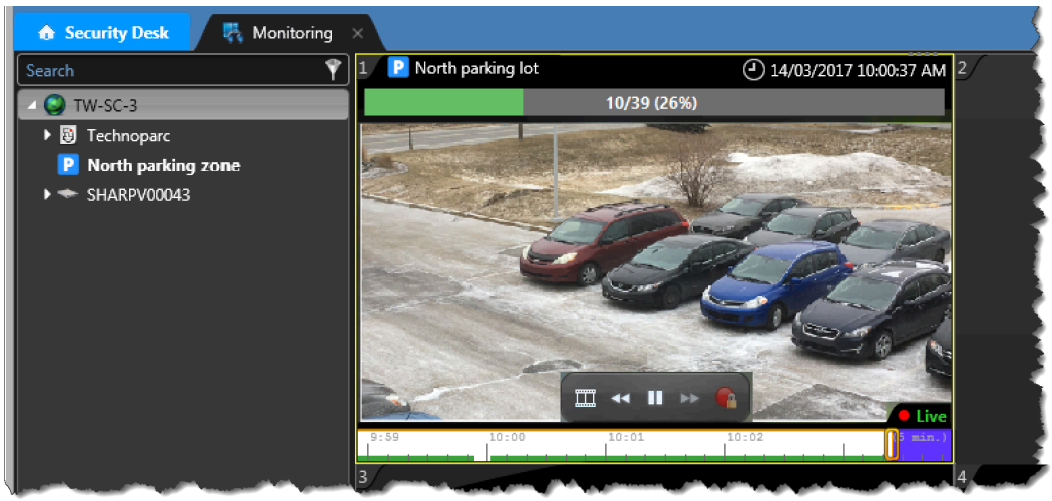


If additional video cameras are linked to the parking zone, the following information is displayed in the tile:

- Video feeds from linked surveillance video units

  NOTE: You can cycle the video feeds in the monitoring tile using the controls in the tile widget.
- Parking zone name
- The current parking zone occupancy displayed as a ratio, a percentage, and a bar graph above the video feed
- Current violations, expressed as both a number and a percentage of active parking sessions

  NOTE: The occupancy graph changes from green to orange when the parking zone reaches 70% occupancy. When the parking zone reaches 90% occupancy, the occupancy graph changes from orange to red and starts to flash.
- Time and date at which the tile information was updated



3 (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*.

AutoVu™ Free-Flow reports

Using the AutoVu™ Free-Flow reports, you can identify the vehicles that are parked in violation of the parking rules. These reports can be used when manually issuing tickets, or they can be used to export violations to a third-party ticketing system.

You can generate parking zone reports from the following reporting tasks:

- **Parking sessions:** The *Parking sessions* task gives you a real-time inventory of the parking sessions for vehicles that are currently in the parking zone, or that have already left the parking zone. 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 zone activities:** Using the *Parking zone activities* task, you can track the parking zone-related events that occur between the time the vehicle's plate is read at the entrance and the exit of the parking zone. This is the main task used for investigation purposes or for when a parking ticket is contested.

Investigating parking sessions

Security Desk tracks several parking session states related to a parked vehicle. Using these states, you can generate a list of vehicles that are currently in violation, or 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.

What you should know

- The *Parking sessions* task can also display information such as when the vehicle entered, when it left, how long it has been in violation, and whether the violation has been enforced.
- Parking zones that are displayed in a *Monitoring task* tile show the parking zone occupancy as well as the number of vehicles in violation.

To investigate the vehicle parking sessions that have occurred in a parking zone:

1. From the home page, open the *Parking sessions* task.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **Time selection:** This is the time range for the report. The time selection filter is useful for post-enforcement purposes. For example, you can generate a report that includes all of the completed parking sessions in the past 24 hours. You can then export the report to be processed by the payment system.

     You can set the following time filters:

     - **Time range:** Use the **During the last...** and **Specific range** filters to list all parking sessions that were started or completed within the given time range.
     - **Specific time:** Use the **Now** filter to generate a current inventory list, or use the **Specific date** filter to generate an inventory list for a point in the past.
   - **Parking Zone:** Select one or more parking zones to be included in the report.
   - **Minimum duration of stay:** Exclude vehicles from the report that have not exceeded the minimum duration of stay.
   - **Session state:** Select which of the following vehicle states to include in the report:
     - **Completed:** The vehicle's parking session is no longer active for one of the following reasons:
       - The vehicle has exited the parking zone.
       - The parking zone inventory has been reset.
       - The maximum inventory time has been reached.

NOTE: To determine if the parking session is in violation, refer to the violation timestamp in the *Parking sessions* report.

- **Enforced:** The vehicle is in the parking zone, is in violation, and has been issued a ticket.
- **Valid:** The vehicle is in the parking zone and is not in violation.
- **Violation:** The vehicle is in the parking zone, is in violation, and has not been issued a ticket.

- **State reason:** Select one or more state reasons to be included in the report.

  TIP: In AutoVu™ Free-Flow parking lots, because a violation can only be enforced if the vehicle is still in the parking lot, it is useful to exclude the **Vehicle exited** state reason from the parking sessions report.
- **License plate:** Enter a *Full* or *Partial* license plate number to generate a report on a specific vehicle.

3 Click **Generate report**.

The parking sessions are listed in the report pane.

4 To view the query results in the canvas, double-click or drag the event from the report pane to a tile on the canvas.

5 Print ( ) the report or export ( ) the report as an Excel, CSV, or PDF file.

Related Topics

About license plate filters on page 415

Report pane columns for the Parking sessions task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Parking sessions task.

- **Completed timestamp:** When the vehicle's parking session was completed. Typically, this occurs when the vehicle exited the parking zone.
- **Convenience time timestamp:** When the session's convenience time began (free parking period before parking enforcement takes effect).
- **Convenience time duration:** Duration of the vehicle's convenience time (free parking period before parking enforcement or paid time takes effect).
- **Enforced duration:** Duration of time that the vehicle was marked as enforced before the parking session was completed.
- **Enforced timestamp:** Time that the parking violation was enforced by an operator.
- **Entry context image:** The context image that was captured when the vehicle entered the parking zone.
- **Entry ALPR image:** The license plate image that was captured when the vehicle entered the parking zone.
- **Entry plate number:** The license plate number that was read when the vehicle entered the parking zone.
- **Exit context image:** The context image that was captured when the vehicle exited the parking zone.
- **Exit ALPR image:** The license plate image that was captured when the vehicle exited the parking zone.
- **Exit plate number:** The license plate number that was read when the vehicle exited the parking zone.
- **Grace period duration:** The duration of the vehicle's grace period. Following the expiration of the vehicle's convenience time or the paid period, the grace period is the extra time that is given before a vehicle is flagged as a violation.
- **Grace period timestamp:** The time that the vehicle's grace period began. Following the expiration of the vehicle's parking time, the extra time that is given before a vehicle is flagged as a violation.
- **Paid duration:** Duration of the vehicle's paid time in the parking zone.
- **Paid timestamp:** When the vehicle's paid time began.
- **Parking rule:** The parking rule that is associated with the parking zone in a parking session.
- **Parking zone:** The parking zone associated with a parking session.
- **Session state:** The state of the vehicle's parking session.
- **State reason:** Indicates the reason for the vehicle's session state.
- **Start timestamp:** Time that the vehicle's parking session began. Typically, this occurs when the vehicle enters the parking zone.

- **Total duration:** Total duration of stay from when the vehicle session was initially opened until it was closed.
- **Violation duration:** Duration of time the vehicle was in violation.
- **Violation timestamp:** Time that the vehicle was flagged as a violation.

Investigating parking zone activities

Using the *Parking zone activities* task, you can 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.

What you should know

You can use the *Parking zone activities* task to audit the activities for a single license plate or to investigate cases where vehicle owner contests a parking ticket.

To investigate the parking state events that have occurred for a vehicle in a parking zone:

1 From the home page, open the *Parking zone activities* task.

2 Set up the query filters for your report. Choose one or more of the following filters:

- **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
- **Parking Zone:** Select one or more parking zones to be included in the report.
- **License plate:** Enter a *Full* or *Partial* license plate number to generate a report on a specific vehicle.
- **Events:** Select the events of interest. The event types available depend on the task you are using.

For more information on the events and sub-events related to AutoVu™ Free-Flow, see Parking zone events on page 425.

3 Click **Generate report**.

The parking sessions are listed in the report pane.

4 To view the query results in the canvas, double-click or drag the event from the report pane to a tile on the canvas.

5 Print ( ) the report or export ( ) the report as an Excel, CSV, or PDF file.

Related Topics

About license plate filters on page 415

Report pane columns for the Parking zone activities report task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Parking zone activities task.

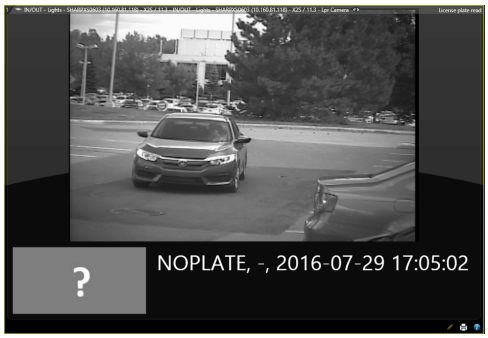
- **Context image:** Wide angle color image of the vehicle that was captured by the context camera.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **Expires:** When the selected activity expires, for example, when the convenience time or paid time expires.
- **Parking zone:** The parking zone associated with a parking session.
- **Plate image:** The license plate image captured by the ALPR camera.
- **Plate read:** The license plate read generated by the Sharp unit.

Editing license plate reads in a parking zone

If a Sharp camera that is monitoring an AutoVu™ Free-Flow parking zone misreads a plate or fails to capture a plate, you can edit the read so that the entrance and exit reads match.

What you should know

- This information applies to systems that use AutoVu™ Free-Flow. If you are not using this feature, see Editing license plate reads on page 403.
- If the camera fails to capture a plate, no ALPR image is associated with the read and the plate number *NOPLATE* is associated with the read. This ensures that all objects that pass through the camera's field of view are captured for review, thereby helping to maintain higher vehicle occupancy count accuracy in the parking zone. This is particularly useful in installations where there is a high chance of missed plate reads, for example, in muddy or snowy weather conditions.



- You cannot edit a plate read if the read is protected or if the read generated a hit.
- When a plate read is edited, if there is a confidence score associated with the plate read, the confidence score is changed to 100%.
- The details of the plate read edit appear in the *Activity trails* report.
- If the system generates too many NOPLATE reads (one car generates multiple NOPLATE reads, or a vehicle is detected but does not appear in the image) or too few NOPLATE reads (vehicles that pass the camera are not detected), it may indicate that there is a problem with the installation, for example, partial obstruction, bad lighting, bad positioning, or configuration issues. You might also need to recalibrate the Sharp camera's virtual loop feature. For more information refer to the administrator guide for your Sharp camera.
- You can edit plate reads from the following tasks:
  - Reads task
  - Monitoring task
  - Parking sessions task (not including NOPLATE reads)
  - Parking zone activities task (not including NOPLATE reads)
  - Alarm monitioring task (if alarms are configured for NOPLATE reads or reads with a low confidence score)

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.

To edit a plate read:

1 From the license plate read tile, click **Modify** ( ).

NOTE: If you are trying to modify a plate read in a *Reads* report, you must first double-click the read to display it in a tile.

2 In the *Edit read* window, manually modify the **Plate** and **State** information as required.
3 Click **Save**.

To investigate and edit a *NOPLATE* read:

1 From the home page, open the *Reads* task.
2 From the **ALPR units - Patrollers** list, select the camera to investigate.
3 Select the **License plate** filter and enter `NOPLATE`.
4 Click **Generate report**.
Reads with no associated plate number are listed in the report pane.
5 If the vehicle's plate is visible in the context image, you can edit the plate read to include the correct plate number.
   a) Double-click the read to display it in a tile.
   b) From the license plate read tile, click **Modify** ( ).
   c) In the *Edit read* window, manually modify the plate information as required.
   d) Click **Save**.

In *Reads* reports, the **Edited** column shows you if the plate read has been edited.

Enforcing parking zone violations

When vehicles in a parking zone are in violation, the steps required to enforce the violation depend on whether parking tickets are issued on-site by a parking attendant, or are issued by a third-party system.

What you should know

- This procedure is only required if the patrol vehicle cannot send live hits. Generally, Security Desk can monitor ALPR events from patrol vehicles and can automatically update the status of parking sessions.
- If parking tickets are manually issued while the vehicles are still in the parking zone, then every time a ticket is issued to a vehicle that is in *violation* (as indicated in the *Parking sessions* report), and the vehicle's parking session is marked as *enforced*, the violation count for the parking zone is decreased.
- If your AutoVu™ Free-Flow system uses a third-party ticketing system to enforce parking zone violations, then you do not need to flag parking sessions as *enforced* in the system.

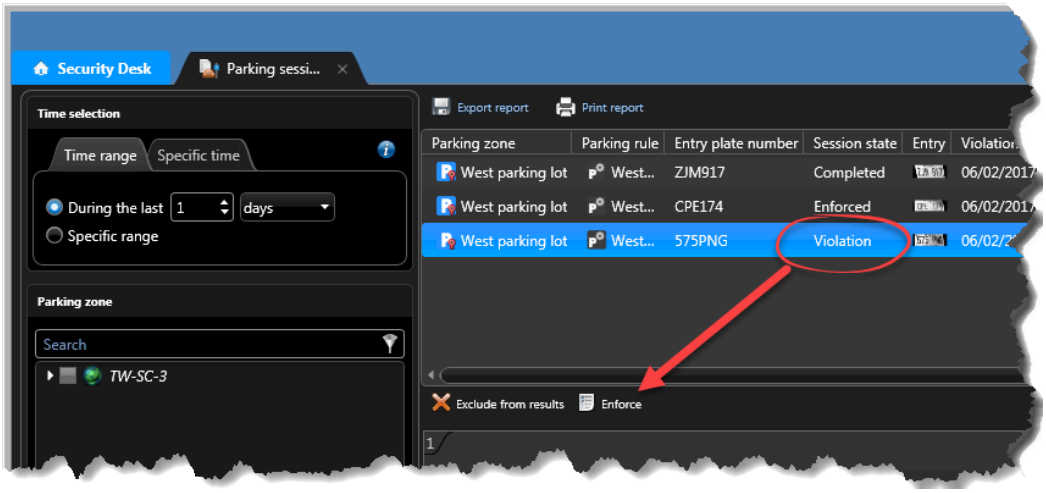
To enforce a parking session when tickets are issued on-site:

1 From the home page, open the *Parking sessions* task.

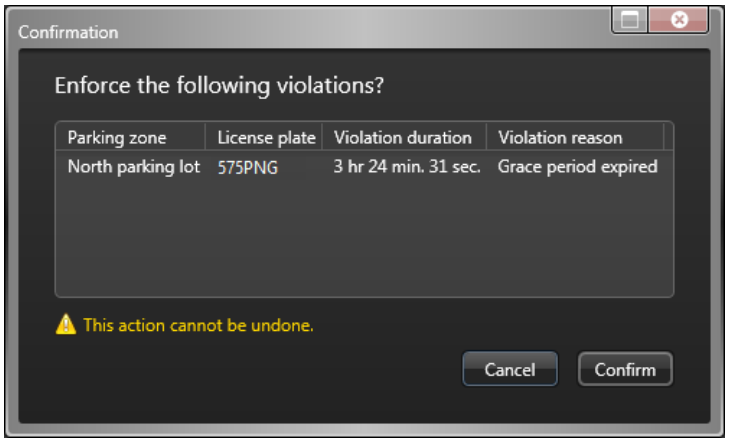
2 Generate a parking sessions report that displays the vehicles that are in violation.

3 Issue parking tickets for the vehicles that are in violation.

4 In the parking session report results, click each vehicle for which a parking ticket has been issued, and click **Enforce**.



5 In the *Confirmation* window, click **Confirm**.



To enforce a parking session when tickets are issued by a third-party system:

1 From the home page, open the *Parking sessions* task.

2 Generate a parking sessions report that displays the vehicles that are in violation.

3 Export (💾) the report as an Excel, CSV, or PDF file and send the report to the third-party ticketing system.

Resetting the inventory of a parking zone

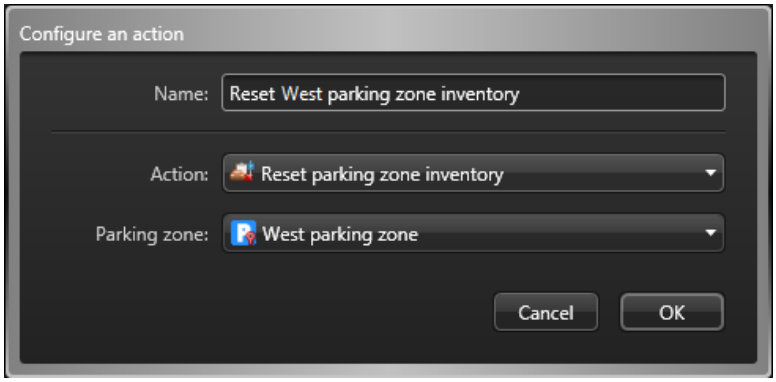
At a certain point (for example, when the parking lot closes) you can assume that all parking sessions have ended and that any vehicles remaining in the parking zone have been issued tickets or must be towed. You can reset the occupancy count of a parking zone using a hot action.

What you should know

Resetting the inventory ends all active parking sessions and removes all reported parking violations. To do this, you must create a hot action for the parking zone using the action *Reset parking zone inventory*.

To reset the inventory of a parking zone:

1. In the Security Desk notification tray, click **Hot actions** ( ).
2. In the *Hot actions* dialog box, click **Edit**.
3. Click **Add** ( ).
4. Enter a **Name** to appear in the hot actions list. For example, *Reset West parking zone inventory*.
5. From the **Action** drop-down list, select **Reset parking zone inventory**.
6. From the **Parking zone** drop-down list, select the parking zone you want to reset.



7. Click **OK**.
   The hot action is created, and the *Hot actions* dialog box closes.
8. To open the *Hot actions* dialog box again, click **Hot actions** ( ) in the notification tray.
9. (Optional) Click **Edit**. If you have more than one hot action created, click or to move the selected hot action up or down the list. This changes the function key that the action is assigned to.
10. Click **Done**.
    The hot action you created is listed with its assigned function key (F1, F2, and so on).
11. Trigger the hot action to reset the parking zone inventory in one of the following ways:
    - Select the hot action, and then click **Execute**.
    - Press Ctrl+F*n*.

Example

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

Closing parking sessions manually in Security Center

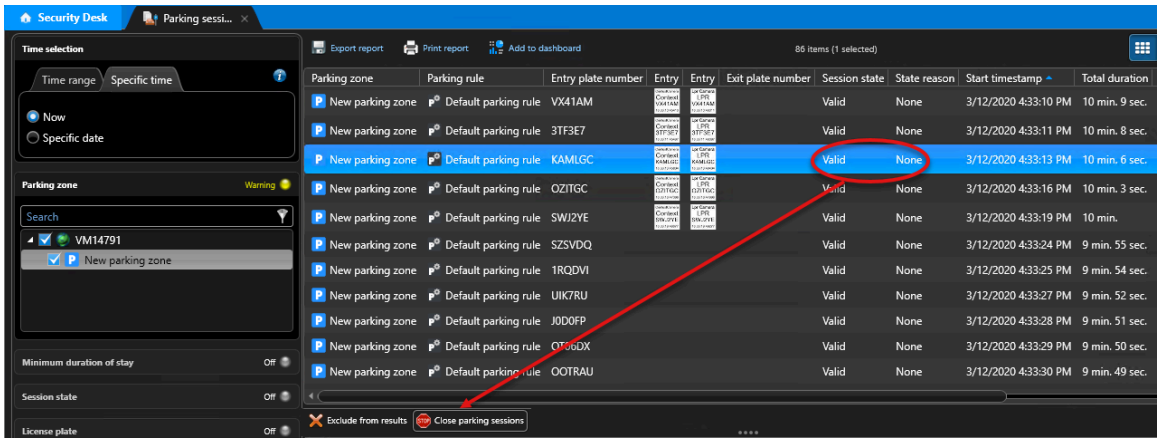
For sites with a long maximum session time value, multiple invalid entries in the parking sessions report, created by false or duplicate reads, can impede parking zone management. You can manually close these entries to remove them from the report.

Before you begin

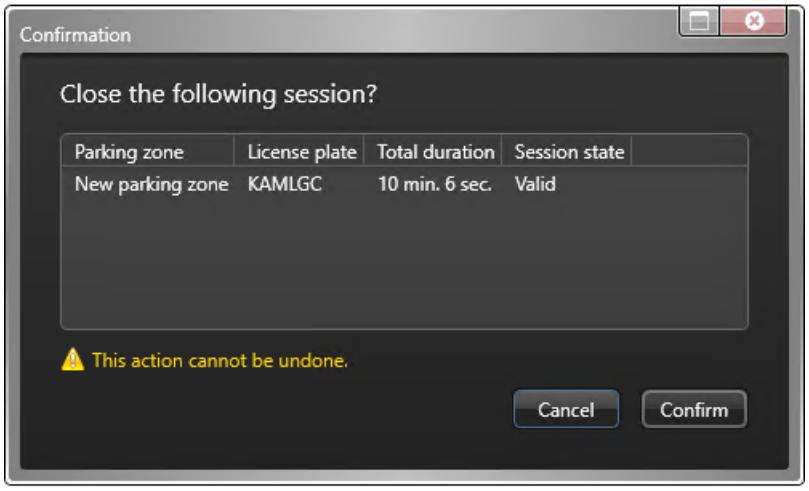
To manually close the parking sessions, you must have the *Close parking sessions* privilege enabled.

To close parking sessions:

1. From the Security Desk home page, open the *Parking sessions* task.
2. Set up the following query filters for your report:
   a) In the *Time selection* area, click **Specific time** and then select **Now**.
   b) Click the **Session state** filter and select **Valid**.
   c) Click the **State reason** filter and select **None**.
3. Click **Generate report**.
   The parking sessions are listed in the report pane.
4. In the parking sessions report results, select every result without *Exit plate number* and click **Close parking sessions**.



5. In the *Confirmation* window, click **Confirm**.



6 In the *Information* dialog box, click **Close**.

7 Click **Generate report** to view updated results.

Sessions terminated by this procedure are labeled **Completed** in the *Session state* column and **None** in the *State reason* column.

Modifying the occupancy of a parking zone

If the occupancy that is reported for a parking zone does not match the number of cars that are physically parked in the parking zone, you can correct the occupancy in the system using a manual action, a hot action, or an event trigger.

What you should know

- A mismatch between the occupancy that is reported for a parking zone and the number of cars that are physically parked in the parking zone can be caused by license plates that are not read correctly at the entrance or exit of the parking zone, which generate misreads or NO PLATE reads, depending on how the system is configured. In such cases, the occupancy increases or decreases accordingly, but parking sessions are not opened or closed.
- When you modify the occupancy of a parking zone, the system does not close any of the active parking sessions. This is because, for example, if a vehicle's plate is not read at the exit of the parking zone and is registered as a NO PLATE read, the system does not know which parking session to close because the NO PLATE read cannot be linked to a parking session. This differs from what happens when you reset the inventory of a parking zone, in which case all parking sessions are automatically closed and the remaining vehicles must be issued tickets or must be towed.

The following example uses a manual action to modify the occupancy. You can also configure a hot action or an event trigger.

To modify the occupancy of a parking zone using a manual action:

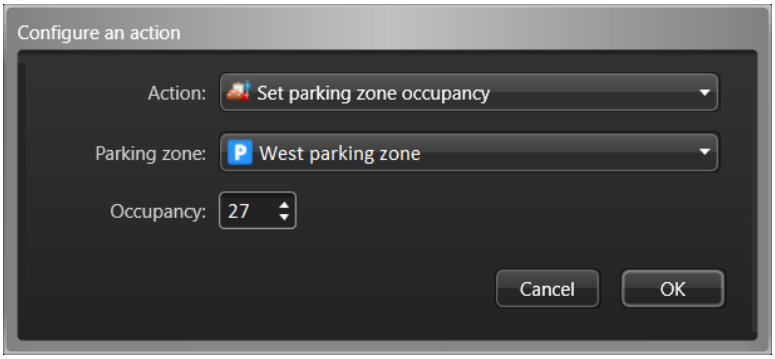
1 In the Security Desk notification tray, click **Hot actions** ( ).

2 In the *Hot actions* dialog box, click **Manual action**.

3 In the *Configure an action* dialog box, select **Set parking zone occupancy** from the list of actions.

4 From the **Parking zone** drop-down list, select the parking zone you want to modify.

5 Enter the **Occupancy** for the parking zone, indicating the current number of vehicles in the parking zone.



6 Click **OK**.

The manual action is triggered and the occupancy of the parking zone is set.

Related Topics

Triggering one-time actions on page 93
Triggering hot actions on page 92

25

Genetec Patroller™

This section includes the following topics:

About Genetec 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 *Genetec Patroller™* interface alerts users of license plates matching the above rules so that immediate action can be taken.

Depending on your AutoVu™ solution, Genetec 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.

Replaying patrol vehicle routes

You can replay the route taken by a vehicle running Genetec Patroller™ on a given date on a map, using the *Patroller tracking* report.

Before you begin

To view your query results in the canvas, you must know how to monitor ALPR events in Security Desk in map mode.

What you should know

The Patroller tracking report gives you a more visual representation than the *Hits* or *Reads* reports. For example, if you want to see the exact route a patrol vehicle operator took during their shift, select that patrol vehicle, and the date of their shift.

An animated playback of the patrol vehicle route is displayed in map mode, and a graphical representation of the patrol vehicle route is displayed in the timeline chronologically. In the map, the 15 ALPR events that occurred before and after the current patrol vehicle location are displayed. You can navigate through the route from the timeline, and review the hits and reads captured by Genetec Patroller™.

To replay a patrol vehicle route:

1. From the home page, open the Patroller tracking task.
2. From the **Patroller** drop-down list, select a Genetec Patroller™ unit.
3. Click **Date**, and select the day you want to view.
4. Click **Refresh**.

   Security Center receives the Genetec Patroller™ data from the *database*. The route is plotted on the map, and on the timeline.
5. To navigate through the patrol vehicle route and locate ALPR events, use the timeline controls.
6. To view the properties of an ALPR event, double-click an item on the map.

After you finish

Print a hit for proof of violation if required.

Related Topics

Overview of the Patroller tracking task on page 596
Genetec Patroller™ tracking timeline controls on page 597

Tracking the current location of a patrol vehicle

You can view the current location of patrol vehicles running Genetec Patroller™ on a map using the Patroller tracking report.

What you should know

Genetec Patroller™ requires a live connection to Security Center for this feature to work.

To view the current location of a patrol vehicle:

1 From the home page, open the *Patroller tracking* task.

2 Click **Go live**.

All active patrol vehicles are plotted on the map, and you can see their current position.

Investigating how Genetec Patroller™ applications are used daily

You can view the *total* daily time (in minutes) and the *percentage* of daily time a Genetec Patroller™ application is opened, stopped, or shut down, using the *Daily usage per patroller entity* report. You can also view the average amount of time the Genetec Patroller™ was opened, stopped, shut down, and so on, for the selected time range.

What you should know

This report is used in mobile Genetec Patroller™ installations only. You can use these statistics to calculate the efficiency of your Patrollers. For example, to view the statistics of a specific Genetec Patroller™ during their last shift, you can search for that Genetec Patroller™, and set the time range.

To investigate how a Genetec Patroller™ application is used on a particular day:

1 From the home page, open the **Daily usage per patroller entity** task.

2 Set up the query filter for your report. Choose one or more of the following filters:

- **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.
- **Patrollers:** Restrict the search to Genetec Patroller™ units (including all their fitted ALPR units).
- **Time range:** The time range for the report.

3 Click **Generate report**.

The results are listed in the report pane.

4 In the **Statistics** section, review the following usage statistics of the selected Genetec Patroller™:

- **Operating time (Average):** Average operating time over the selected time range.
- **Longest stop (min.) (Average):** Average longest stop time in minutes over the selected time range.
- **Longest stop % (Average):** Average longest stop time percentage during the selected time range.
- **Total Stop (min.)(Average):** Average total stop time in minutes during the selected time range.
- **Total stop % (Average):** Average total stop time in percentage during the selected time range.
- **Instances (Average):** Average number of times that Genetec Patroller™ was opened during the selected time range.
- **Longest shutdown (min.) (Average):** Average longest shutdown time in minutes during the selected time range.
- **Longest shutdown % (Average):** Average longest shutdown time in percentage during the selected time range.
- **Total Shutdown (Average):** Average total shutdown time in minutes during the selected time range.
- **Total shutdown % (Average):** Average total shutdown time in percentage during the selected time range.

Report pane columns for the Daily usage per patroller entity task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Daily usage per patroller entity 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.
- **Date:** Day of the patrol vehicle shift.
- **Instances:** Total number of times the Genetec Patroller™ application is opened during the day.
- **Longest shutdown (%):** Percentage of Longest shutdown over the total number of minutes in a day.

- **Longest shutdown (min.):** Single longest number of minutes in a day that the Genetec Patroller™ application is closed.
- **Longest stop (%):** Percentage of longest stop time over operating time.
- **Longest shutdown (min.):** Single longest number of minutes in a day that the Genetec Patroller™ application is closed.
- **Operating time:** Total number of minutes in a day that the Genetec Patroller™ application is open.
- **Total shutdown (%):** Percentage of Total shutdown over the number of minutes in a day.
- **Total shutdown (min.):** Total number of minutes in a day that the Genetec Patroller™ application is closed. The total shutdown value plus the operating time value equals 1440 minutes.
- **Total stop (%):** Percentage of total stop time over operating time.
- **Total stop (min.):** Total number of minutes in operating time when the vehicle is stationary.

Investigating logon/logoff records of Patrollers

You can view the logon and logoff records for Patrollers during a specific time range, using the *Logons per Genetec Patroller™* report.

What you should know

Using this report, you can keep track of which patrol vehicles are out in the field. This report is used in mobile Genetec Patroller™ installations only.

NOTE: When using this report at a Security Center Federation™ host, the User column will remain empty for federated Genetec Patroller™ entities because the user entities are not federated.

To investigate the logon/logoff records of a Genetec Patroller™:

1 From the home page, open the **Logons per Genetec Patroller™** task.

2 Set up the query filter for your report. Choose one or more of the following filters:

- **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.
- **Patrollers:** Restrict the search to Genetec Patroller™ units (including all their fitted ALPR units).
- **Time range:** The time range for the report.
- **Users:** Select the Patroller user name, or the Patrollers' parent user groups.

3 Click **Generate report**.

The results for the selected Genetec Patroller™ are listed in the report pane.

Report pane columns for the Logons per Patroller task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Logons per Patroller 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.
- **Date:** Day of the patrol vehicle shift.
- **Log on/Log off:** Log on and log off timestamp.
- **User:** The Genetec Patroller™ user name. Not available at a Security Center Federation™ host for federated Genetec Patroller™ entities.

Investigating the number of vehicles in parking zones

You can view the number of vehicles parked in a *parking zone*, and the percentage of occupancy, using the *Zone occupancy* task.

What you should know

You can also use the *Zone occupancy* report to search for *overtime rules* and *permit restrictions* that occurred in a zone. For example, on a university campus or in an airport, you can find out the occupancy of a parking lot at certain times of the day. If the occupancy is always at full capacity during that time, the report can help you determine that you need more spots in your parking lot.

The percentage of occupancy of a parking zone is calculated differently whether the Genetec Patroller™ was used for *University Parking Enforcement* or for *City Parking Enforcement*.

Genetec Patroller™ configuration	Percentage of occupancy
University Parking Enforcement	Calculated using the specific zone selected in Genetec Patroller™, which corresponds to a single parking lot defined in an overtime rule or in a permit restriction.
City Parking Enforcement	• If an overtime rule is selected: calculated using all parking lots defined within the rule. • If no overtime rule is selected: occupancy cannot be calculated because no parking lot is associated to a permit. In this case the *Spaces* and *Percentage of occupancy* columns will show 0.

To investigate the reads/hits reported in a parking zone:

1 From the home page, open the **Zone occupancy** task.

2 Set up the query filter for your report. Choose one or more of the following filters:

- **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.
- **Hit rules:** Select the hit rules to include in the report.
- **Overtime and permit restriction:** Both rules have parking lots configured and each parking lot can be defined in terms of a number of parking spaces. This allows the occupancy to be estimated when selecting these rules in Genetec Patroller™.
- **Patrollers:** Restrict the search to Genetec Patroller™ units (including all their fitted ALPR units).
- **Time range:** The time range for the report.

3 Click **Generate report**.

The results are listed in the report pane.

4 View the statistics on the total number of vehicles in all the selected parking zones in the *Statistics* section.

Report pane columns for the Zone occupancy task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Zone occupancy 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.
- **From/To:** Date and timestamp of read vehicles within the zone.

- **Lot:** Parking zone where a given parking regulation is in force.
- **Percentage occupancy:** Percentage of occupied places within the parking zone.
- **Spaces:** Number of spaces in the parking lot.
- **To/from:** Date and timestamp of read vehicles within the zone.
- **Vehicles:** Number of vehicles that were read within the zone.
- **Zone:** The name of the Overtime rule or Permit restriction.

26

Mobile License Plate Inventory

This section includes the following topics:

How AutoVu™ MLPI works

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 AutoVu™ MLPI process works as follows:

- A *parking facility* is created in Config Tool. The parking facility describes the layout of the parking area in sectors and rows. For information about configuring a parking facility, see the *Security Center Administrator Guide*.
- Genetec Patroller™ routes are associated to sectors and rows configured in the parking facility. The sector and row of a *license plate read* represents the location of the vehicle in the parking facility.
- *AutoVu MLPI* Genetec Patroller™ (or handheld device approved by Genetec Inc.) collects license plate reads in the parking facility, and then offloads the data to Security Center.

  NOTE: Handheld device reads are imported to the ALPR Manager database using the XML import module. A single *ghost patroller*, called XML import, appears in the list to identify this. No matter how many handheld devices exist, all their reads are imported to the same ghost patroller.
- Security Center polls the *Offload* folder for new MLPI data.
- The Inventory icon ( ) in Security Desk indicates when there is new data that can be added to an inventory.

For more information about reconciling reads or about the MLPI solution, see the *AutoVu™ Genetec Patroller™ Mobile License Plate Inventory User Guide*.

Removing license plate reads from offload files

Before adding the data from an offload file to an inventory using the *Inventory management* task, you can remove license plate reads from the offload.

What you should know

You can only remove *unreconciled reads* from an offload file. You cannot compare inventories, since unreconciled reads have not been added to an inventory.

To remove a license plate read from an offload file:

1. From the home page, open the *Inventory report* task.
2. In the *Inventory* section in the **Filters** tab, click **Unreconciled reads**.
3. Set up other query filters to refine your search.

   Example: In the **License plate** section, enter the plate numbers of the vehicles that were towed away since the plate reads were taken by Genetec Patroller™.
4. To only display unreconciled reads that were manually removed, select the **Only show manually removed reads** option from the **Advanced search** section.
5. Click **Generate report**.
6. In the report pane, select the vehicle you want to remove.
7. At the bottom of the report pane, click **Remove** ( ).

   The plate read is displayed as *Vehicle manually removed* in the *Statistics* section.

After you finish

After you have removed the unreconciled reads from the offload file, you can create the inventory for the offload. For more information about creating parking facilities, see the *Security Center Administrator Guide*.

Related Topics

Investigating reported license plate reads on page 405

Removing data from offload files

You can remove the data in an offload file from the ALPR Manager database.

What you should know

Patrollers and handheld devices offload to an *ALPR Manager*. The offloads are duplicated and stored in the ALPR Manager *database*. In the *Inventory management* task, the reads are associated with a parking facility, and they are marked as not yet part of an inventory.

If you delete an offload from the *Offloads* list, the reads are no longer linked to a parking facility. However, the data remains in the Security Center database as regular plate reads, and they can still be queried using the *Reads* task.

To remove data from an offload file:

1. From the home page, open the *Inventory management* task.
2. In the *Offloads* section, select a Genetec Patroller™ from the list.
   If a handheld device is used, use the Genetec Patroller™ named **XML Import**.
3. Under the *Offloads* section, click .

Creating parking facility inventories

You can add and reconcile MLPI license plate reads from an offload file to a parking facility inventory, using the *Inventory management* task.

Before you begin

Before adding the data from an offload files to an inventory, you can remove unreconciled plate reads from the offload, using the *Inventory Report* task.

What you should know

You must know the following about creating inventories:

- When new MLPI plate reads are available in the database, a notification appears on the Inventory icon ( ) in the notification tray. The inventory alert is updated every 10 minutes. You can also update the alert by right-clicking the Inventory icon, and clicking **Refresh**.
- You can only create one parking facility inventory at a time.
- If a Genetec Patroller™ offloads multiple times before an inventory is created, they are all grouped in a single entry.
- You cannot set the start time of an inventory. The first time you create an inventory, the start time is undefined. The next time you create an inventory, the start time is the end time of the previous inventory.
- Reconciling is when a read is confirmed and added to an inventory. If there is a conflict while reconciling a read to an inventory (for example, two vehicles with the same plate numbers, but from different states), you might have to manually confirm the read.
- A partial inventory is when you perform a spot check on an inventory at a specific time, and the reads are not reconciled with the previous inventory. This is useful if Genetec Patroller™ is unable to perform a complete sweep of a parking facility. For example, if there is a heavy snowfall and Genetec Patroller™ can only sweep half of the parking lot because the other half has not been plowed, a partial inventory can be created so the reads are still recorded.

To create a parking facility inventory:

1 From the home page, open the *Inventory management* task.

NOTE: The *Offloads* panel only contains information if an offload file has been duplicated and stored in the ALPR Manager database.

The *Offloads* panel includes the following information:

- **Genetec Patroller™:** Name of the Genetec Patroller™ unit that performed the offload.

  NOTE: A single *ghost patroller*, called XML import, is displayed for reads that were taken by a handheld device, because they were imported to the ALPR Manager database using the XML import module.
- **First seen:** Timestamp of the first read in the offload.
- **Last seen:** Timestamp of last read in the offload.
- **Read count:** Number of reads in the offload.

2 From the **Parking facility** drop-down list, select the parking facility you want to add the inventory to.

3 Click **Create inventory**.

4 In the *Create inventory* dialog box, type the name of inventory, and the end time.

5 If you want to create a partial inventory, select **Partial**.

6 Click **Create**.

The plate reads are reconciled and the plate read data is added to the parking facility inventory.

7 If there is a conflict while the reads are being reconciled (for example, a license plate appears in two locations), then the *Plate confirmation* dialog box opens, and you must verify that the license plate in the context image is the same as the plate image and *OCR* read as follows:

TIP: You should only compare the ALPR image and the OCR read, because the plate in the context image might be difficult to see.

a) If the OCR reading is incorrect, type the correct license plate number in the **OCR reading** box.

NOTE: This plate read is tagged as *Edited* in the *Inventory report* task.

b) If the OCR reading is correct, but the plate state is different, enter the state name in the **State** box.

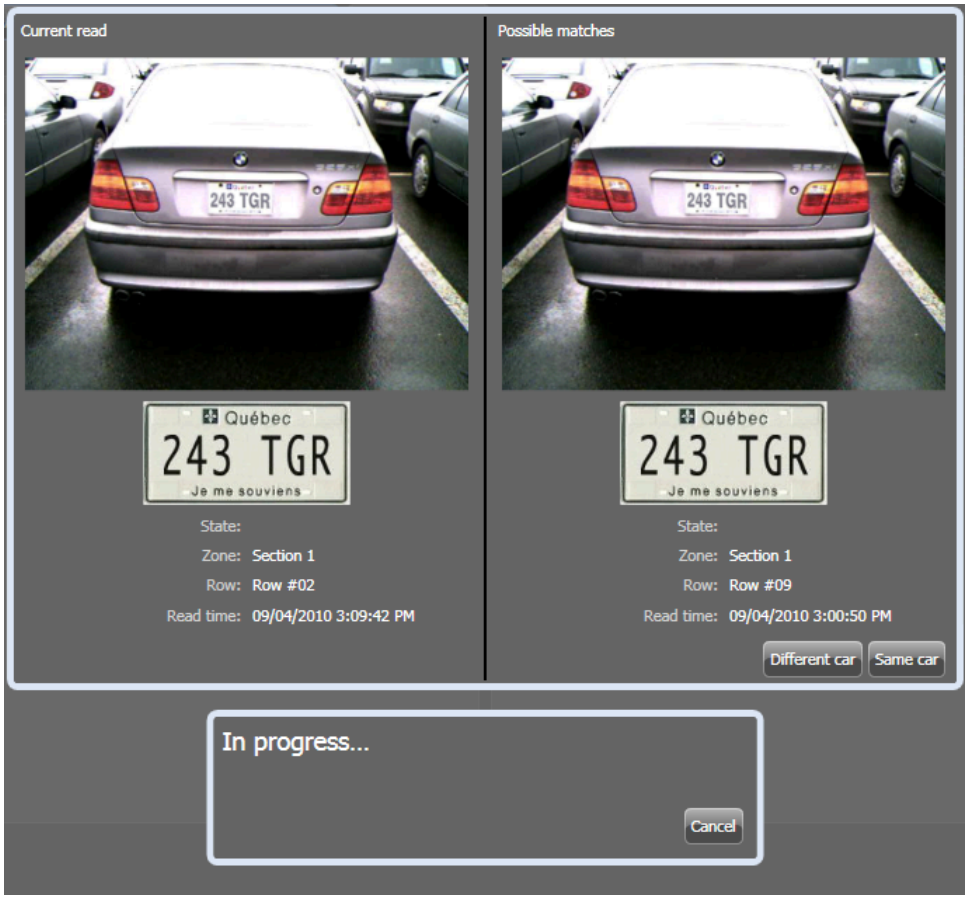
You can enter the state abbreviation or full name.

c) Click **Confirm**.

The data from the offload is added to the parking facility inventory.

8 If a conflict is detected during the inventory process (for example, a license plate appears in two locations), then a dialog box opens that displays the plate read in the current parking facility inventory

(**Current read**), and the possible plate match (**Possible matches**) in the data it is trying to reconcile to that inventory.



Select one of the following:

- **Different car:** Select if the plate numbers are the same, but the plate state and the vehicle are different from the vehicle in the current inventory. The vehicle displayed under **Possible matches** is added as a new vehicle in parking facility inventory.
- **Same car:** Select if the plate numbers, state, vehicle are the same, but the vehicle has moved locations since the last inventory was taken.
- **Cancel:** Cancel the reconciliation. If the conflicts are not reconciled, a new plate read is created which says that a new vehicle arrived (as opposed to marking the same vehicle down for an additional day), and it is considered a **Different car**.

A message appears warning you that the operation was canceled. Click **OK**.

The inventory you canceled appears in red under *Existing inventories*, but the offload data remains in the Offload folder until it is added or removed from the parking facility.

9 If there are any canceled inventories, you must delete them before you can create another inventory as follows:

a) In the *Existing inventories* panel, select the canceled inventory (in red).
b) Under the *Existing inventories* panel, click **Delete** ().

Related Topics

How AutoVu™ MLPI works on page 452
Removing license plate reads from offload files on page 453
Overview of the Inventory management task on page 595

Viewing and comparing parking facility inventories

You can view an inventory or compare two inventories from a specific *parking facility*, using the *Inventory report* task.

What you should know

In the *Inventory report*, you can view and compare vehicle inventories from different time periods to determine the following:

- Current and previous inventories of parked cars
- Vehicles that have been added (entered) or removed (exited)
- Vehicle location (sector and row)
- Vehicles that have been manually removed (towed)
- Vehicle stay duration
- Vehicles whose data was edited and manually reconciled into the inventory.

To prevent performance issues, plate images are not displayed for reports that include more than a thousand rows.

BEST PRACTICE: For best results, compare the more recent inventory with the previous inventory. For example, if the parking facility is swept on a daily basis, you should compare the inventory from today and yesterday.

To view or compare parking facility inventories:

1. From the home page, open the Inventory report task.
2. From the **Parking facility** drop-down list in the *Source* section, select the name of the parking facility.
3. In the *Inventory* section, select the inventory you want to view or compare.
   - **Latest non-partial:** The latest inventory.
   - **Specific:** A specific inventory.
4. To compare the inventory with another inventory in the parking facility, select a second inventory from **Other inventory** drop-down list.
5. From the Added drop-down list, select the vehicle state you want to compare.

   You can query vehicles that were *Unchanged*, *Added*, *Removed*, or *Moved*. You can select multiple actions at the same time.
6. Set up other query filters to refine your search. Choose from one or more of the following filters:
   - **Advanced search:** By default, ALPR images are not displayed in the Inventory report. To view images, click **Get images**. To prevent performance issues, plate images are not displayed if a report includes more than a thousand rows.
   - **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.
   - **License plate:** Enter a full or partial license plate number. To enter multiple license plates, see Filtering a report with multiple license plates on page 417
   - **Location:** Specify the location in the parking facility you want to view. You can select the entire facility, or specify the sectors and rows within the facility.
7. To include ALPR images in the report, select the **Get images** option from the **Advanced search** section.

8 Click **Generate report**.

The results are listed in the report pane.The following statistics of the changes between the two inventories are shown:

- **Vehicles added:** Total number of vehicles added to the parking facility.
- **Vehicles removed:** Total number of vehicles removed from the parking facility.
- **Vehicles moved:** Total number of vehicles that moved in the parking facility.
- **Vehicles manually removed:** Total number of vehicles manually removed from the parking facility.
- **Number of manual entries:** Total number of unreconciled reads removed from the offload file.

Related Topics

About license plate filters on page 415

Report pane columns for the Inventory report task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Inventory report task.

- **Action:** The change in the vehicle state: *added*, *removed*, *moved*, or *unchanged*.
- **Arrival:** The first time the vehicle was read. This is used to calculate the elapsed time if a vehicle is read a second time, for example the next day.
- **Context image:** Wide angle color image of the vehicle that was captured by the context camera.
- **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.
- **Edited:** Vehicle license plate and state were edited by a user in Security Desk.
- **Elapsed time:** The difference between the Arrival time and the Event timestamp.
- **Event timestamp:** Date and time that the event occurred.
- **Manual capture:** Displays the plate number entered manually by the Genetec Patroller™ user.
- **Manually removed:** Vehicle was removed manually (towed) from the parking facility.
- **Parking:** Parking facility name.
- **Patroller entity:** The patroller entity that read the plate. If a handheld device was used, *XML import* is shown instead.
- **Plate image:** The license plate image captured by the ALPR camera.
- **Plate origin:** State that issued the license plate.
- **Plate read:** The license plate read generated by the Sharp unit.
- **Row:** Row name.
- **Sector:** Sector name.

Part V

Alarms and critical events in Security Desk

This part includes the following chapters:

27

Alarms

This section includes the following topics:

How alarms are displayed in the Security Desk canvas

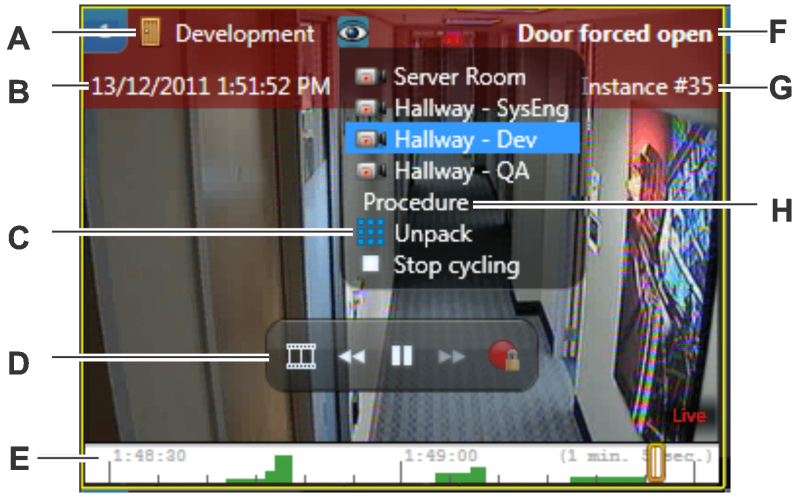
You can view active and past alarms in the canvas in the *Alarm monitoring* task, the *Alarm report* task, and the *Monitoring* task.

In the *Alarm monitoring* task and *Monitoring* task, active alarms are automatically displayed in the canvas so you can review the alarm details and the associated video. In the *Alarm report* task, all videos associated to the alarm are displayed in playback mode. The playback starts at the time the alarm was triggered.

Alarms are often *composite entities* because they are attached to multiple cameras, doors, or areas, and might include still frames. To view all the attached entities at once, you must unpack the tile where the alarm is displayed.

NOTE: If the triggered alarm is attached to an entity (for example a door) that is linked to cameras, then the linked cameras are displayed first in the canvas, before the attached entity itself.

The following figure shows an active alarm in a canvas tile in the Alarm monitoring task.



A	Source of the alarm
B	Alarm timestamp
C	Allows you to view all attached entities at once
D	On-tile video controls
E	Timeline
F	Alarm name
G	Alarm instance number
H	Displays the alarm procedure if it is defined

Related Topics

On-tile video controls on page 189
Unpacking content in tiles on page 28
Enabling alarm monitoring in the Monitoring task on page 463

Enabling alarm monitoring in the Monitoring task

To avoid switching between tasks when an alarm occurs, you can enable alarm monitoring in the *Monitoring* task.

Before you begin

Create your alarms. For more information, see the *Security Center Administrator Guide.*

What you should know

When tiles are armed to monitor alarms in the *Monitoring* task, alarms are no longer displayed as pop-up windows in the notification tray. You can configure alarms as pop-ups.

To enable alarm monitoring in the Monitoring task:

1 Open the *Monitoring* task.

2 At the bottom of the *Monitoring* task, click **Monitoring** ( ).

3 Switch the **Alarm monitoring** option to **ON**.

You can arm or disarm all the tiles from monitoring alarms by clicking ( ). When a tile is armed to monitor alarms, the tile ID background is red.

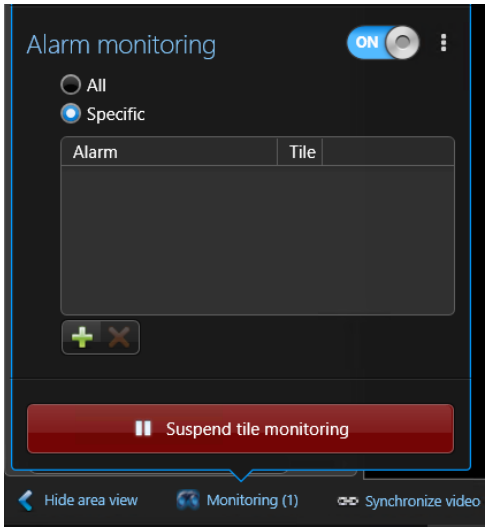
4 Select whether you want to monitor **All** alarms or **Specific** alarms.

5 If you selected **Specific**, do the following:

a) Click and select the alarms you want to monitor.

TIP: To select multiple alarms, hold Ctrl or Shift when selecting the alarms.

b) Click **Add**.



The **Events** and **Alarms** toggle button appears in the top-right corner of the *Monitoring* task so you can easily switch between monitoring events and alarms. If you cannot see the **Events/Alarms** toggle button, drag the top of the canvas down to expose the alarm list that appears at the top of the screen.

You can pause tile monitoring at any time by clicking **Suspend tile monitoring**.

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

Filtering and grouping alarms in Security Center on page 468

Acknowledging alarms

You can view and acknowledge the alarms from the *Alarm monitoring* and the *Monitoring* task.

Before you begin

To view and acknowledge alarms from the *Monitoring* task, you must enable alarm monitoring for that *Monitoring* task.

What you should know

You only receive an alarm in Security Desk if you are a recipient of that alarm. Alarms are displayed in the canvas by order of their priority.

NOTE: You might not have to acknowledge all the alarms that are triggered. Certain alarms are configured to be automatically acknowledged after a set amount of time.

To acknowledge an alarm:

1. In the notification tray, double-click the **Alarms** ( ) icon in the notification tray.

   All new alarms are automatically listed and the associated video is displayed in the *canvas*.

2. To filter the alarm list, click the filter icon ( ) and select one or more of the following filters:
   - **Show all:** Display all alarms (no filter).
   - **Show active:** Show active alarms.
   - **Show under investigation:** Show alarms that are currently under investigation.
   - **Show acknowledgment required:** Show alarms where their acknowledgment conditions are cleared but they must still be acknowledged.
   - **Show acknowledged:** Show acknowledged alarms.
3. Double-click or drag an alarm from the alarm list to view the alarm video in a tile. The video is displayed with a colored overlay that provides the alarm details.
4. In the widget, click one of the following:
   - **Acknowledge (Default) ( ):** Acknowledge the alarm. The alarm is no longer active, and is removed from the canvas and the alarm list.

NOTE: Certain alarms require you to report an incident when you acknowledge them.

- **Acknowledge (Alternate) ( ):** Set the alarm to the *alternate* acknowledged state. The reasons for using this acknowledgment type are defined by your company. For example, if a false alarm is triggered, you can acknowledge the alarm this way. This state can be used as a filter in alarm queries.
- **Investigate ( ):** Investigate the alarm. This action lets other users in the system know that you have seen the alarm without acknowledging it, so the alarm is not removed from the active alarm list.
- **Forcibly acknowledge ( ):** Force the alarm to be acknowledged. This is helpful for clearing alarms that are currently under investigation and their acknowledgment condition is not yet cleared.
- **Forcibly acknowledge all alarms ( ):** Force all the active alarms to be acknowledged. This is helpful for clearing alarms that are currently under investigation and their acknowledgment condition is not yet cleared.
- **Snooze alarm ( ):** Put the alarm to sleep for 30 seconds. When the alarm is snoozing, it is temporarily removed from the canvas. You can change the default snooze time from the *Options* dialog box.
- **Show alarm procedure ( ):** Show the alarm's specific procedure (if one is defined by the administrator). Alarm procedures are simple to create and can take the form of HTML pages or a web application developed by the end user.
- **Forward alarm ( ):** Forward the alarm to another user in the system. Before forwarding the alarm, you must select a user, and you can also type a message.
- **Edit context ( ):** Add or modify the alarm annotation.

NOTE: All actions on the alarms are logged in the activity trail.

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

How alarms are displayed in the Security Desk canvas on page 462
Overview of the Alarm monitoring task on page 606

Alarm information available when monitoring alarms

When an alarm is triggered, you can view the following information in the *Alarm monitoring* and the *Monitoring* task.

- **ID:** Alarm instance number. Uniquely identifies each alarm instance.
- **Alarm:** Alarm entity name.
- **Priority:** Alarm priority. All alarms imported from Omnicast™ have their priority set to 1 by default. You can change their priority at a later time in the Config Tool.
- **Alarm color:** Color of the alarm.
- **Source:** Source 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 event is triggered manually. The source is not shown if you do not have permission to access the source entity.
- **Triggering event:** Event that triggered the alarm (if triggered through an event-to-action). *Manual action* is indicated when the alarm was manually triggered by a user.
- **Trigger time:** Time the alarm was triggered in Security Center.
- **State:**

Current state of the alarm.

- **Active:** Alarm is not yet acknowledged. Selecting an active alarm shows the alarm acknowledge buttons in the report pane.
- **Acknowledged (Default):** Alarm was acknowledged using the default mode.
- **Acknowledged (Alternate):** Alarm was acknowledged using the alternate mode.
- **Acknowledged (Forcibly):** Alarm was forced to be acknowledged by an administrator.
- **Under investigation:** Alarm that is under investigation, meaning that someone has seen it but not necessarily able to take care of it.
- **Acknowledgment required:** Alarm with an acknowledgment condition that was cleared and that is ready to be acknowledged.

- **Context:** Alarm annotation.
- **Acknowledged by:** User who acknowledged the alarm. When the alarm is acknowledge automatically by the system, **Service** is indicated.
- **Acknowledged on:** Time the alarm was acknowledged.
- **Investigated by:** The user who put the alarm into the *under investigation* state.
- **Investigated on:** The timestamp when the alarm was put into the *investigation* state.
- **Occurrence period:** Period when the event occurred.
- **Source entity type:** The source entity type that triggered the alarm, when the alarm is triggered by an event-to-action. It shows **User** when the alarm is triggered manually.
- **Source time:** Time of the alarm-triggering event. The only time *Source time* and *Triggering time* are different is when the event occurred while the access control unit was offline.
- **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.

Filtering and grouping alarms in Security Center

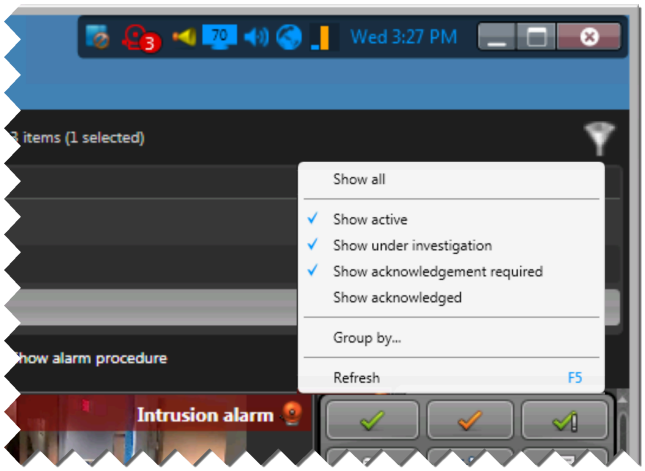
You can filter and group alarms to control how they appear in the *Alarm monitoring* task and the *Monitoring* task.

To filter alarms:

1 In the *Alarm monitoring* task or the *Monitoring* task, click the filter icon ( ).

NOTE: In the *Monitoring* task, you must select **Alarms** from the **Events/Alarms** toggle button. The **Events/Alarms** toggle button only appears when you enable alarm monitoring in the *Monitoring* task.

If you cannot see the **Filter** ( ) or **Events/Alarms** toggle button, drag the top of the canvas down to expose the alarm list that appears at the top of the screen.



2 Select or clear the following filters:

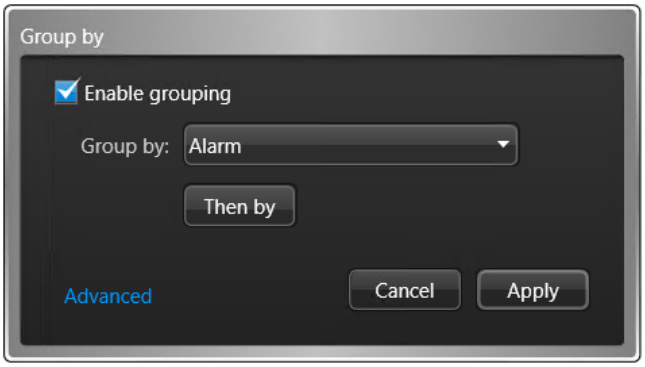
- **Show all:** Display all alarms (no filter).
- **Show active:** Show active alarms.
- **Show under investigation:** Show alarms that are currently under investigation.
- **Show acknowledgment required:** Show alarms where their acknowledgment conditions are cleared but they must still be acknowledged.
- **Show acknowledged:** Show acknowledged alarms.

To group alarms:

1 In the *Alarm monitoring* task or the *Monitoring* task, right-click a column heading and select **Group by**.

NOTE: In the *Monitoring* task, you must select **Alarms** from the **Events/Alarms** toggle button. The **Events/Alarms** toggle button only appears when you enable alarm monitoring in the *Monitoring* task. If you cannot see the **Events/Alarms** button, drag the top of the canvas down to expose the alarm list that appears at the top of the screen.

2 In the *Group by* dialog box, select **Enable grouping**.



3 From the drop-down list, select the highest level of grouping you would like to apply to the alarms.

You can group the alarms by:

- **Alarm:** Alarm entity name.
- **Priority:** Alarm priority. All alarms imported from Omnicast™ have their priority set to 1 by default. You can change their priority at a later time in the Config Tool.
- **Source:** Source 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 event is triggered manually. The source is not shown if you do not have permission to access the source entity.
- **Source entity type:** The source entity type that triggered the alarm, when the alarm is triggered by an event-to-action. It shows **User** when the alarm is triggered manually.
- **State:**

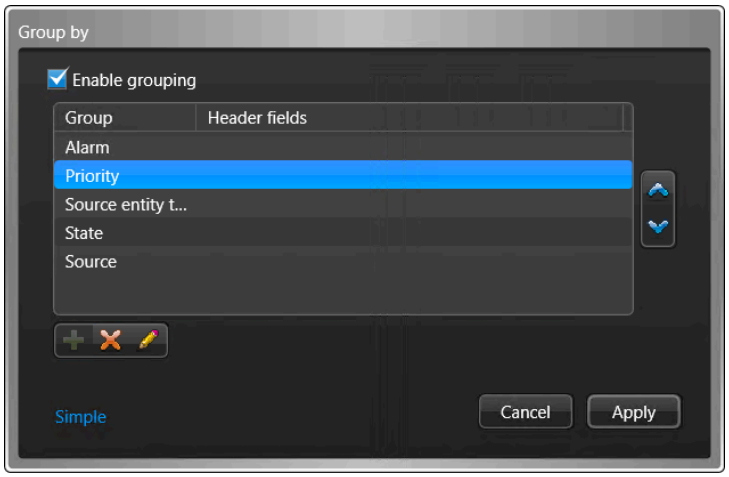
  Current state of the alarm.

  - **Active:** Alarm is not yet acknowledged. Selecting an active alarm shows the alarm acknowledge buttons in the report pane.
  - **Acknowledged (Default):** Alarm was acknowledged using the default mode.
  - **Acknowledged (Alternate):** Alarm was acknowledged using the alternate mode.
  - **Acknowledged (Forcibly):** Alarm was forced to be acknowledged by an administrator.
  - **Under investigation:** Alarm that is under investigation, meaning that someone has seen it but not necessarily able to take care of it.
  - **Acknowledgment required:** Alarm with an acknowledgment condition that was cleared and that is ready to be acknowledged.

4 To apply additional grouping levels, select **Then by**.

5 Click **Advanced**.

6 To change the grouping order, select a group, and then use the and arrows.



7 To show alarm information in the header of the group, do the following:
   a) Select a group, and then click **Edit the item** ( ).
   b) Select the alarm columns you want to show.
   c) To change the column order of appearance, use the and arrows.
   d) Click **OK**.
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

Enabling alarm monitoring in the Monitoring task on page 463
Alarm information available when monitoring alarms on page 466

Muting repeated alarm sounds

If many *active alarms* on your system are causing sound bites to be repeatedly played, you can silence the alarm sounds by muting them from the notification tray.

What you should know

To avoid unintentionally ignoring alarms, you can configure your Security Desk to play a sound bite repeatedly as long as there are active alarms in the system. The sound will stop when all alarms are acknowledged, or when you decide to mute them temporarily.

To mute all sounding alarms:

- In the notification tray, right-click the **Alarms** icon (), and click **Mute all alarms**.

All sounding alarms are muted. The sounding will restart the moment a new alarm is received, and will continue as long as there are active alarms in the system.

Related Topics

Customizing alarm behavior on page 478

Forwarding alarms to other users automatically

If you must leave your desk and you want someone else to receive alarms while you are gone, you can set alarms to *auto-forward*.

Before you begin

Make sure that you have the *Forward alarms* user privilege.

To forward an alarm automatically:

1 Do one of the following:

- In the notification tray, right-click the **Alarms** icon (or), and click **Start alarms auto-forward**.
- In the upper-left corner of the **Alarm monitoring** or **Monitoring** task, click **Start alarms auto-forward** ( ).

2 In the *Select alarm recipients* dialog box, select the destination user or user group.

3 (Optional) Write a message to send with the forwarded alarm.

4 Click **Start alarms auto-forward**.

All alarms sent to you are forwarded to the specified user until you cancel the *auto-forward* option.

5 To cancel *auto-forward*, do one of the following:

- In the notification tray, right-click the **Alarms** icon (or), and click **Stop alarms auto-forward**.
- In the upper-left corner of the **Alarm monitoring** or **Monitoring** task, click **Stop alarms auto-forward** ( ).

Forwarding alarms to other users manually

If you receive an important alarm and you want someone else to see it, you can manually forward the alarm to them from the *Alarm monitoring, Monitoring,* and *Alarm report* tasks.

Before you begin

Make sure that you have the *Forward alarms* user privilege.

What you should know

Forwarding an alarm does not remove it from your workspace. The alarm is forwarded to the user you selected, and one of you must acknowledge the alarm.

To forward an alarm manually:

1. Under the alarm list, or in the alarm widget, click **Forward alarm** ( ).
2. In the *Select alarm recipients* dialog box, select the destination user or user group.
3. (Optional) Write a message to send with the forwarded alarm.
4. Click **Forward alarm**.

Investigating current and past alarms

You can search for and investigate current and past alarms, using the *Alarm report* task.

What you should know

In Security Desk, you can investigate all of the alarms that were triggered during the last week or since your last shift. You can also investigate major events that happened in your system (by only selecting critical alarms), who acknowledged a specific alarm, and why. You can also review the video associated to an alarm, which can then be exported and sent to law enforcement as evidence.

To investigate an alarm:

1 From the home page, open the *Alarm report* task.

2 Set up the query filters for your report. Choose one or more of the following filters:

- **Alarms:** Select the types of alarms you want to investigate. Alarms can be locally defined (), or imported from federated systems ().
- **Acknowledged by:** Users who acknowledged the alarm.
- **Acknowledged on:** Alarm acknowledgment time range.
- **Acknowledgment type:**

  Select one of the following acknowledgment type options:

  - **Alternate:** Alarm was acknowledged by a user using the alternate mode.
  - **Default:** Alarm was acknowledged by a user, or auto-acknowledged by the system.
  - **Forcibly:** An administrator forced the alarm to be acknowledged.
- **Alarm priority:** Alarm priority.

  NOTE: All alarms imported from Omnicast have their priority set to 1 by default. You can change their priority at a later time in the Config Tool.
- **Context:** Restrict the search to alarms with a specific text in the annotation. The search is case insensitive.
- **Investigated by:** Which user put the alarm into the *under investigation* state.
- **Investigated on:** Specify a time range when the alarm was put into the *under investigation* state.
- **Source:** Source entity that triggered the alarm in the case of an event-to-action, or the user who triggered the alarm manually.
- **State:** Current state of the alarm.
  - **Active:** Alarm is not yet acknowledged. Selecting an active alarm shows the alarm acknowledge buttons in the report pane.
  - **Acknowledged:** Alarm was acknowledged by a user, or auto-acknowledged by the system.
  - **Under investigation:** Alarm that is under investigation.
  - **Acknowledgment required:** Alarm with an acknowledgment condition that was cleared is ready to be acknowledged.
- **Triggered on:** Alarm trigger time range.
- **Triggering event:** Events used to trigger the alarm.
- **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 alarms are listed in the report pane.

4 To show the corresponding video of an alarm in a tile, double-click or drag the item from the report pane to the canvas.

5 To control the alarms, use the alarm widget.

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

How alarms are displayed in the Security Desk canvas on page 462
Alarm widget on page 35
Overview of the Alarm report task on page 608

Report pane columns for the Alarm report task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Alarm report task.

NOTE: If you generated the Alarm report using Web Client, not all of the report columns are available.

- **ID:** Alarm instance number. Uniquely identifies each alarm instance.
- **Alarm:** Alarm entity name.
- **Priority:** Alarm priority. All alarms imported from Omnicast™ have their priority set to 1 by default. You can change their priority at a later time in the Config Tool.
- **Alarm color:** Color of the alarm.
- **Source:** Source 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 event is triggered manually. The source is not shown if you do not have permission to access the source entity.
- **Source time:** Time of the alarm-triggering event. The only time *Source time* and *Triggering time* are different is when the event occurred while the access control unit was offline.
- **Triggering event:** Event that triggered the alarm (if triggered through an event-to-action). *Manual action* is indicated when the alarm was manually triggered by a user.
- **State:**

  Current state of the alarm.

  - **Active:** Alarm is not yet acknowledged. Selecting an active alarm shows the alarm acknowledge buttons in the report pane.
  - **Acknowledged (Default):** Alarm was acknowledged using the default mode.
  - **Acknowledged (Alternate):** Alarm was acknowledged using the alternate mode.
  - **Acknowledged (Forcibly):** Alarm was forced to be acknowledged by an administrator.
  - **Under investigation:** Alarm that is under investigation, meaning that someone has seen it but not necessarily able to take care of it.
  - **Acknowledgment required:** Alarm with an acknowledgment condition that was cleared and that is ready to be acknowledged.
- **Acknowledged by:** User who acknowledged the alarm. When the alarm is acknowledge automatically by the system, **Service** is indicated.
- **Acknowledged on:** Time the alarm was acknowledged.
- **Context:** Alarm annotation.
- **External instance ID:** Only for federated alarms. The original alarm instance ID on the federated system.
- **Investigated by:** The user who put the alarm into the *under investigation* state.
- **Investigated on:** The timestamp when the alarm was put into the *investigation* state.
- **Occurrence period:** Period when the event occurred.
- **Trigger time:** Time the alarm was triggered in Security Center.

- **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.

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:

1 From the home page, open the *Alarm monitoring* task or the *Monitoring* task.

2 Click **Trigger alarm** ( ).

3 From the list, select an alarm, and then 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 515

Customizing alarm behavior

When you are familiar with how alarms work, you can customize how the system handles alarms from the *Options* dialog box.

What you should know

The **Display entity names with their full path** option is saved as part of your user profile. The other alarm settings are saved locally for your Windows user profile.

To customize the alarm behavior:

1 From the home page, click **Options** > **Alarms**.

2 Set the following alarm options:

- **Bring Security Desk in front of other windows:** Brings the Security Desk window to the foreground when a new alarm occurs.
- **Play a sound:** Sets the sound bite to play when a new alarm occurs and how often to play it: *Once* (default), *Every n seconds*, or *Continuously*. Click **Test** to hear the selected sound bite.
- **Display in:**
  - **Pop-up:** Displays alarms in a pop-up window in the notification tray of the *Monitoring* task.
    NOTE: Pop-up alarms are only used when there are no armed tiles in the *Monitoring* task.
  - **Alarm monitoring task (and bring to front):** Automatically switches to the *Alarm monitoring* task when a new alarm occurs. If *Alarm monitoring* is not in the active task list, it is added.
  - **Map (and bring to front):** Automatically switches to display alarms in the *Maps* task. If the *Maps* task is not in the active task list, it is added.
- **Order alarm monitoring tiles by latest:** When enabled (default), displays alarms in armed tiles from newest to oldest. When disabled, displays alarms in armed tiles from oldest to newest.

  NOTE: Alarms with higher priority always have precedence.
- **Revert to original task after alarm is handled:** After you acknowledge the alarm, automatically returns to the task you were working on before the alarm occurred.
- **Center map on received alarm:** When set to display alarms in the *Maps* task, automatically centers the map view on the linked object and zooms in.
- **Automatically display alarm in unpacked mode:** When the alarm is triggered, displays all the attached entities of the alarm in separate tiles instead of cycling through them.
- **Snooze time:** Sets the duration of the snooze when an alarm is put to sleep with the command.

3 Click the **Visual** tab.

4 To show the full path of the entity that triggered the alarm in the **Source** column in the Monitoring task and Alarm monitoring task, select the **Display entity names with their full path** option.

An entity's path is the hierarchy of *areas* above that entity in the area view. When the path is too long, an "*" is displayed instead.

Example: "Montreal office/Main entrance", or "*/*/Back entrance".

NOTE: This option also applies to other entities. When this option is selected, the full path of other entities is shown in tile toolbars.

5 Click **Save**.

Related Topics

Acknowledging alarms on page 465
Muting repeated alarm sounds on page 471

Overview of the Alarm monitoring task on page 606
How alarms are displayed in the Security Desk canvas on page 462
Inverting the alarm display priority in Security Desk on page 481
Muting repeated alarm sounds on page 471

Customizing picture-in-picture windows for alarms

In Security Desk, you can customize the size and position of the inset window for an alarm that is configured for picture-and-picture display. You can also switch the content displayed in the inset window.

Before you begin

Configure picture-in-picture as the video display option for your alarm. For more information, see the *Security Center Administrator Guide.*

To customize the inset window of a picture-in-picture alarm:

1 Open the *Monitoring* or *Alarm monitoring* task.

2 Select a tile that is displaying an alarm configured for picture-in-picture display.

3 You can do the following:

- Click within the inset window to switch the displayed video type with the video type displayed in the full tile. For example, if you configure your alarm to display live and playback video, and live video is displayed in the inset window, clicking within the inset window switches the content to playback video.
- Click and drag the inset window to move it to a new location.
- Click and drag the box handles around the inset window to resize it.

Your changes are applied immediately.

Inverting the alarm display priority in Security Desk

To ensure that an alarm you are monitoring remains on the canvas when new alarms are triggered, you can configure Security Desk to display older alarm tiles before newer alarm tiles.

What you should know

Security Desk follows two rules to display alarms in *armed tiles*:

1. Highest priority alarm first: This rule takes precedence and cannot be changed.
2. Newest alarm first (default): This rule can be changed to *Oldest alarm first*.

Alarms are always displayed in descending priority. If all armed tiles are occupied when an alarm is triggered, the lowest priority alarm is not displayed. Active alarms without a tile are listed in the report pane, and are displayed on the canvas when space becomes available.

Alarms with the same priority are displayed according to the *Newest alarm first* or *Oldest alarm first* rules:

- **Newest alarm first (default):** Active alarms with equal priority are displayed on the canvas from newest to oldest. If all armed tiles are occupied when an alarm is triggered, the oldest alarm is removed from the canvas.
- **Oldest alarm first:** Active alarms with equal priority are displayed on the canvas from oldest to newest. If all armed tiles are occupied when an alarm is triggered, that alarm is not displayed on the canvas until space becomes available.

To change the display rule to *Oldest alarm first*:

1 From the Security Desk home page, click **Options** > **Alarms**.
2 Under *When a new alarm occurs*, clear **Order alarm monitoring tiles by latest**.
3 Click **Save**.

Related Topics

Customizing alarm behavior on page 478

28

Incidents and threat levels

This section includes the following topics:

Reporting incidents

When you see a situation that must be remembered, you can report it as an *incident*. Events and entities (cameras, doors, and so on) can be attached to an incident report as supporting information.

What you should know

When you report an incident about an event or an alarm, the event is attached to the reported incident, along with the entities referenced by that event or alarm. You might also be required to report an incident when you acknowledge an alarm, if the alarm is configured that way in Config Tool.

Incident reports can be searched for at a later time from the *Incidents* task.

To report an incident:

1 Do one of the following:

- To report an incident that is not related to an entity, click the home tab, and then click **Tools** > **Report an incident** > .
- To report an incident about an event or alarm, right-click an item in the event list or report pane, and then click **Report an incident**.
- To report an incident about the entity in the selected tile, right-click inside the tile, and then click **Report an incident**.

2 In the *Report an incident* dialog box, type a **Title** for the incident.

3 From the **Category** drop-down list, do one of the following:

- Select a category for the incident.
- If no categories exist, then click **Manage categories** > **Add an item** (), type a name for the category, and then click **Add** > **Save**.

4 In the *Description* section, describe the incident.

The description you add is searchable in the *Incidents* task.

5 In the *References* section, click to add other entities as supporting information.

All the entities related to what you were viewing in the tile are added by default. If you are viewing an alarm, both the alarm and the alarm source (the entity that triggered the alarm) are added by default.

6 To add a video sequence to the incident, click **More**, and do the following:

a) In the *Video sequences* section, click **Add an item** ().

b) Select a camera and a time range, and click **Add**.

c) To protect the video sequence, select the **Protect video from deletion** option.

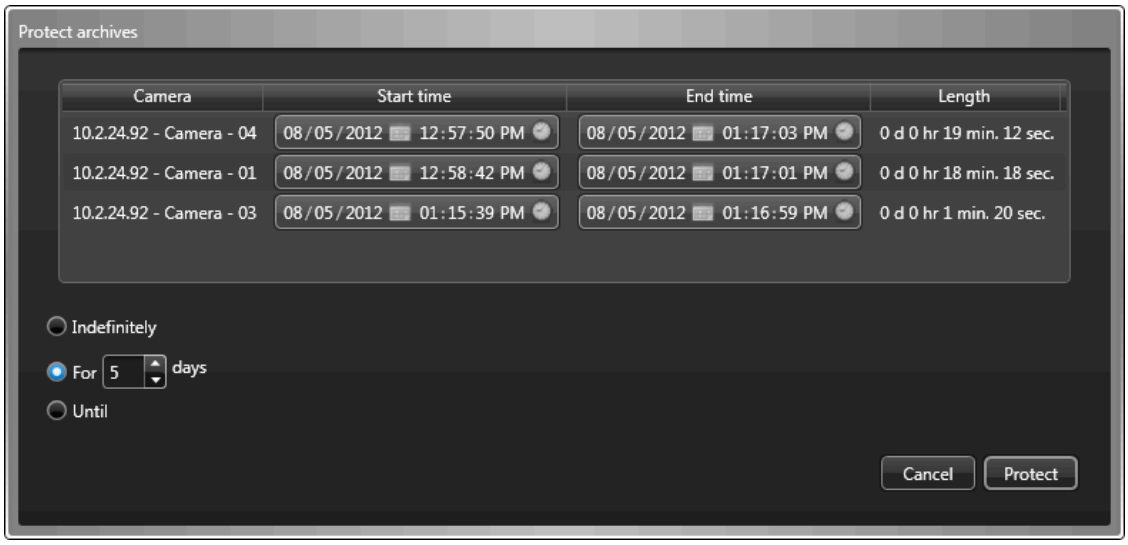
7 Create the incident report one of the following ways:

- Click **Create**.
- To create the incident report and notify other users on the system, click **Create and email**, select the users, and click **Create and email**.

  The user must have a valid email address and the server must be configured to send emails.

If you chose to protect the video sequences that you added to the incident, then the *Protect archives* dialog box opens.

8 In the *Protect archives* dialog box, set the **Start time** and the **End time** for the video that you want to protect.



9 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 information about archive storage, see the *Security Center Administrator Guide*.
- **For x days:** The video file is protected for the selected number of days.
- **Until:** The video file is protected until the selected date.

10 Click **Protect**.

If you cancel the protection settings in the *Protect archives* dialog box, the incident report is still created.

The incident report is saved in the database for reporting purposes. If you selected a user, the report is sent to them.

Related Topics

Tile menu commands on page 25
Reviewing and modifying reported incidents on page 488
Protecting video files from deletion on page 272

Creating incident packages

You can add live and playback video to a tile, and then saving the information as an incident package. This is helpful when you want to report a situation and build a case.

What you should know

When incident recording is turned on, the live or playback video related to any entity that is placed in the tile (cameras, areas, doors, cardholders, and so on) is recorded. Entity cycling inside the tile is supported. Cameras that are placed in the tile start recording if they are not already recording.

You can export the related video sequences as a single G64x file. The G64x file can be played back in Security Desk, or in the Genetec™ Video Player.

You can create multiple incident packages simultaneously.

To create an incident package:

1 To make sure that the tile contents are not overwritten when new events are received in Security Desk, turn off monitoring for that tile as follows:
   a) In the *Monitoring* task, select the tile in the canvas.
   b) In the tile widget, click **Monitoring** ( ).
   c) Click **Monitor alarms** and **Monitor events** to make sure you turn off all monitoring for the tile.

      TIP: When monitoring is turned off for a tile, the tile ID background turns black.

2 Right-click inside the tile that is displaying the camera where the incident is happening, and then click **Start incident recording** ( ).

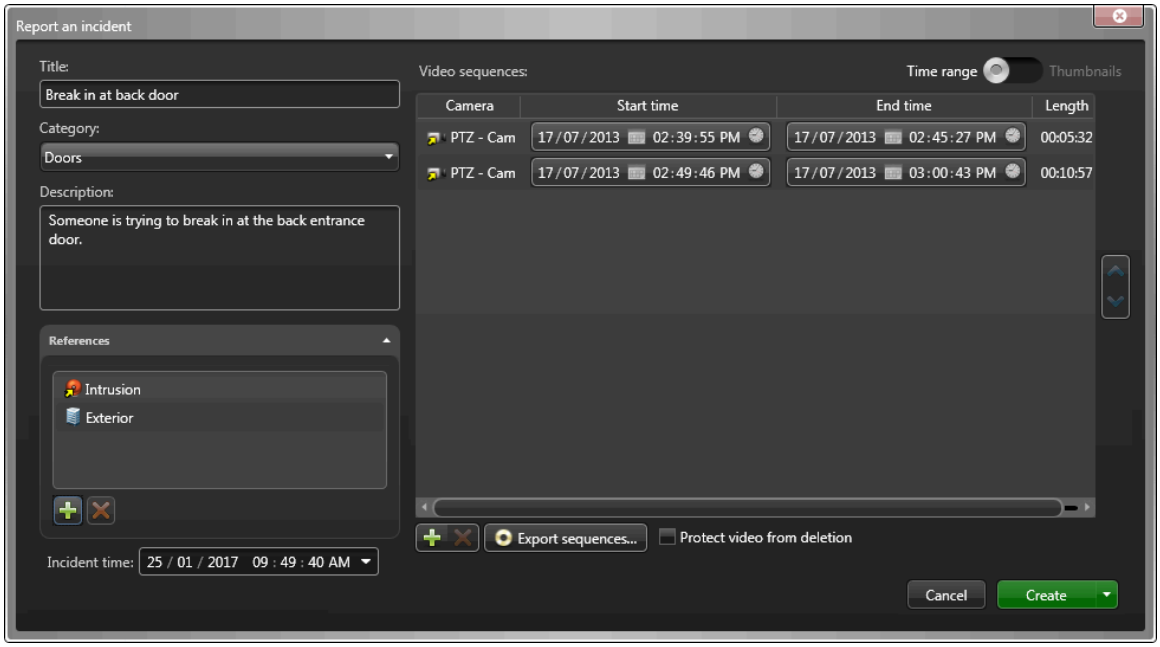
   The tile is outlined in red.

3 To build your case, add other cameras, or entities that have attached cameras, to the tile.

   The sequence is created in the order that you add a new cameras and entities, and can be adjusted afterwards.

4 Right-click inside the tile, and click **Stop incident recording** ( ).

5 In the *Report an incident* dialog box, type a **Title** for the incident.



6 From the **Category** drop-down list, do one of the following:

- Select a category for the incident.
- If no categories exist, then click **Manage categories** > **Add an item** (), type a name for the category, and then click **Add** > **Save**.

7 In the *Description* section, describe the incident.

The description you add is searchable in the *Incidents* task.

8 In the *References* section, click to add other entities as supporting information.

All the entities related to what you were viewing in the tile are added by default. If you are viewing an alarm, both the alarm and the alarm source (the entity that triggered the alarm) are added by default.

9 In the *Video sequences* section, you can do the following:

- For each camera, edit the time range of the video sequence you want to include in the incident report.

  For example, one of the cameras might only have two minutes of video that relates to the incident.
- To add another camera to the package, click **Add an item** (), select a camera and the time range, and click **Add**.

  Adding additional cameras is helpful if you forgot to place one of the cameras in the tile while it was recording the incident.
- To protect the video sequence, select the **Protect video from deletion** option.

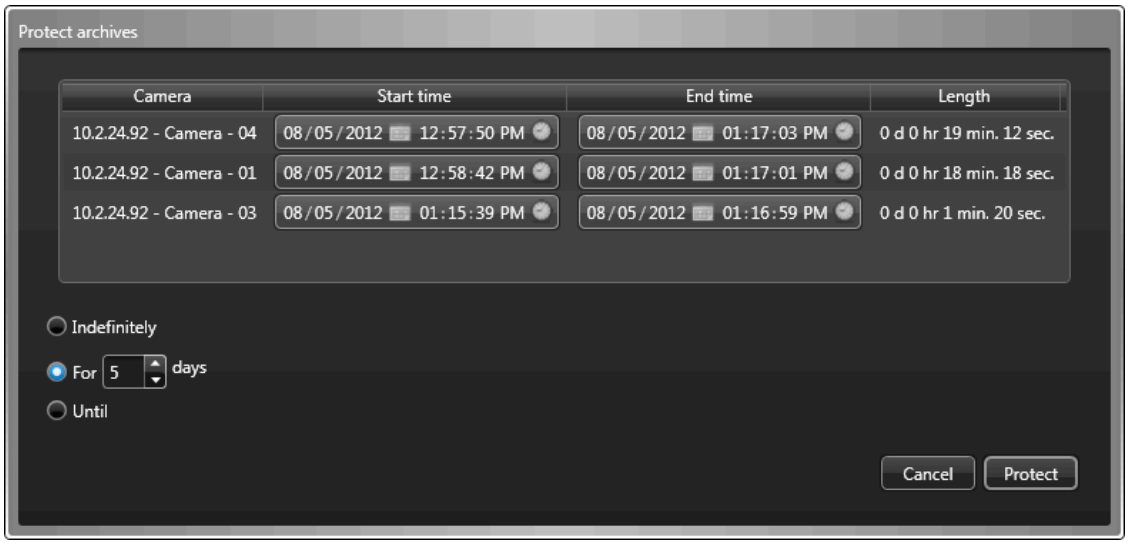
10 Create the incident package one of the following ways:

- Click **Create**.
- To create the incident report and notify other users on the system, click **Create and email**, select the users, and click **Create and email**.

  The user must have a valid email address and the server must be configured to send emails.
- To export the video sequences from all the cameras and stitch them together as a G64x file, click **Create and export**.

If you chose to protect the video sequences that you added to the incident package, then the *Protect archives* dialog box opens.

11 In the *Protect archives* dialog box, set the **Start time** and the **End time** for the video that you want to protect.



12 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 information about archive storage, see the *Security Center Administrator Guide*.

- **For x days:** The video file is protected for the selected number of days.
- **Until:** The video file is protected until the selected date.

13 Click **Protect**.

If you cancel the protection settings in the *Protect archives* dialog box, the incident package is still created.

The incident package is saved in the database for reporting purposes. If you selected a user, the package is sent to them by email.

After you finish

After the incident package is created, you can send it to authorities or other users, or review it a later time using the Incidents report.

Related Topics

Reviewing and modifying reported incidents on page 488
Protecting video files from deletion on page 272

Reviewing and modifying reported incidents

You can search for, review, modify, and delete reported incidents and incident packages, using the *Incidents* task.

What you should know

If you previously reported an incident, but must edit its content (for example, modify the description, or add another camera to the report), you can search for that report using the title you wrote while creating it. Or, if you remember what camera you wrote the incident for, you can search by specific camera. If you want to search for all the noteworthy activity that was logged by other users during the last week, or since your last shift, you can search for those incidents by setting a time range.

To modify an incident report, you need the *Modify reported incidents* privilege. To delete an incident report, you need the *Delete reported incidents* privilege.

To review, modify, or delete a reported incident:

1 From the home page, open the *Incidents* task.

2 Set up the query filters for your report. Choose one or more of the following filters:

- **Title:** Restrict the search to incidents containing specific text in their title.
- **Category:** If incident categories are created, restrict the search to specific categories.
- **Creation time:** Incidents created or reported within the specified time range.
- **Description:** Restrict the search to entries that contain this text string.
- **Incident time:** Incidents reported within the specified time range. The incident time corresponds to the event or alarm timestamp the incident refers to. If the incident does not refer to any event or alarm, then the incident time corresponds to the creation time.
- **Modification time:** Incidents modified within the specified time range.
- **References:** Incidents referencing all the selected entities.
- **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 reported incidents and incident packages are listed in the report pane.

4 To review an incident and show the corresponding video in a tile, double-click or drag the item from the report pane to the canvas.

If there is no camera attached to the incident, the *Edit incident* dialog box opens. If you select an incident package, the video sequences are played back within a single tile in the order that they were recorded, and entities that were added as additional resources are displayed in different tiles.

5 If you are viewing video from an incident package, you can control the playback from the *Video sequences* widget in the *Controls* pane, as follows:

- To switch to another camera in the package, select a camera the drop-down list.
- To jump to the next or previous cameras in the package, click **Next sequence** (⏭) or **Previous sequence** (⏮).
- To jump to a specific moment in time, move your cursor to that spot on the timeline.

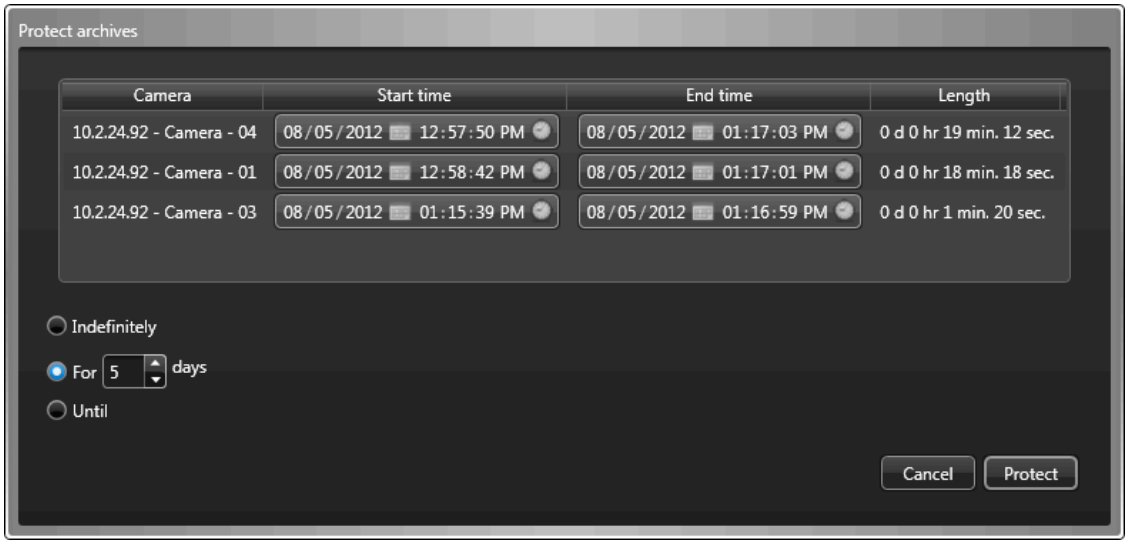
6 Modify or delete the incident as follows:
   a) Select an incident in the report pane.
   b) At the bottom of the report pane, click **Edit** ( ) or **Delete** ( ).
   c) If modifying, in the *Edit incident* dialog box, edit the incident description.
   d) From the **Category** drop-down list, change the incident category.
   e) In the *References* section, click or to add or remove referenced entities.
   f) In the *Video sequences* section, you can do the following:
      - Edit the time ranges of the video sequences included in the incident report.
      - To add another camera to the package, click **Add an item** ( ), select a camera and the time range, and click **Add**.
      - To protect the video sequences, select the **Protect video from deletion** option.

7 To save the report, do one of the following:
   - To save the incident report, click **Save**.
   - To save the incident and notify other users on the system, click **Save and email**, select the users, and click **Save and email**.

     NOTE: The user must have an valid email address and the server must be configured to send emails.

   If you chose to protect the video sequences that are included in the report, then the *Protect archives* dialog box opens.

8 In the *Protect archives* dialog box, set the **Start time** and the **End time** for the video that you want to protect.



9 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 information about archive storage, see the *Security Center Administrator Guide*.
   - **For x days:** The video file is protected for the selected number of days.
   - **Until:** The video file is protected until the selected date.

10 Click **Protect**.

   If you cancel your changes in the *Protect archives* dialog box, the incident report is still saved.

The updates you made to the incident report are saved in the database. If you selected a user, the incident report is sent to them by email.

Related Topics

Reporting incidents on page 483
Creating incident packages on page 485

Report pane columns for the Incidents task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Incidents task.

- **Title:** Title of the incident.
- **Category:** Category of the incident.
- **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.
- **References:** List of entities referenced by the incident.
- **Incident time:** The timestamp of the referenced alarm or event. If no event is referenced, it corresponds to the incident creation time.
- **Created by:** User who first reported the incident.
- **Creation time:** Time the incident was reported.
- **Modification time:** Time the incident was last modified.
- **Modified by:** User who last modified the incident.
- **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.

Responding to critical events through threat levels

If a dangerous situation arises while you are monitoring your system (for example, a fire or shooting), you can respond by changing the state of the entire Security Center system or specific areas, using threat levels.

Before you begin

To set threat levels, you need the *Set threat level* user privilege. If the Threat levels icon ( ) is not displayed in the notification tray, you can show it from the *Options* dialog box.

What you should know

When you set a threat level, you could force a complete lock down, temporarily override lock schedules, trigger an alarm, deny certain cardholders access to areas, and so on. The exact effects of setting a threat level depend on how it is configured in Config Tool. For information about configuring threat levels, see the *Security Center Administrator Guide*.

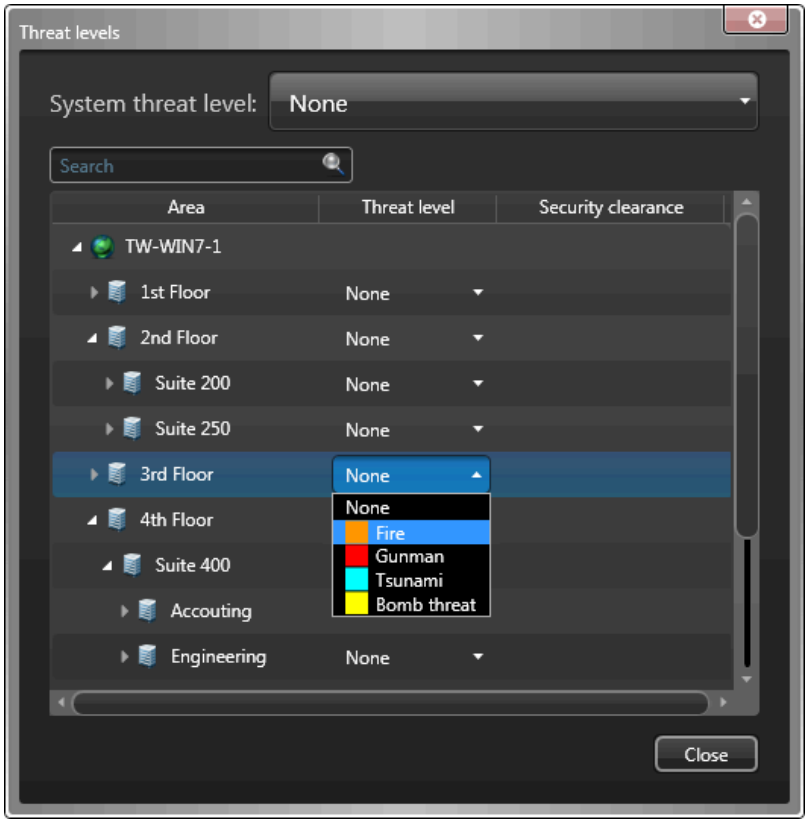
To set a threat level:

1 Open the *Threat levels* dialog box one of the following ways:

- In the notification tray, double-click the **Threat levels** ( ) icon.
- From the home page, click **Tools** > **Threat levels**.

2 Do one of the following:

- To set a threat level on the entire system, select a threat level from the **System threat level** drop-down list.
- To set a threat level on a specific area, select a threat level from the drop-down list next to the desired entity.



3 In the confirmation dialog box that opens, click **Apply** > **Close**.

The **Threat levels** icon in the notification tray turns red ( ). If you set a threat level on the entire system, the background of Security Desk turns the color of the threat level. Additional effects of setting the threat level depend on how the threat level was configured.

TIP: You can view the current threat level status of areas in the *System status* task.

Example

If a fire broke out and you set the *Fire* threat level, the fire alarm could be triggered, all doors could be unlocked, cameras could start recording, and so on.

Related Topics

Configuring the notification tray on page 94

Clearing threat levels

Once the critical event is no longer active, you can clear the threat level and return Security Center to its normal state.

To clear a threat level:

1. From the notification tray, double-click the **Threat levels** ( ) icon.
2. To reset the security clearance level to **None** (level 7) for all areas while the threat is still set, click **Reset minimum security clearance**.
3. To clear the threat level, do one of the following:
   - If a threat level was set on the entire system, from the **System threat level** drop-down list, select **None**.

     NOTE: You can also clear the threat level on specific areas. This also clears the threat level on all sub-areas.
   - If a threat level was set on a specific area, from the drop-down list next to the entity, select **None**.
4. Click **Close**.

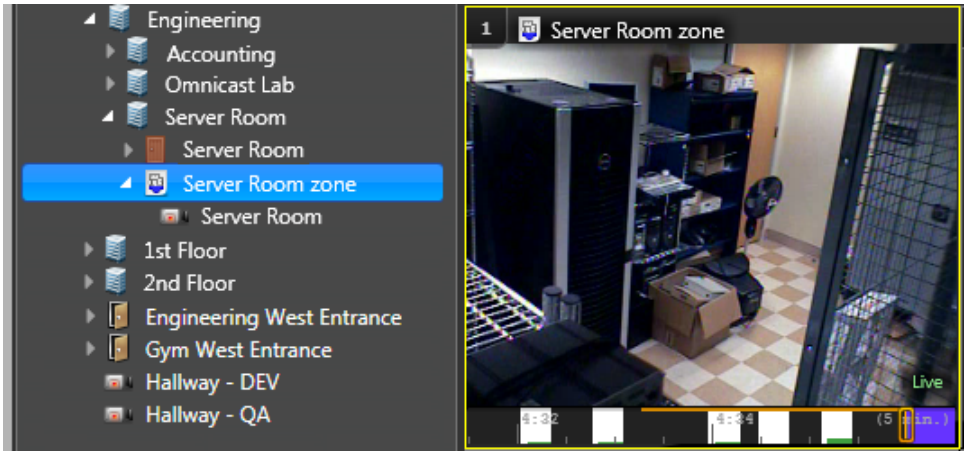
29

Zones and intrusion detection

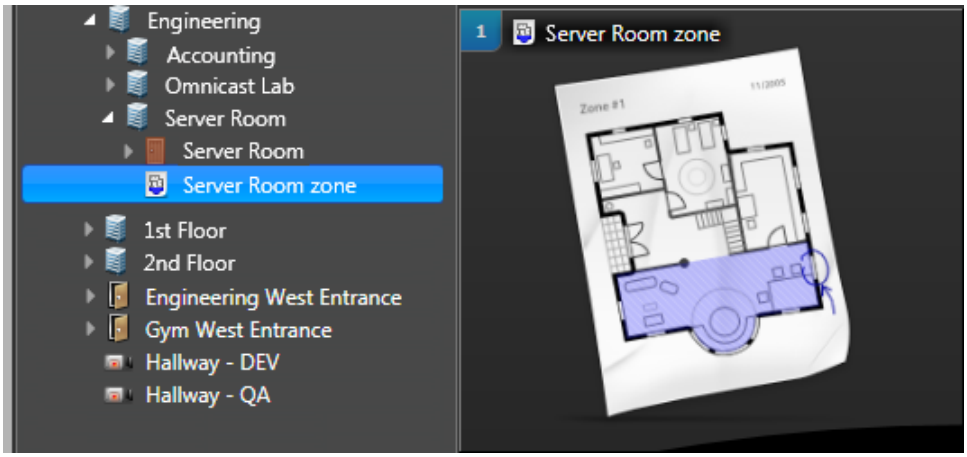
This section includes the following topics:

How zones are displayed in the Security Desk canvas

When you double-click or drag a zone entity ( ) to a tile and there is a camera linked to the zone, the camera video stream is displayed.



If a zone is not linked to any cameras, the zone icon is displayed.



About the intrusion detection overview

You can use the intrusion detection overview to monitor intrusion detection entities that require your attention. For example, an intrusion detection area in an active alarm state or an input pin in a trouble state. You can pin the overview in Security Desk to be visible at all times.

Notification tray icon

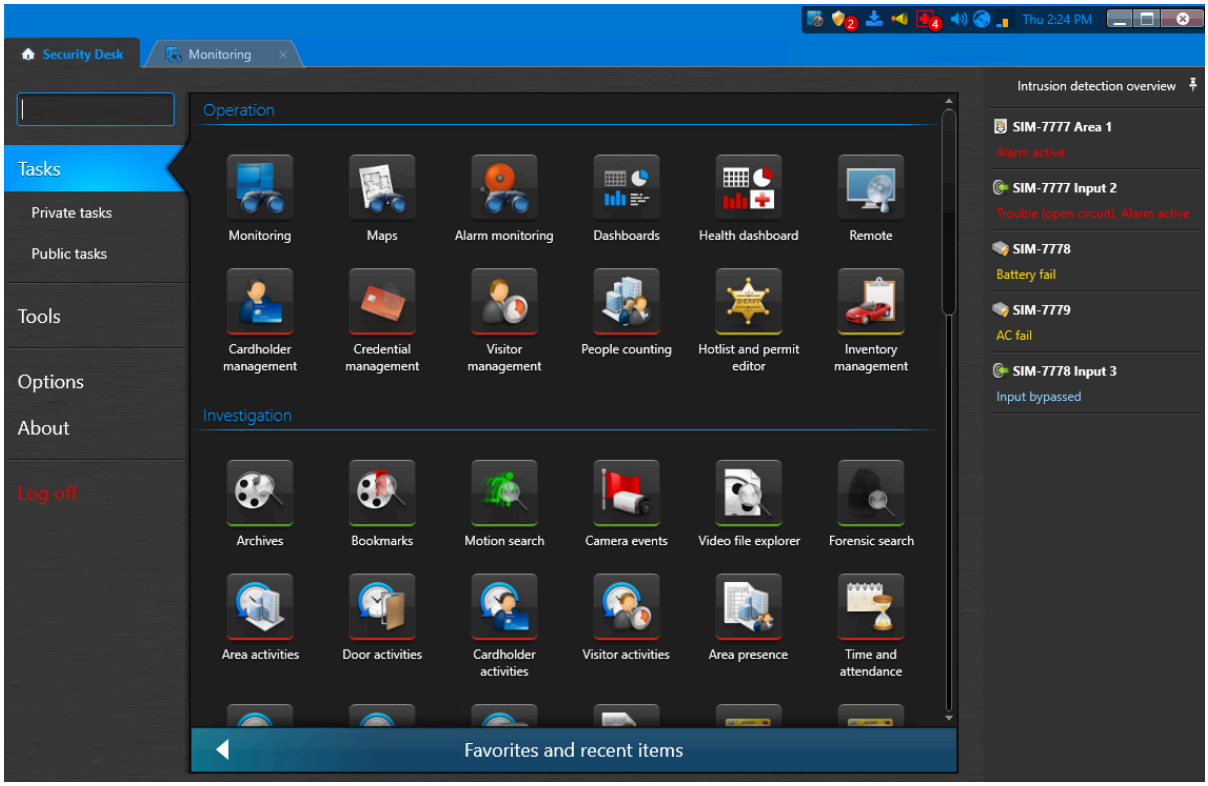
The intrusion detection overview must be enabled in the Security Desk options to be accessible from the notification tray.

When the overview is enabled, the intrusion detection icon ( ) is displayed in the notification tray. You must click the icon to initialize the overview. After it is initialized, the number of entities with issues is indicated on the notification badge, color-coded by level of importance: red for high importance, and yellow for moderate importance.

NOTE: The badge only displays the number of entities with the highest level of importance in the list. For example, if there are two high-importance issues and one moderate-importance issue, the badge only displays the number of high-importance issues ( ).

Intrusion detection overview pane

Clicking the notification tray icon displays a list of the intrusion detection entities in the system that require your attention. The entities you can monitor include intrusion detection areas, units, and inputs. The entity list can be pinned to be visible from any task you are working in.



Commands from the overview

Depending on the entity type, different commands are available by right-clicking the entity in the list. If the entity is on a map, you can double-click it in the list to open a dialog box showing the entity on the map.

Arming and disarming zones

You can arm and disarm a zone from the *System status* task.

What you should know

You can also arm and disarm zones using the *Zone* widget in the *Controls* pane when a zone is displayed in a tile.

To arm or disarm a zone:

1 From the home page, open the *System status* task.
2 From the **Monitor** drop-down list, select **Zones**.
3 In the *Selector*, select an area.
4 To search for zones within sub-areas, select the **Search member entities** option.
The zones are listed in the report pane.
5 Select a zone, and do one of the following:

- To arm the zone, click **Arm** ( ).
- To disarm the zone, click **Disarm** ( ).

Related Topics

Zone widget on page 51

Investigating zone events

You can investigate events related to *zones* (zone armed, zone disarmed, lock released, and so on), using the *Zone activities* report.

What you should know

For example, if you want to see all the activities that happened in a particular zone during a certain time period, you can select a zone, and a time range for the report. You can search for critical events only, by selecting the zone related events you are interested in (for example, door forced open).

To investigate zone events:

1. From the home page, open the **Zone activities** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **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.
   - **Events:** Select the events of interest. The event types available depend on the task you are using.
   - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
   - **Zones:** Select the zones to investigate.
3. Click **Generate report**.
   The zone events are listed in the report pane.
4. To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.
   If there is no camera attached to the zone, the zone icon is displayed.
5. To control the zones, use the zone widget.

Related Topics

Zone widget on page 51

Report pane columns for the Zone activities task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Zone activities 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.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **Occurrence period:** Period when the event occurred.
- **Zone:** Zone name.

Changing intrusion detection area statuses

You can arm and disarm an intrusion detection area, and trigger an intrusion alarm, from the *Maps* task, the *Monitoring* task, and the *System status* task.

What you should know

You can arm, disarm, and trigger an intrusion alarm using the *Intrusion detection area* widget when an intrusion detection area is displayed in a tile or on a map. You can also silence and acknowledge the intrusion alarm when it is active.

To change the status of an intrusion detection area from the *System status* task:

1. From the home page, open the *System status* task.
2. From the **Monitor** drop-down list, select **Intrusion detection area**.
3. In the *Selector*, select an intrusion detection area.
4. To search for intrusion detection areas within sub-areas, select the **Search member entities** option.
   The intrusion detection areas are listed in the report pane.
5. Select an intrusion detection area, and do one of the following:
   - To arm the area, click .
   - To disarm the area, click .
   - To trigger an intrusion alarm, click .
   - To silence the intrusion alarm, click .
   - To acknowledge the intrusion alarm, click .

To change the status of an intrusion detection area from the *Monitoring* or *Maps* task:

1. Do one of the following:
   - Use the Intrusion detection area widget on page 45.
   - Right-click the tile and click **Intrusion detection area**.

Investigating intrusion detection area events

You can investigate events that occur in intrusion detection areas (Intrusion detection area master armed, Intrusion detection area duress, Intrusion detection area input trouble, and so on), using the *Intrusion detection area activities* report.

What you should know

For example, if you are aware of a critical intrusion detection event (for example, *Intrusion detection area duress*) that occurred in the last 5 minutes, you can search for that event, review the video associated with the event, and trigger an intrusion alarm, if needed.

To investigate intrusion detection area events:

1 From the home page, open the *Intrusion detection area activities* task.

2 Set up the query filters for your report. Choose one or more of the following filters:

- **Intrusion detection areas:** Select the intrusion detection areas 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. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
- **Events:** Select the events of interest. The event types available depend on the task you are using.
- **Initiator:** Restrict the search to the entities at the source of the events that triggered the activity. For example, if you configured an event-to-action to trigger the action *Disarm intrusion detection area* on *Access granted (to cardholder)* event, then the cardholder would be the initiator of the *Intrusion detection area disarmed* event.

3 Click **Generate report**.

The intrusion detection area events are listed in the report pane.

4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If there is no camera associated to the intrusion detection area, the intrusion detection area icon is displayed.

5 To control the selected tile, use the intrusion detection area widget.

Related Topics

Intrusion detection area widget on page 45

Report pane columns for the Intrusion detection area activities task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the Intrusion detection area activities task.

- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **Intrusion detection area:** Intrusion detection area name.
- **Description:** Description of the event, activity, entity, or incident.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Initiator:** Who or what performed the activity or caused the activity event.
- **Input type:** The type of input.
- **Intrusion detection unit:** Intrusion detection unit involved.
- **Occurrence period:** Period when the event occurred.

- **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 intrusion detection unit events

You can investigate events related to intrusion detection units (AC fail, Unit lost, Intrusion detection unit input trouble, and so on), using the *Intrusion detection unit events* task.

To investigate intrusion detection unit events:

1 From the home page, open the *Intrusion detection unit events* task.

2 Set up the query filters for your report. Choose one or more of the following filters:

- **Intrusion detection units:** Select the intrusion detection units to investigate.
- **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
- **Events:** Select the events of interest. The event types available 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 intrusion detection unit events are listed in the report pane.

Report pane columns for the Intrusion detection 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 Intrusion detection unit 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.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).

  NOTE: This column is empty if the event is an *input bypass*.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **Intrusion detection unit:** Intrusion detection unit involved.
- **Occurrence period:** Period when the event occurred.

Part VI

Overview of troubleshooting topics in Security Desk

This part includes the following chapters:

30

General troubleshooting

This section includes the following topics:

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
- 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.

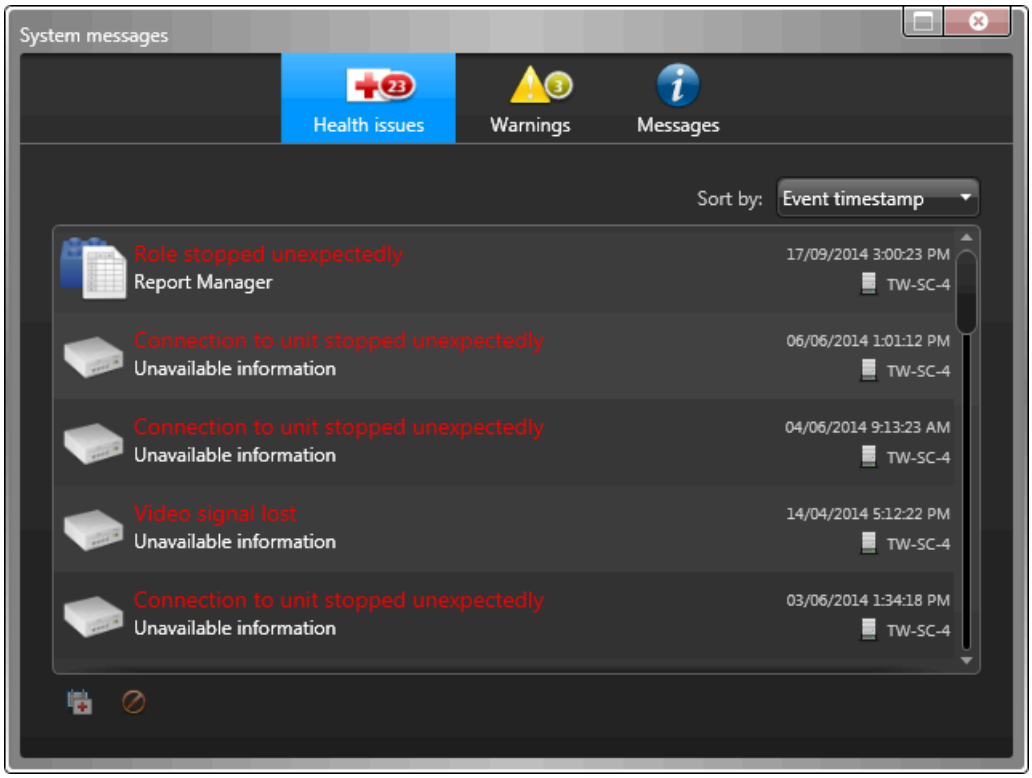
2 On the *Health issues* page of the *System messages* dialog box, do one of the following:

- 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. You must have access to Config Tool.
- 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: This option is only available to users with the *Dismiss health events* privilege. 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**.



3 On the *Warnings* ( ) page, do one of the following:

- To open the configuration page of an entity, click the entity. You must have access to Config Tool.
- 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 507

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
- 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 information about selecting which health events to monitor in Config Tool, see the *Security Center Administrator Guide*.

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 home page, 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. The range can be defined for a specific period or for global time units, such as the previous week or the previous month.
- **Health event:** Name of the health event.
- **Health severity:**

  Severity level of the health event:

  - 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

Reviewing system messages on page 505

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:
  - 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.
- **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 even 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. The range can be defined for a specific period or for global time units, 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.

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 needs to select which health events to monitor by configuring the Health Monitor role. For information about selecting which health events to monitor in Config Tool, see the *Security Center Administrator Guide*.
- **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 come and look at 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 *maintenance 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 *maintenance 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 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** drop-down 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

Viewing system health events on page 507
Troubleshooting: entities on page 514
Overview of the System status task on page 599

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. For information about schedule conflicts, see the *Security Center Administrator Guide*.
- Troubleshoot the Archiver role.

Related Topics

Viewing entities in the canvas on page 27
Searching for entities on page 90
Troubleshooting: entities on page 514

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** drop-down 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 513

Setting entities to maintenance mode

If you must change the configuration of an entity or perform maintenance on a device, such as a camera or access control unit, you can put the device in maintenance mode to avoid affecting health statistics.

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:
  - Roles
  - Video units
  - Cameras
  - Access control units
  - Intrusion detection units
  - Hardware zones
  - Alarms
  - Patrol vehicles
  - ALPR units
- You can unlock doors for maintenance purposes using **Override unlock schedules** for the door in the *Monitoring* task or the *Maps* task.
- You cannot trigger alarms that are set to maintenance mode, not through event-to-actions nor manually.

  NOTE: Setting an active alarm to maintenance mode does not acknowledge it.

To set an entity to maintenance mode:

1. Open the *Monitoring* task in Security Desk
2. Select the entity or entities from the entity tree, right-click and select **Maintenance mode** ( ).

   You can also select maintenance mode from right-clicking a tile or map entity.
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. In the **Reason** field, enter the reason you are setting the entity in maintenance mode.
6. Click **Save**.

   If Federation™ role icons are not refreshed right away, press F5 to refresh the entity tree.

The entity is in maintenance mode for the duration 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 when applicable. When you hover over the entity icon in the area view or on maps, the reason the entity is in maintenance mode is displayed.

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. For more information about configuring roles in Config Tool, see the *Security Center Administrator Guide*.

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

To deactivate a role:

1 From the home page, open the *System status* task.

2 From the **Monitor** drop-down 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** ().

Troubleshooting: query filters

When you are generating a report or searching for entities, you must use filters to specify your search criteria. When a filter is activated, it is indicated with the On ( ) LED icon. However, if a filter is invalid, an error or warning message is displayed.

- **Warning ( ):** There is a potential problem with the information in the filter. The report or search might take longer than usual to generate.
- **Error ( ):** There is a problem with the information in the filter. You cannot generate the report or search when there is an error.

Hover your mouse over the icon to see the warning or error message in a tooltip. The following table lists some examples of messages you can receive, and what you do to fix the issue.

Warning/error message	Try this
The search covers multiple days	Decrease the time range for your report or search.
There are no selected entities	Your filter is empty. Select an entity, or turn off the filter.
There is no selection	Your filter is empty. Select an option, or turn off the filter.
The dates and times are invalid	The time range is invalid. You might have set the start date and time after the end date and time, or the end date and time before the start date and time. Reconfigure your time range for the report.

Related Topics

Generating reports on page 72
Searching for entities on page 90
Selecting date and time ranges for reports on page 73

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, Archiver collection and Video inventory. See the steps below for a complete list of these collections and what they contain.
- Running the Diagnostic data collector may temporarily impact system performance.
- If your system is running Windows XP or 2003, Windows event logs and performance monitor data are not collected.

To collect diagnostic information:

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

2 From the dialog box, select one of the following:

- **Default data collection on all Security Center servers:** Sends only a set of predefined data collections (default)"
- **Specific data collection and servers:** Sends a set of data collection and server information that you have selected.

3 If selecting **Specific data collection and servers**, do the following:

a) On the left pane, select the server(s) you need information from.

b) On the right pane, select the specific collection type(s) from that server.

You can select from the following collections:

- **System Information:** (Selected by default) A data collection used for diagnostic testing that includes system logs and system information not specific to Genetec applications. This collection contains:
  - Genetec Event logs
  - System Event logs
  - Application Event logs
  - Security Event logs
  - Installed applications
  - Installed updates
  - Currently running applications
  - Currently active network connections
  - .NET CLR assemblies required for debugging
- **Genetec System Information:** (Selected by default) A data collection used for diagnostic testing that includes Genetec™ applications specific information. It contains:

- Security Center configuration files
- Security Center trace logs
- Security Desk and Config Tool error logs (when the clients are selected)
- Performance monitor data
- Running processes information
- Security Center running processes information with loaded assemblies
- Memory dumps
- Registry Keys (only the ones that are used or created by Genetec Inc.)

- **Archiver Agent:** A data collection used for diagnostic testing that includes Archiver-specific information such as Archiver cache and Archiver logs.
- **Access Manager:** A data collection used for diagnostic testing that includes Access Manager-specific information. It includes configuration files, currently active network connections, VertX file cache and VertX temp files.
- **Video Unit Inventory:** A data collection used for diagnostic testing that lists video units enrolled by the system and Security Center federated cameras

4 Click **Start**.

The status bars show the progress for each data collection. The information is saved on the computer from which the tool was run to folder: *C:\ProgramData\Genetec Security Center 5.10\Diagnostics*. For Windows XP and 2003, the data is saved in: *C:\Documents and Settings\All Users\Application Data\Genetec Security Center 5.10\Diagnostics*.

5 To open the folder, click **Open drop folder**.

You can now send the diagnostic information to Genetec™ Technical Assistance Center.

31

Troubleshooting video

This section explains some of the reasons why you might not be able to view video in Security Desk, and what you can do to fix those issues. It also explains how to respond when you receive certain error messages when trying to view video. To perform these procedures, you need access to Config Tool and Security Desk. If you are not an administrator, you might not be able to perform every troubleshooting step.

This section includes the following topics:

Video units offline in Security Center

When a camera is red in the area view, it means 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.

Before you begin

Ensure that you have access to Security Desk and Config Tool to perform the following steps.

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 caused by 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 the unit is supported by Security Center, and that it 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 will 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.

Cannot watch live video in Security Desk

If you cannot view live video in Security Desk, you can troubleshoot the issue.

Before you begin

Ensure that you have access to Security Desk and Config Tool to perform the following steps.

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 it was 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:

- **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 stream was requested and received by the client workstation. 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 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 the unit is supported by Security Center, and that it 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** drop-down 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 a list of default ports that are used in Security Center, see the *Security Center Administrator 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.

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 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**.

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:

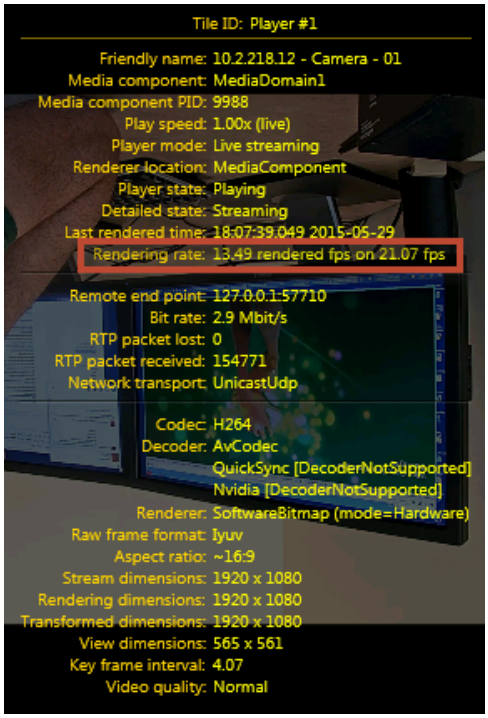
- The speed at which the workstation processes video, which indicates how much load is on the workstation's CPU and memory.
- The speed at which the network is sending video to the workstation.

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.



Example

If your rendering rate is "13.49 rendered fps on 21.07 fps", your workstation is processing 13.49 fps. However, it is receiving video at 21.07 fps. The workstation cannot process all the frames it is receiving. Your workstation is the cause of the degraded quality of the video you are monitoring. In this case, lighten the load and check the hardware and its drivers.

- Reduce the number of cameras you are monitoring to reduce the load on the workstation.
- Check the hardware requirements to make sure 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 all drivers are up to date.

If your rendering rate is "13.49 rendered fps on 13.49 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 to determine whether the network is not 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.

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.

Before you begin

Ensure that you have access to Security Desk and Config Tool to perform the following steps.

To diagnose an Impossible to establish video session with the server error:

1. Make sure 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:
   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 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.

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.

Cannot watch playback video in Security Desk

If you cannot view playback video or video archives in Security Desk, you can troubleshoot the issue.

What you should know

Ensure that you have access to Security Desk and Config Tool to perform the following steps.

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 521.

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 the unit is supported by Security Center, and that it 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 a list of default ports that are used in Security Center, see the *Security Center Administrator Guide*.

6 If you still cannot view playback video, contact Genetec™ Technical Assistance Center.

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.

Before you begin

Ensure that you have access to Security Desk and Config Tool to perform the following steps.

What you should know

If you can view live video from a camera but cannot record video, it might be due to the recording mode of the camera, the Archiving schedule, the Archiver role database, or even your CPU usage.

Here are some ways to identify if the camera is not recording:

- When viewing live video, the recording status of the camera is indicated in the lower-right corner of the tile. If the status indicates Live, the camera is not recording.
- You are trying to view playback video, but no video is available for the date and time you selected, and you know that there should be.
- 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 the unit is supported by Security Center, and that it 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 is 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**, then continue with the next substep.
   c) In the *Video* task, select the Archiver.
   d) Click the **Camera default settings** tab.
   e) In the *Recording modes* section, make sure the Archiver is set to record on the correct **Schedule**, and that the recording **Mode** is not set to **OFF**.
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 the **Motion detection** tab.
   c) Verify the motion detection settings.
      For more information about motion detection settings, see the *Security Center Administrator 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.

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 *Transmission 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 not over 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.

      For more information about adding units in Security Center, see the *Security Center Administrator Guide*.

After you finish

If you still cannot record video on the camera, contact Genetec™ Technical Assistance Center.

32

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. The range can be defined for a specific period or for global time units, 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.
- **Firmware version:** Firmware version installed on the unit.
- **Time zone:** Time zone of the unit.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **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.

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 home page, 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 537

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 home page, 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 home page, 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.

Troubleshooting: Driver fails to install for HID OMNIKEY USB readers

If, each time you try to enroll a credential using an HID OMNIKEY USB reader, you see an error message from Windows indicating that the driver failed to install, there are some troubleshooting steps you can use to resolve the issue.

Before you begin

- Disconnect the OMNIKEY reader from your workstation.
- Close Security Desk and Config Tool.

What you should know

This issue typically occurs because Windows cannot find the appropriate driver for the reader. Because Windows will try to load the default USB driver, the reader can appear to work properly until you observe some undesirable behavior. To avoid such behaviors, it is recommended to install the driver that is specific to this type of readers provided by the manufacturer.

To troubleshoot the driver that fails to install:

1. Make sure that your OMNIKEY reader is compatible with Security Center and is configured properly.

   For a list of compatible devices and configuration settings, see Knowledge Base article KBA01374 on Genetec™ TechDoc Hub.
2. Install the driver following the instructions provided in the *OMNIKEY Smart Card Reader User Guide*.

   You can obtain this guide by visiting HID's website at http://www.hidglobal.com/documents.
3. When installation is completed, start Security Desk, and then check that the reader is enabled.
4. Try to enroll a credential again.

The error message should not be displayed anymore.

Appendices

Security Desk reference

This section includes the following topics:

A

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.

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.
Access denied: Inactive cardholder	cardholder, door, or elevator	A cardholder with an inactive profile has attempted to access a door or elevator.

Event	Source entity	Description
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.
Agent started	Wearable Camera Manager role	Health event generated when a role agent starts.

Event	Source entity	Description
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.
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.
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.

Event	Source entity	Description
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.
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.

Event	Source entity	Description
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.
Intrusion detection area canceled postponed request	intrusion detection area	Intrusion detection area postponed request is canceled.

Event	Source entity	Description
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.
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.

Event	Source entity	Description
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.
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.
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.

Event	Source entity	Description
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.
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.

Event	Source entity	Description
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, Genetec Patroller™	An offload from Genetec Patroller™ to Security Center has failed.
Offload successful	ALPR Manager, Genetec Patroller™	An offload from Genetec 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.
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.

Event	Source entity	Description
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.
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 field, and the two sources are labeled and . You can find the faulty unit that is causing this conflict.

Event	Source entity	Description
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 565.
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. If you see this error, contact your system Administrator to resolve the issue.
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.
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.

Event	Source entity	Description
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.
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.

Event	Source entity	Description
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.
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.

Event	Source entity	Description
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.
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.

Event	Source entity	Description
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	Genetec Patroller™, Mobile Sharp	An update on Genetec Patroller™ or a Mobile Sharp unit has failed, or a file could not be synchronized on a Genetec Patroller™ computer.
Update installation completed	Genetec Patroller™, Mobile Sharp	An update has completed on Genetec Patroller™ or a Mobile Sharp unit, and no reboot is required.
Update installation started	Genetec Patroller™, Mobile Sharp	A user has started an updated on Genetec Patroller™ by clicking the “Update” icon.
Update published	Genetec Patroller™, Mobile Sharp	An update has been processed, and is ready to be deployed to Genetec Patroller™.
Update uninstallation completed	Genetec Patroller™, Mobile Sharp	A rollback on Genetec Patroller™ or a Mobile Sharp unit has completed.
Update uninstallation started	Genetec Patroller™, Mobile Sharp	A user has started a rollback on Genetec 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.
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.

Event	Source entity	Description
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*.

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*. • **Report:** Select a saved public task. • **Recipients:** Select the users to the send the report to. • **Export format:** Report format, either *PDF* or *Excel*.
Email a snapshot	Sends a series of snapshots of a video feed as an email attachment to a list of users. • **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 who should receive the snapshot. An email address must be defined in the user's settings. • **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.

Action	Description

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.

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.
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.

Action	Description
Ingest event	Saves the event to a system *record type* so you can you can perform correlation queries using the *Records* 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 5.10\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 or cardholders. 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. • **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.

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.

Action	Description
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.

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.

Action	Description
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.

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.

Action	Description
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.

B

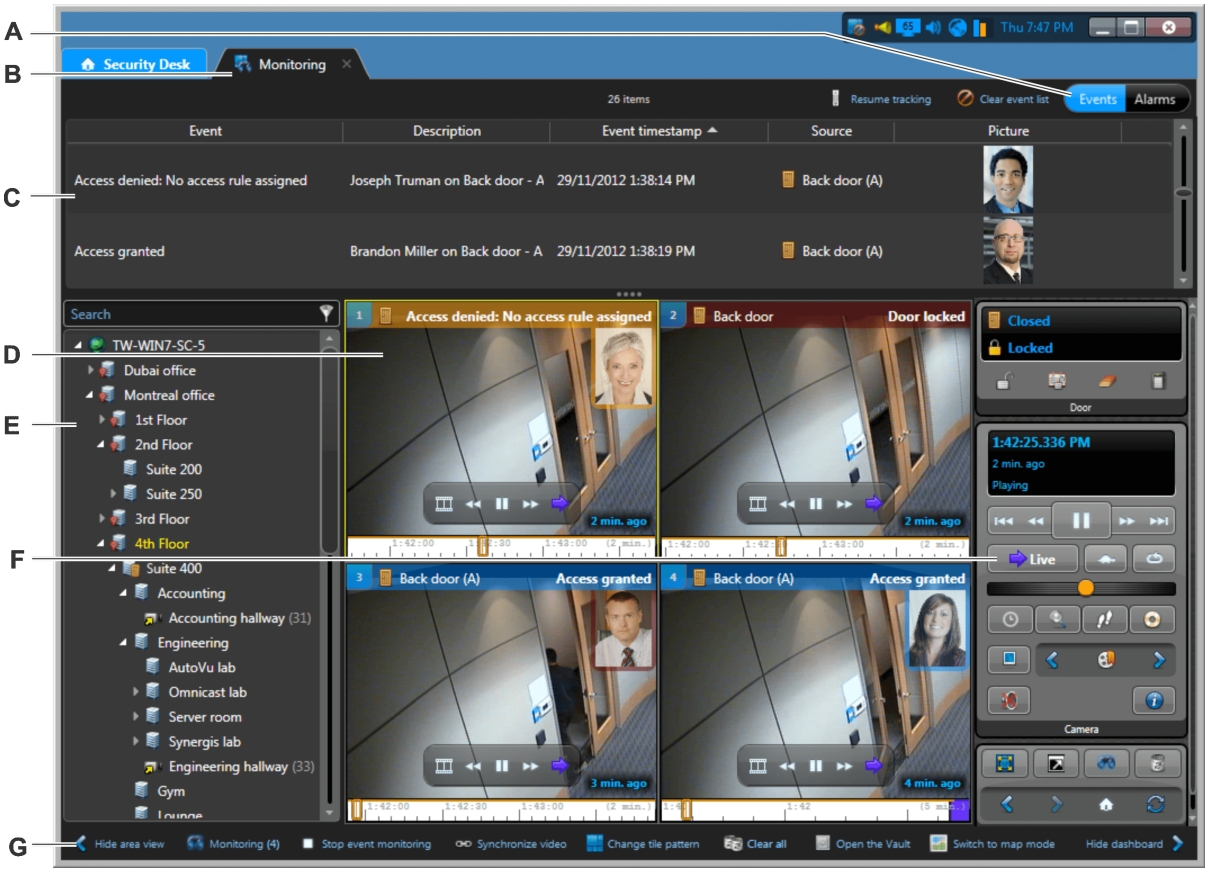
Graphical overview of Security Desk tasks

This section includes the following topics:

Overview of the Monitoring task

Use the *Monitoring* task to monitor events, such as access control events from doors and cardholders, license plate reads and hits from fixed and mobile ALPR units, and camera related events, in real time.

The following figure shows a *Monitoring* task in an access control and video monitoring system.



A	• **Events:** Show events in the report pane.
	  • **Resume tracking:** Show the events in the list as soon as they occur.
	  • **Clear event list:** Remove all the events from the event list.
	• **Alarms:** Show alarms in the report pane. The same commands as found in the Alarm monitoring task.
	NOTE: The **Events** and **Alarms** buttons are only displayed when you enable alarm monitoring for the *Monitoring* task.

B	New event alerts are displayed on the **Monitoring** tab when the task is not in the foreground.
C	The report pane lists events or alarms as they occur, based on your selection.
D	A tile can be used to monitor events (blue tile ID), alarms (red tile ID), both, or neither (grey tile ID).
E	Select entities from the area view to display in the canvas. You can select multiple entities and drag them onto the canvas together.

F	Widgets used to control the entities that you are monitoring.
G	• **Hide area view:** Hide the area view. • **Monitoring:** Select which entities to monitor. • **Synchronize video:** Synchronize the video displayed in the canvas. • **Clear all:** Clear all the configured tiles in the Monitoring task. • **Change tile pattern:** Change the tile pattern in the canvas. • **Open the Vault:** Open the Vault tool to view previously saved snapshots and exported video files. • **Switch to map mode:** Switch between *tile mode* and *map mode*. **NOTE:** To switch between tile mode and map mode, you must have the *Switch to map mode* privilege. • **Hide controls:** Hide the controls.

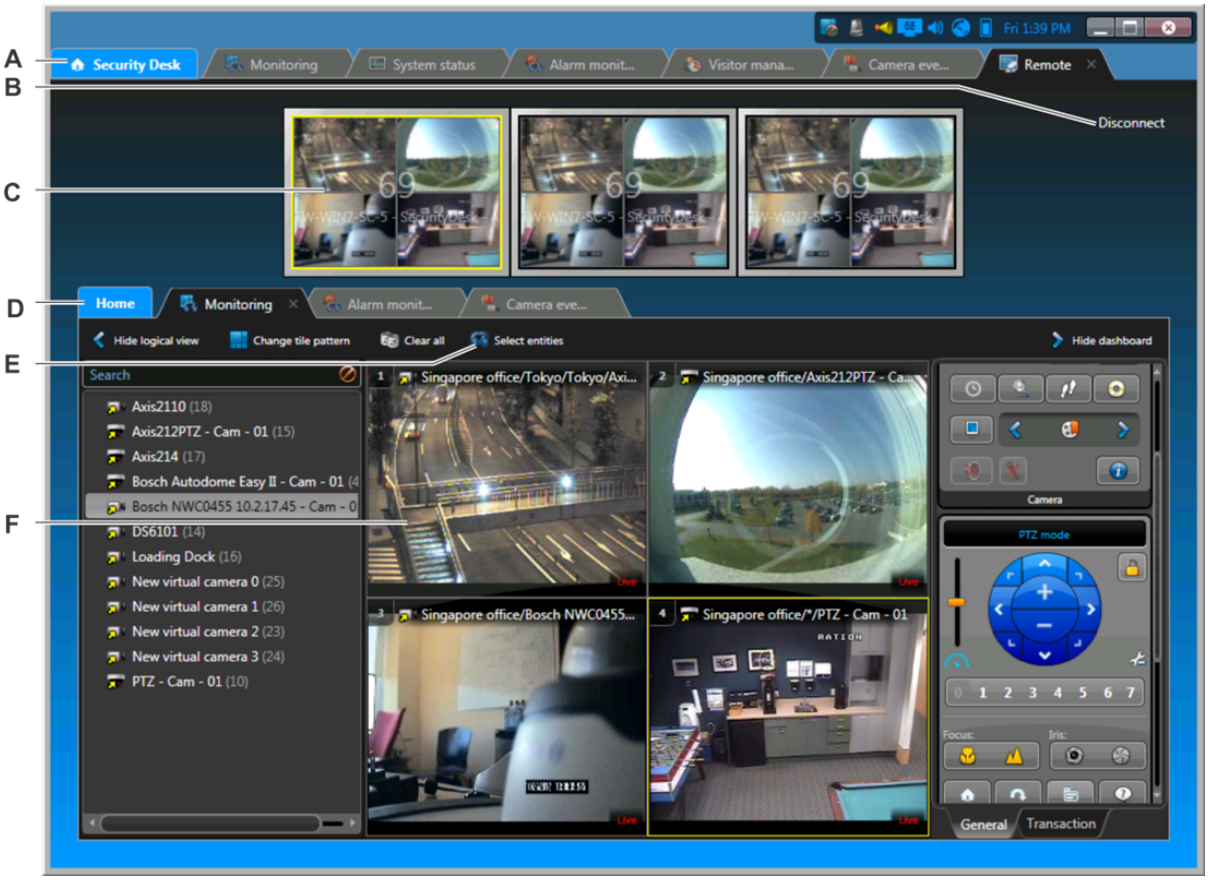
Related Topics

Monitoring events on page 84
Selecting entities to monitor on page 85
Synchronizing video in tiles on page 197
Changing tile patterns on page 31
Taking snapshots of video on page 206
Viewing exported video files on page 260
Monitoring ALPR events in tile mode on page 387

Overview of the Remote task

Use the Remote task to monitor and control other Security Desks that are part of your system remotely.

The following figure shows a Remote task.



A	Local Security Desk tasks you are working on. Click a tab to switch to that task.
B	Disconnect from the remote Security Desk.
C	Switch between Security Desk monitors you are connected to in Wall mode.
D	Remote Security Desk tasks that are open. When you are connecting remotely, you can only use the *Monitoring* task and the *Alarm monitoring* task.
E	Select the entities you want to monitor.
F	Monitor entities in the canvas. What you display in the canvas is also shown in the remote Security Desk canvas.

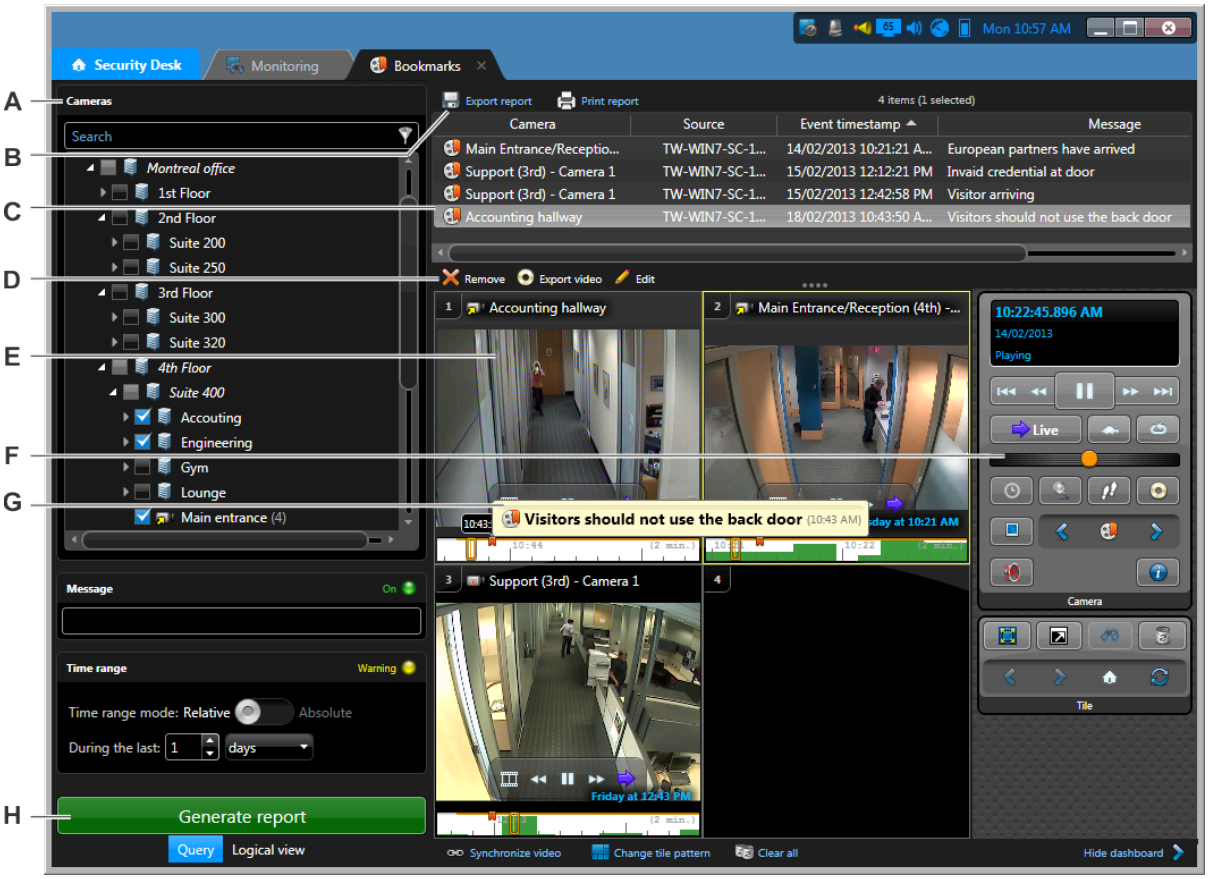
Related Topics

Remote monitoring on page 98
Connecting to remote Security Desk applications on page 99

Overview of the Bookmarks task

Use the Bookmarks task to search for, view, and generate a report of saved bookmarks.

The following figure shows the Bookmarks task.



A	Query filters.
B	Click to export or to print the report.
C	The bookmark events are listed in the report pane.
D	Options available when a bookmark is selected in the report pane: • - Delete the selected bookmarks from the database. • - Export video associated with the selected bookmarks. • - Edit the selected bookmarks.
E	Video of the bookmark in a tile.
F	Camera widget.
G	The bookmark message appears when you hover your mouse pointer over a bookmark in a tile, if one was written.
H	Run the report.

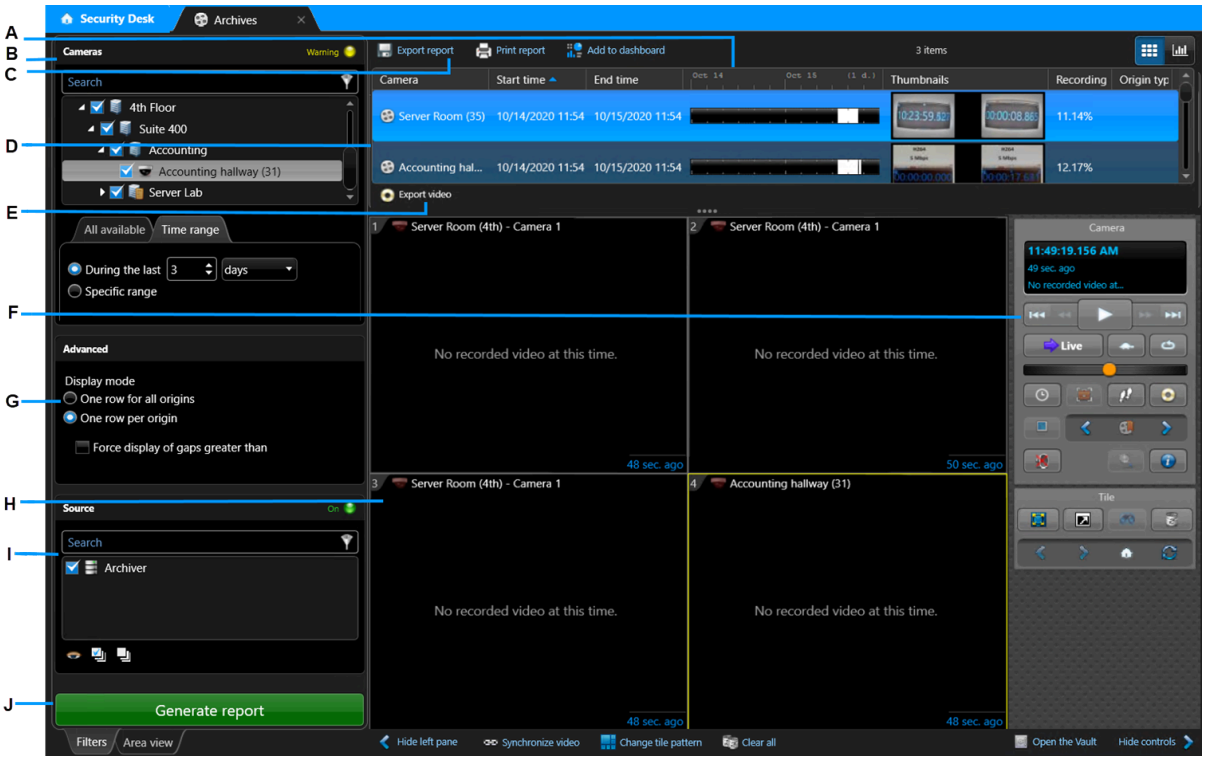
Related Topics

Adding bookmarks to video sequences on page 204
Viewing bookmarked videos on page 205
Exporting generated reports on page 74
Printing generated reports on page 74

Overview of the Archives task

Use the Archives task to find and view available *video archives* on your system by camera and time range.

The following figure shows the Archives task.



A	Report pane columns.
B	Query filters.
C	Export or print the report.
D	The related video recordings are listed in the report pane.
E	Export video from the selected archive.
F	Camera widget.
G	Advanced settings for display mode.
H	Video sequence of an archive in a tile.
I	Select one or more Archiver, Auxiliary Archiver, Cloud Playback, Omnicast™ Federation™, or Security Center Federation™ sources.
J	Run the report.

NOTE: When Cloud storage is enabled, selecting a video archive with content in long-term storage gives you to option to **Retrieve cloud archives** ( ).

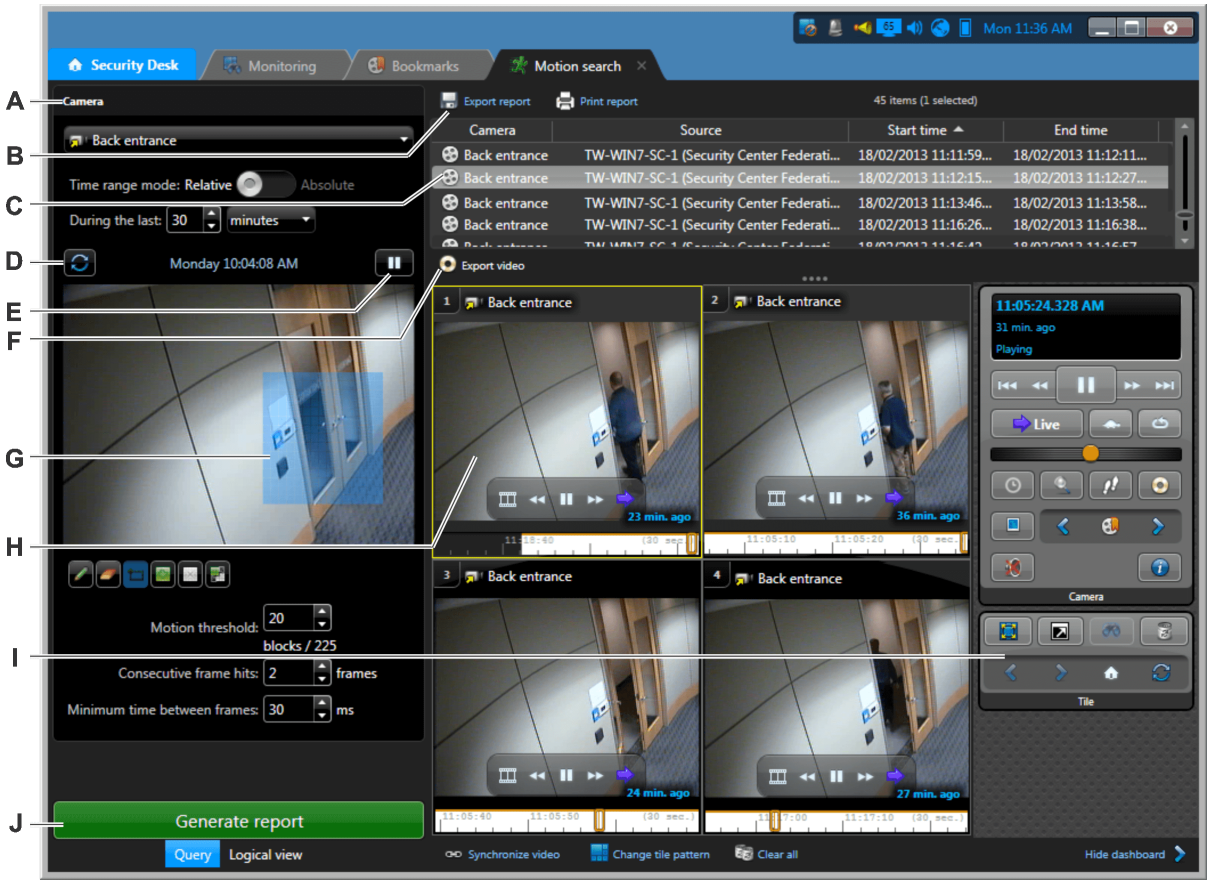
Related Topics

Viewing video archives on page 233
Exporting video in G64x format on page 250
Exporting video in G64, ASF, and MP4 formats on page 255

Overview of the Motion search task

Use the Motion search task to search the video archives for *video sequences* that detect motion in specific areas of a camera's field of view.

The following figure shows the Motion search task.



A	Query filters.
B	Export or print the report.
C	The motion events are listed in the report pane.
D	Refresh the preview image.
E	Play the video in the preview image.
F	Export video associated with the selected bookmarks.
G	Motion detection zone for your search.
H	Video sequence of a motion event in a tile.
I	*Controls* pane widgets.
J	Run the report.

Related Topics

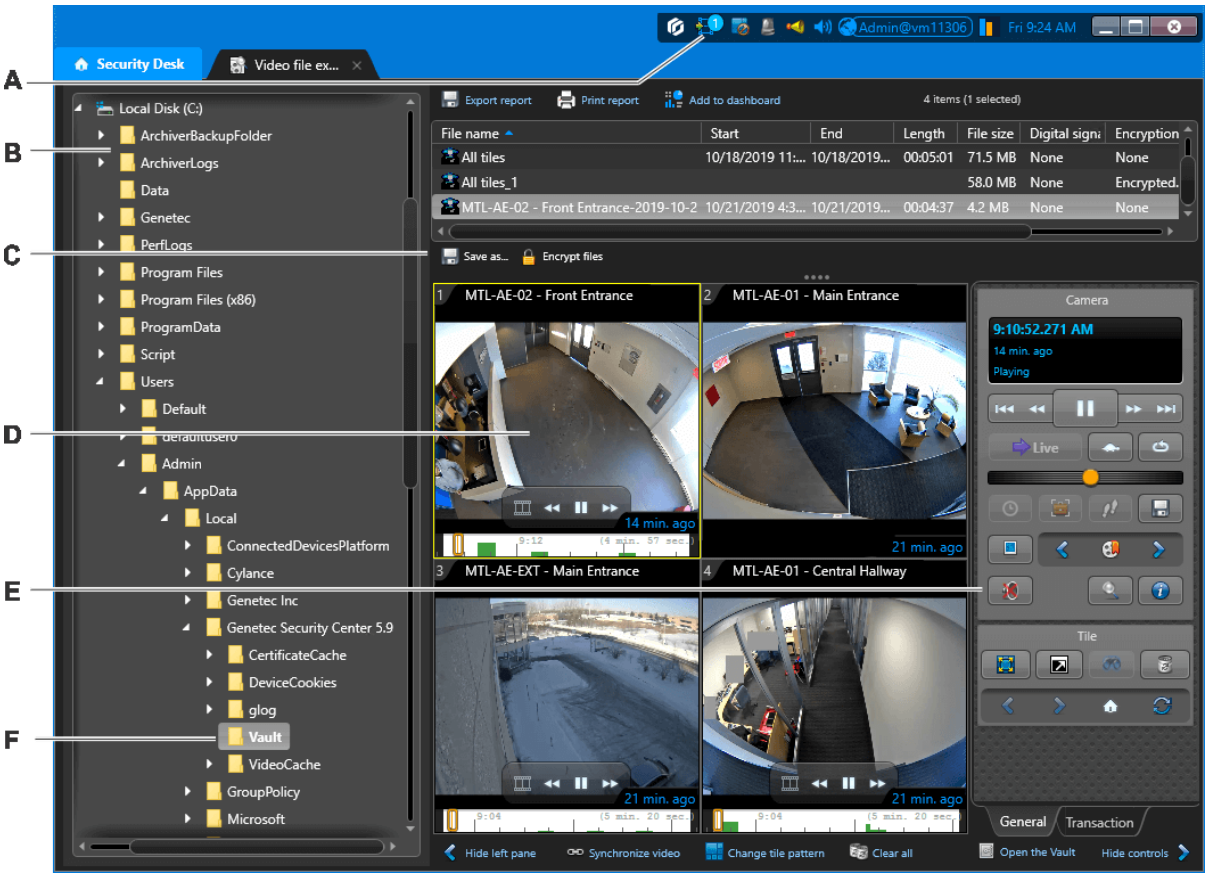
Searching video archives for motion events on page 239
Exporting video in G64x format on page 250
Exporting video in G64, ASF, and MP4 formats on page 255

Overview of the Video file explorer task

You can use the *Video file explorer* task to search for and view your exported G64x video files.

During the playback of a video file, the timeline does not show any event marker if the following applies:

- The video file was created before Omnicast™ 4.x. Video files that were created through the *Export* operation from Omnicast™ 4.x, or later, can contain bookmark or motion event markers.
- The video file is still managed by an Archiver or Auxiliary Archiver (typically found under *\VideoArchives*).
- The video file is part of a backup set (typically found under *\Tables\VideoFile*).



A	Open the *Conversion* dialog box. This icon is only displayed when you are converting G64 files to ASF format.
B	Browse for video files in folders that are on your network.
C	Options that are available when a video file is selected in the report pane: • - Convert the selected video files to ASF format. • - Encrypt the selected video files. If the video file is already encrypted, is displayed instead. • - If the video file is digitally signed, verify the digital signature. **NOTE:** Digital signatures are signed using EdDSA. Video files that were signed using RSA can still pass validation, but are reported as authenticated with an obsolete algorithm.
D	Exported video file in a tile.

E	*Controls* pane widgets.
F	Selected folder. The video files that are contained in the folder are listed in the report pane.

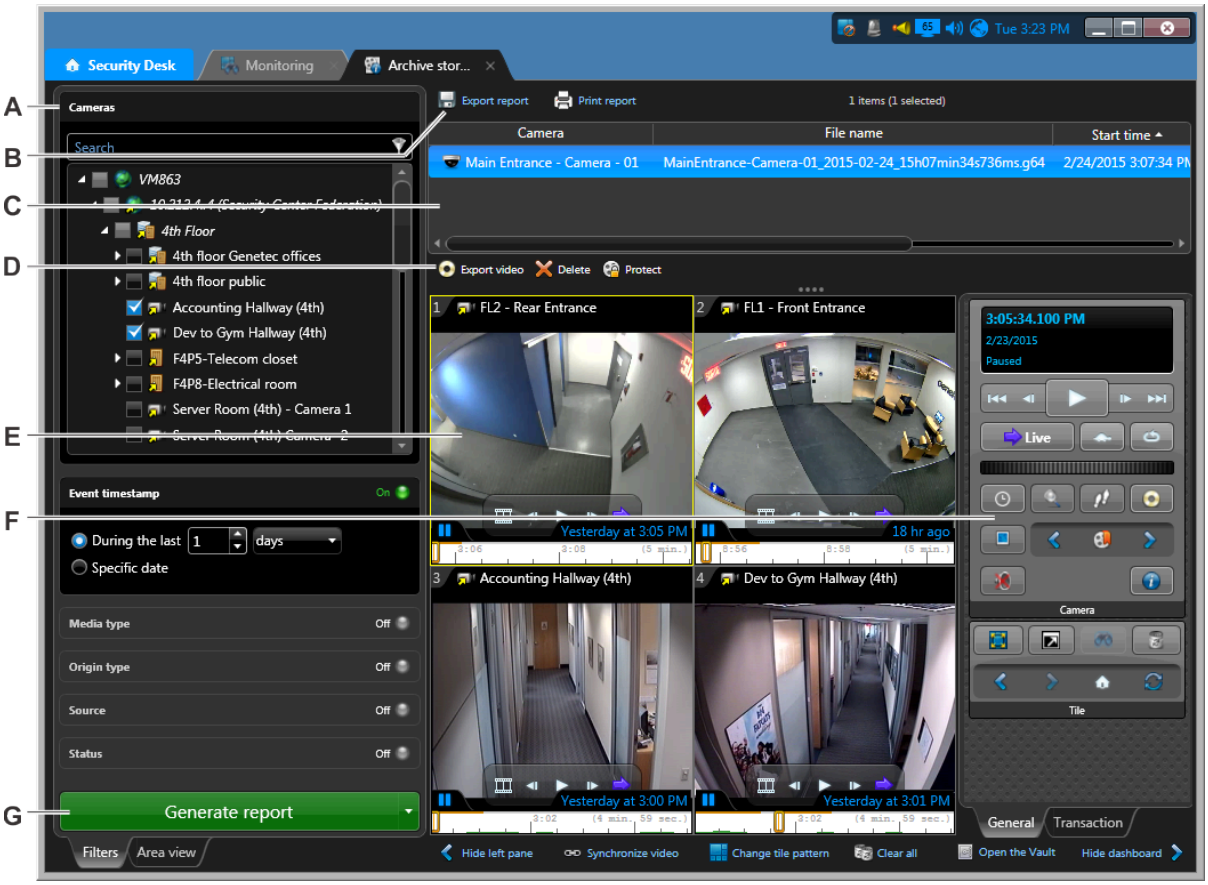
Related Topics

Viewing exported files in the Video file explorer on page 261

Overview of the Archive storage details task

Use the Archive storage details task to find the *video files* used to store *video archives* from cameras and view the properties of the video files.

The following figure shows the Archive storage details task.



A	Query filters.
B	Export or print the report.
C	The video files are listed in the report pane.
D	Options available when a video file is selected in the report pane: • - Export video associated with the selected video files. • - Remove the selected video file from the database. • - Protect the selected video files. • - Remove the automatic deletion protection from selected video files.
E	Video file displayed in a tile.
F	*Controls* pane widgets.
G	Run the report.

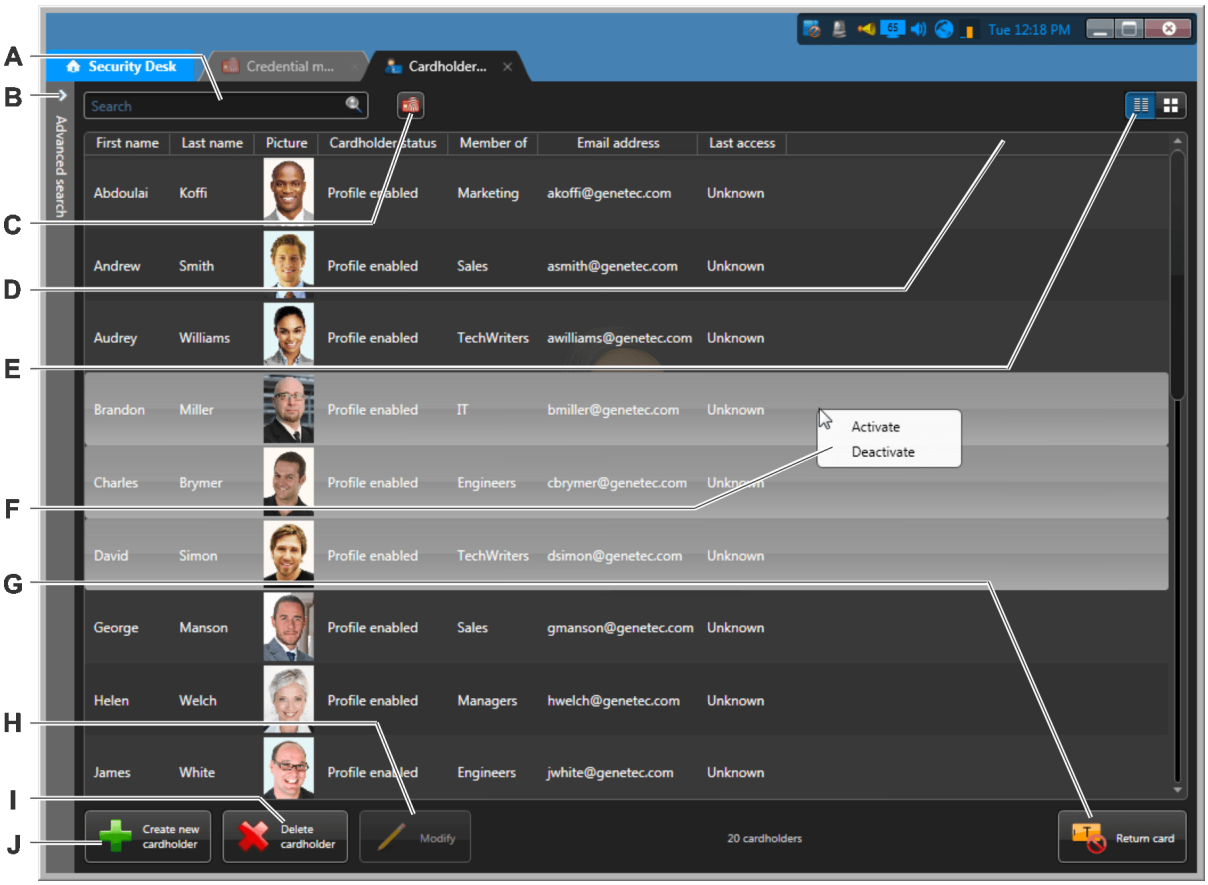
Related Topics

Viewing video file properties on page 270

Overview of the Cardholder management task

Use the Cardholder management task to create new *cardholders* in your system, modify existing cardholders, and assign credentials to cardholders.

The following figure shows the Cardholder management task. You can only have one instance of this task in Security Desk.



A	Find a cardholder by name.
B	Advanced search options.
C	Find a cardholder using their credential.
D	Select which columns to display by right-clicking the column headers or by typing Ctrl+Shift+C..
E	Switch between *Tiles* and *List* view. • **Tiles:** Shows large pictures. Pictures can be resized. • **List:** List all information concerning the entity: first name, last name, picture, activation date, expiration date, and any custom fields that are defined.
F	Activate or deactivate multiple cardholders at once. You can only make bulk changes to cardholders in the *List* view.
G	Return a temporary card.

H	View or modify the selected cardholder.
I	Delete the selected cardholder.
J	Create a new cardholder.

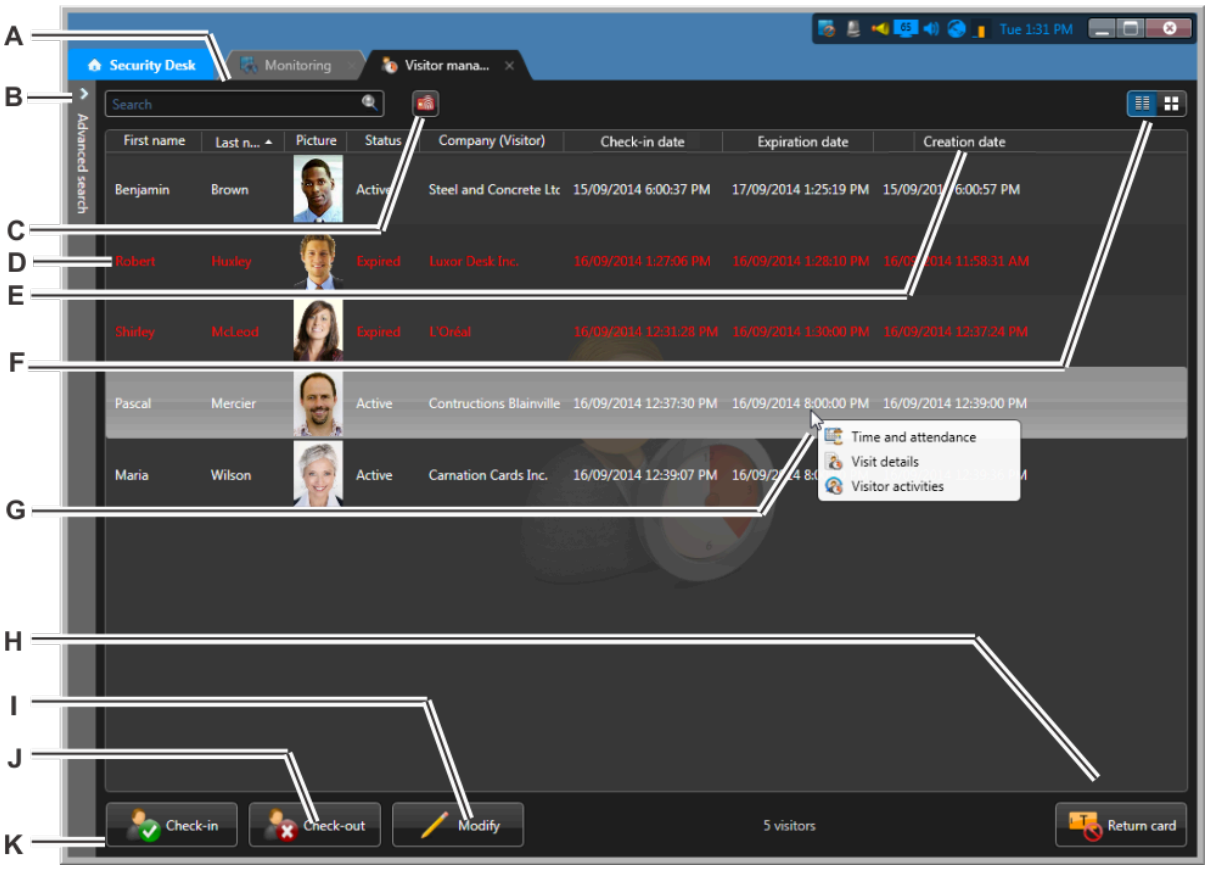
Related Topics

Creating cardholders on page 291
Assigning credentials on page 300
Assigning temporary cards on page 306

Overview of the Visitor management task

Use the *Visitor management* task to check-in new visitors, modify existing visitors, and assign credentials to visitors.

The following figure shows the *Visitor management* task. You can only have one instance of this task in Security Desk.



A	Find a visitor using their credential.
B	Find a visitor by name.
C	Advanced search options.
D	Visitors whose profiles are inactive or expired are displayed in red.
E	Select which columns to display by right-clicking the column headers or by typing **Ctrl+Shift+C**.
F	Switch between *Tiles* and *List* view. • **Tiles:** Shows large pictures. Pictures can be resized. • **List:** List all information concerning the entity: first name, last name, picture, check-in date, expiration date, creation date, and any custom fields that are defined.

G	Generate visitor reports by right-clicking the selected visitor. • () Time and attendance. • () Visit details. • () Visitor activities.
H	Return a temporary card.
I	Check-in a new or returning visitor. After a visitor is checked in, the button changes to **Check out**.
J	Delete the selected visitor.
K	View or modify the selected visitor.
L	Add a new visitor.

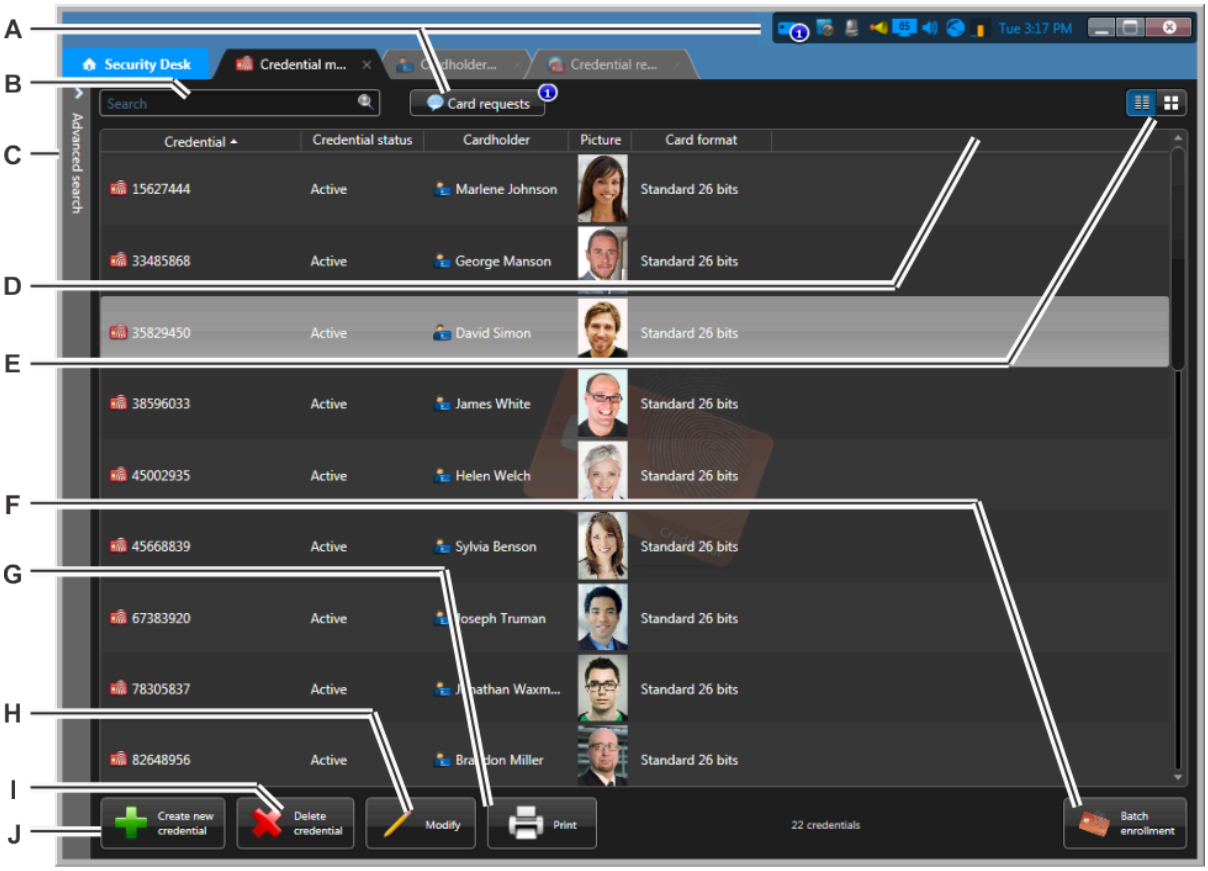
Related Topics

Checking in new visitors on page 295
Checking out visitors on page 309
Tracking attendance in an area on page 317
Tracking the duration of a visitor's stay on page 319
Investigating visitor events on page 312
Restoring original cards to cardholders and visitors on page 306
Checking in returning visitors on page 297

Overview of the Credential management task

Use the Credential management task to create, modify, and delete credentials, and print badges.

The following figure shows the *Credential management* task. You can only have one instance of this task in Security Desk.



A	View, modify, or respond to outstanding credential card requests.
B	Find a credential by name.
C	Advanced search options.
D	Select which columns to display by right-clicking the column headers or by typing Ctrl+Shift+C.
E	Switch between *Tiles* and *List* view. • **Tiles:** Shows large pictures. Pictures can be resized. • **List:** List all information concerning the entity: first name, last name, picture, activation date, expiration date, and any custom fields that are defined.
F	Enroll multiple credentials into your system at once.
G	Print the selected credential cards.
H	View or modify the selected credential.

I	Delete the selected credentials.
J	Create a new credential.

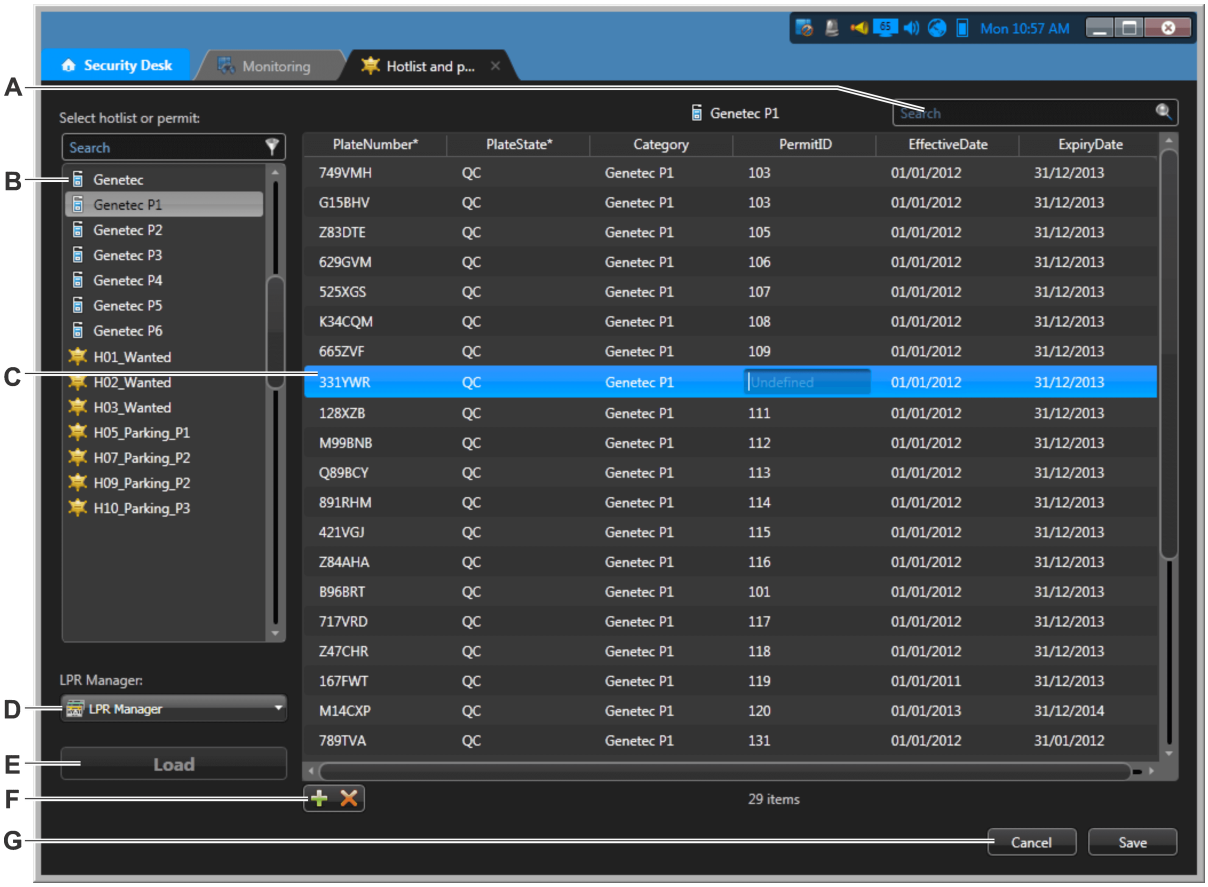
Related Topics

Creating credentials on page 344
Enrolling multiple credentials automatically on page 340
Enrolling multiple credentials manually on page 342
Searching for credentials on page 356

Overview of the Hotlist and permit editor task

Use the Hotlist and permit editor task to edit a *hotlist* or parking *permit* list for all your patrol vehicles at the same time.

The following figure shows the Hotlist and permit editor task.



A	Find specific rows in your list.
B	Available hotlists and permits.
C	Selected row available for editing.
D	List of ALPR Managers.
E	Load the selected hotlist or permit list.
F	Add or delete the selected row from the list.
G	Save or cancel your changes.

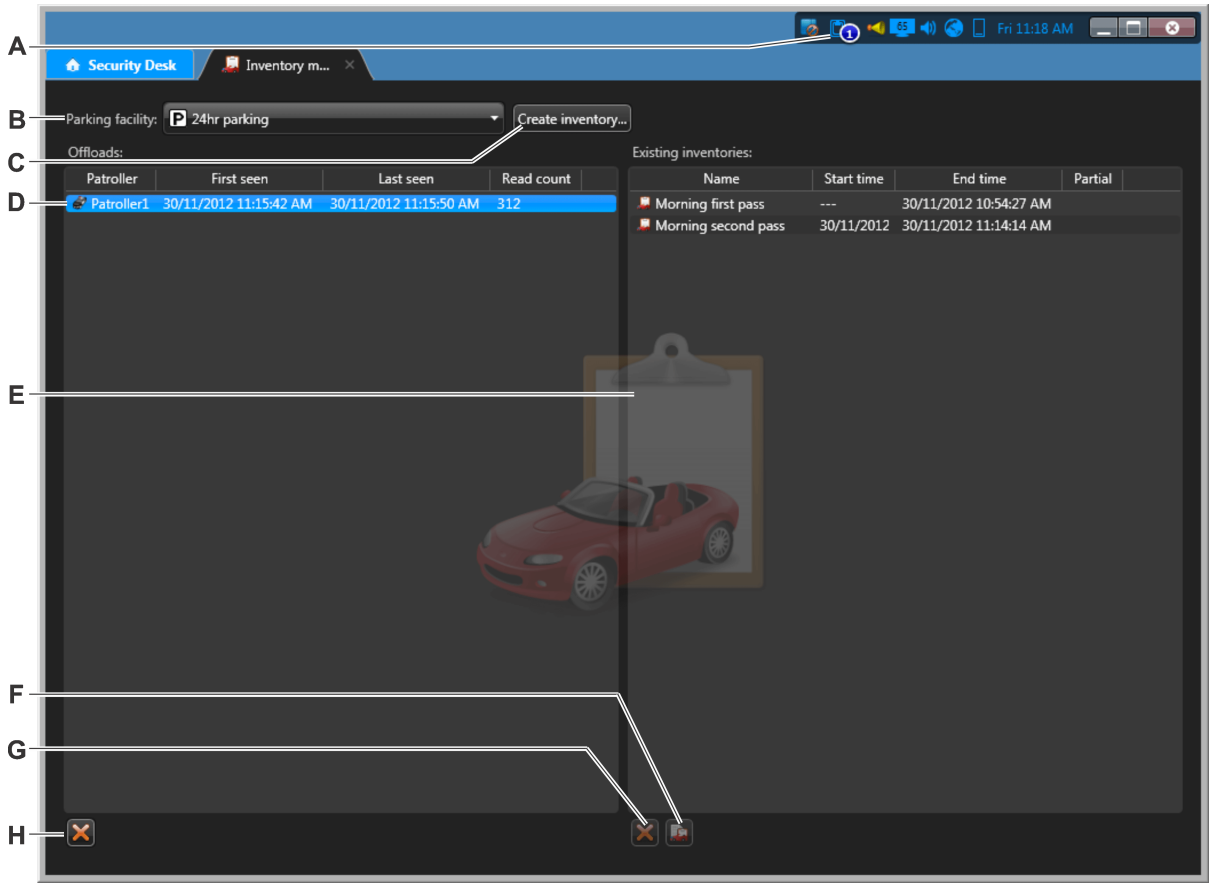
Related Topics

Editing hotlists and permit lists on page 395

Overview of the Inventory management task

Use the *Inventory management* task to add and reconcile MLPI license plate reads to a parking facility inventory.

The following figure shows the *Inventory management* task.



A	The Inventory icon displays the number of MLPI offload files waiting to be reconciled.
B	Parking facility selected to add the inventory to.
C	Create an inventory.
D	The *Offloads* section displays information about the MLPI offload. The file remains in the *Offloads* section until it is added or removed from the parking facility.
E	The *Existing inventories* section displays the inventories you created.
F	Open the *Inventory report* task to view and compare your parking facilities.
G	Delete the selected inventory.
H	Delete an offload file.

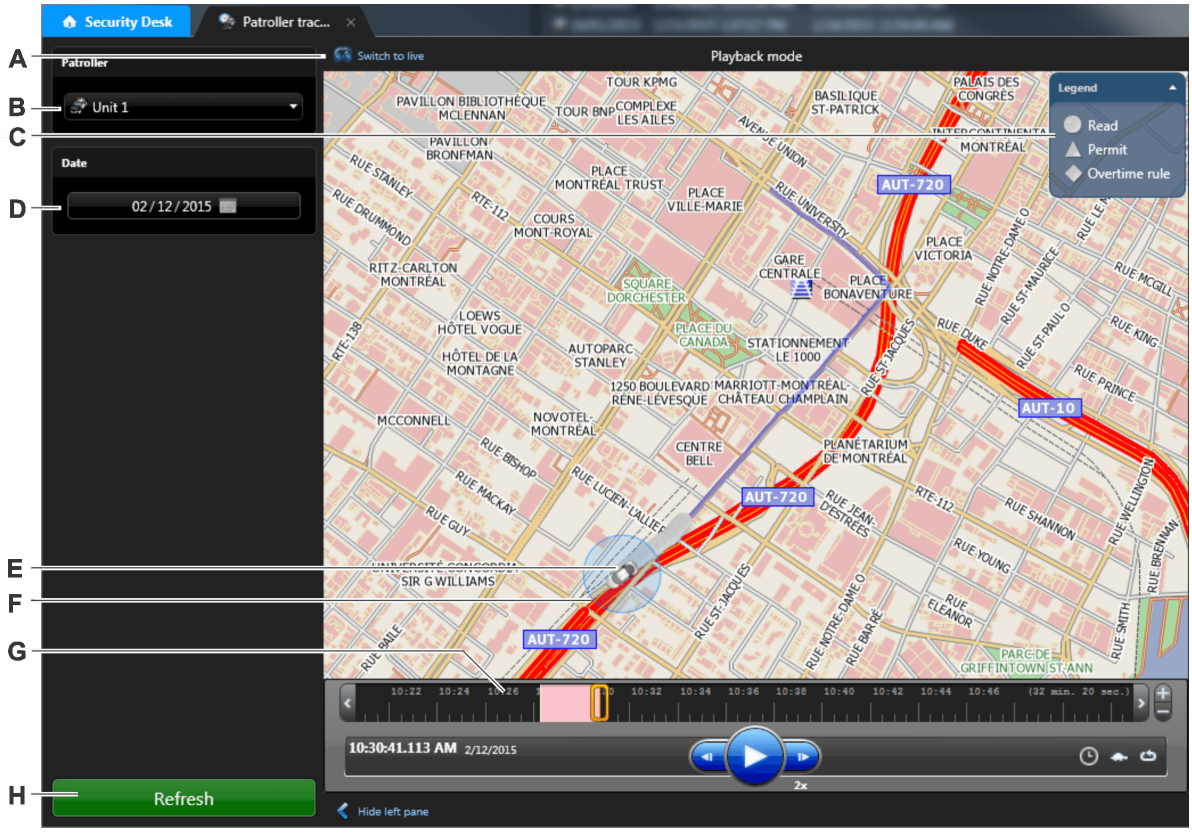
Related Topics

Creating parking facility inventories on page 455

Overview of the Patroller tracking task

Use the *Patroller tracking* task to replay the route taken by a patrol vehicle on a given date on a map, or track the patrol vehicle's live position on a map.

The following figure shows the *Patroller tracking* task.



A	Tracking mode. Click this to select the mode you want. **Playback mode** opens by default but you can click **Switch to live** to track the patrol vehicle's current position on the map.
B	Patrol vehicle you are investigating.
C	Map legend.
D	Date of the patrol vehicle route.
E	The car icon indicates the current patrol vehicle position, and the direction of the vehicle as it moves through the route.
F	The blue circle indicates the last ALPR read or hit that was played back in the timeline.
G	The patrol vehicle route and ALPR events are laid out in chronological order in the timeline ruler.
H	Refresh the screen and generate the Genetec Patroller™ route playback report.

Related Topics

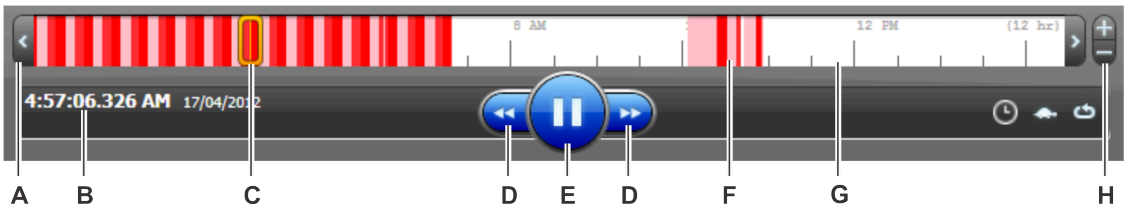
Replaying patrol vehicle routes on page 444

Monitoring ALPR events in map mode on page 389
Tracking the current location of a patrol vehicle on page 445

Genetec Patroller™ tracking timeline controls

Use the *Patrol vehicle tracking* task to replay the route taken by a patrol vehicle on a given date on a map.

Genetec Patroller™ tracking provides the following timeline controls in playback mode to help you navigate through the patrol vehicle route and locate ALPR events.



A	Scroll buttons	Move to another position in the timeline without moving the playback cursor.
B	Playback timestamp	Indicates the time and date of the Playback cursor location in the timeline.
C	Playback cursor	Indicates the current location in the Genetec Patroller™ route. To change the playback frame drag the cursor to the new position or click on the timeline.
D	Rewind/Forward buttons	During playback, the Rewind and Forward buttons appear to the left and right of the Play button. When you click Rewind or Forward, a speed control slider appears. Drag the slider to the right to fast forward (1x, 2x, 4x, 6x, 8x, 10x, 20x, 40x and 100x) or to the left for rewind (-1x, -4x, 10x, -20x, -40x or -100x). When the desired speed is set, release the mouse button. To return to normal speed (1x), click the Play/Pause button. **NOTE:** The map does not automatically center itself when playback is not running at normal speed.
E	Play/Pause	Switch between playing and pausing the route playback. You can also press the Spacebar.
F	Event markers	Light red vertical lines on the timeline ruler indicate read events. Dark red vertical lines on the timeline ruler indicate hit events. Clicking an event marker moves the view in the map to the location on the event.
G	White areas	White areas on the timeline ruler indicate a Genetec Patroller™ route sequence. Black areas indicate that no one is patrolling during that time. Purple areas indicate the future.
H	Zoom controls	Control the portion of playback sequence that appears in the timeline. Zoom in to the timeline to view the exact location of an ALPR event.
	Go to specific time	Open a browser window, and jump to a precise date and time in the recording.

	Slow motion	Play the Genetec Patroller™ route in slow motion. A speed control slider appears to the right of the Play/Pause button. Drag the double-arrow cursor along the slider to change the speed. Slow motion is available in the following speeds:1/8x, 1/4x, 1/3x, 1/2x and 1x. The default playback speed is 1/8x. **NOTE:** Slow motion rewind is not supported.
	Loop playback	Automatically restart the route sequence when it reaches the end of the sequence during playback.

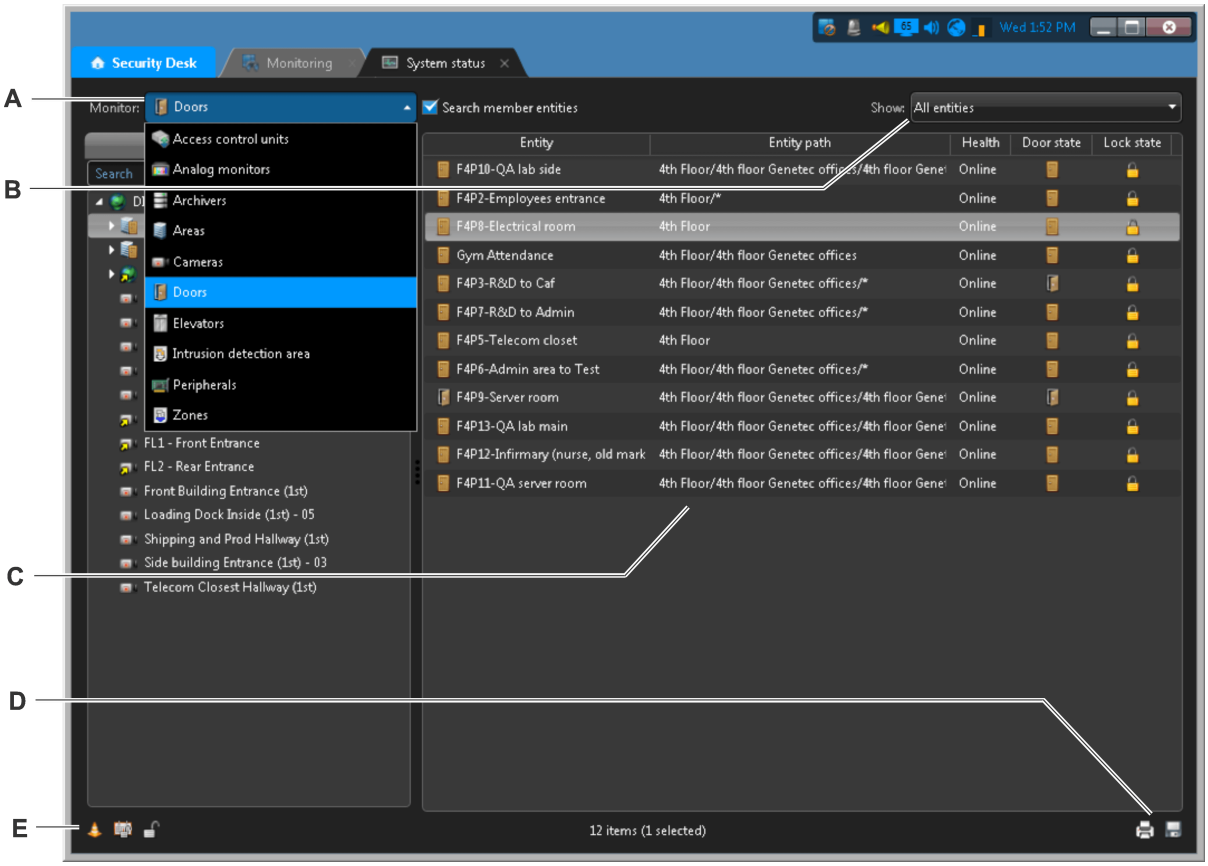
Related Topics

Replaying patrol vehicle routes on page 444
Tracking the current location of a patrol vehicle on page 445

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.



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

Monitoring the status of your Security Center system on page 511
Exporting generated reports on page 74
Printing generated reports on page 74

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** drop-down 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*
	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
	Servers	List of servers assigned to this role
	Active cameras	Number of cameras detected by the Archiver

Entity	Column	Description
	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*
	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
	Health	Online, Offline, or Warning
	Recording	Recording state
	Analog signal	Lost, Available, or Unknown (IP cameras)

Entity	Column	Description
	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*
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*
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
	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)

Entity	Column	Description
	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*
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
	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 ( )

Entity	Column	Description
	Maintenance	Indicates if the entity is in *maintenance mode*, and states the duration of the *maintenance mode*
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*
Video modules	Server	Server hosting the video analytics module
	Entity	Type of video analytics module
	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

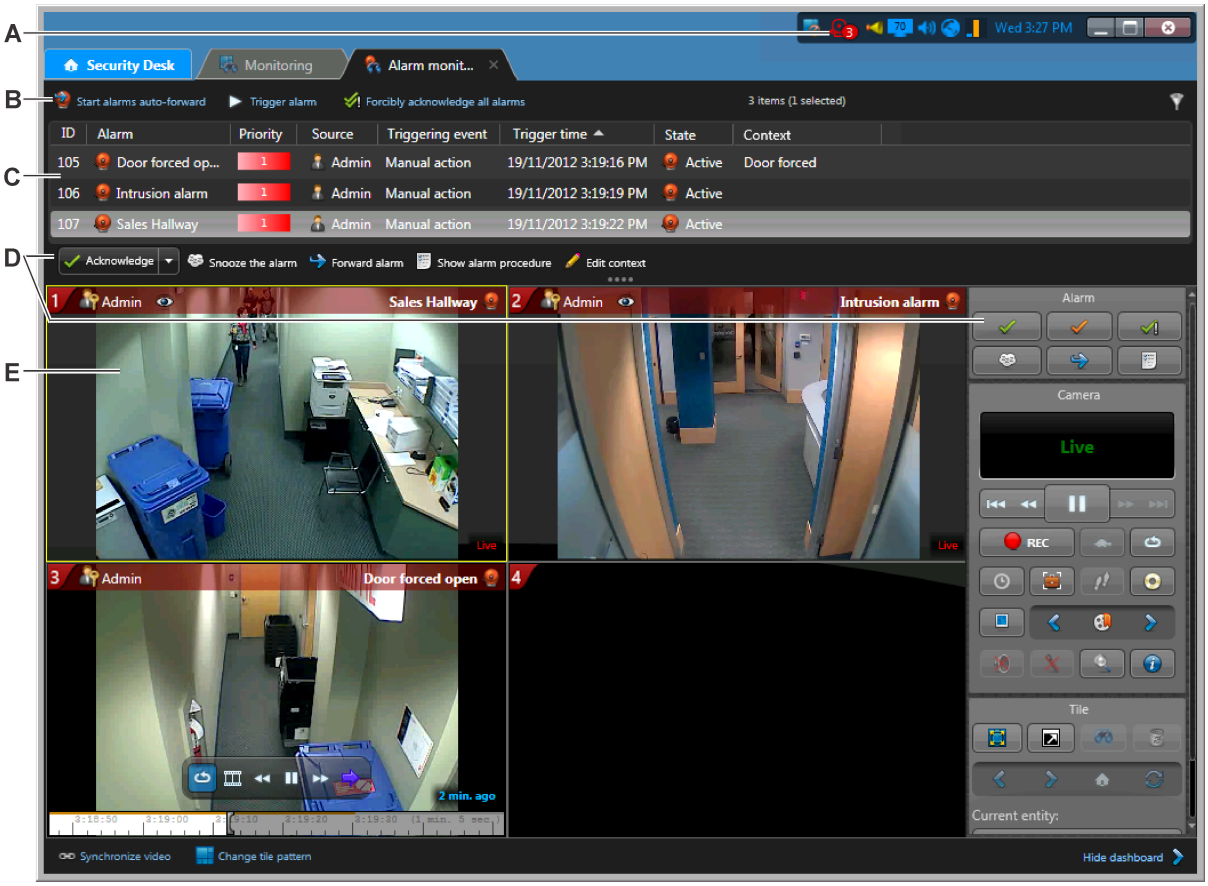
Entity	Column	Description
	Memory controller load	Current memory bandwidth usage on the graphics card (memory transfer between CPU and GPU)
	Last update	Last statistics update
Zones	Entity	Zone name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
	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*

* You can also monitor the I/O status of individual units from their *Peripherals* page in Config Tool.

Overview of the Alarm monitoring task

Use the *Alarm monitoring* task to monitor and respond to *active alarms* in real time, as well as review past alarms.

The following figure shows the *Alarm monitoring* task.



A	The alarm monitoring icon turns red when there is an active alarm. Double-click to open the *Alarm monitoring* task.
B	Additional alarm commands. • Start alarms auto-forward. • Trigger alarm. • Force acknowledge all alarms. • Set the alarm filter options.
C	Current alarms are listed in the alarm list. To change the columns that are shown, right-click a column heading, and then click **Select columns**. Right-click an alarm to go to the configuration page of the alarm or its source entity.
D	Commands to control active alarms. Click the **Acknowledge** drop-down list to see all available commands.
E	Video of an alarm in a tile. The video is displayed with a colored overlay with details of the alarm.

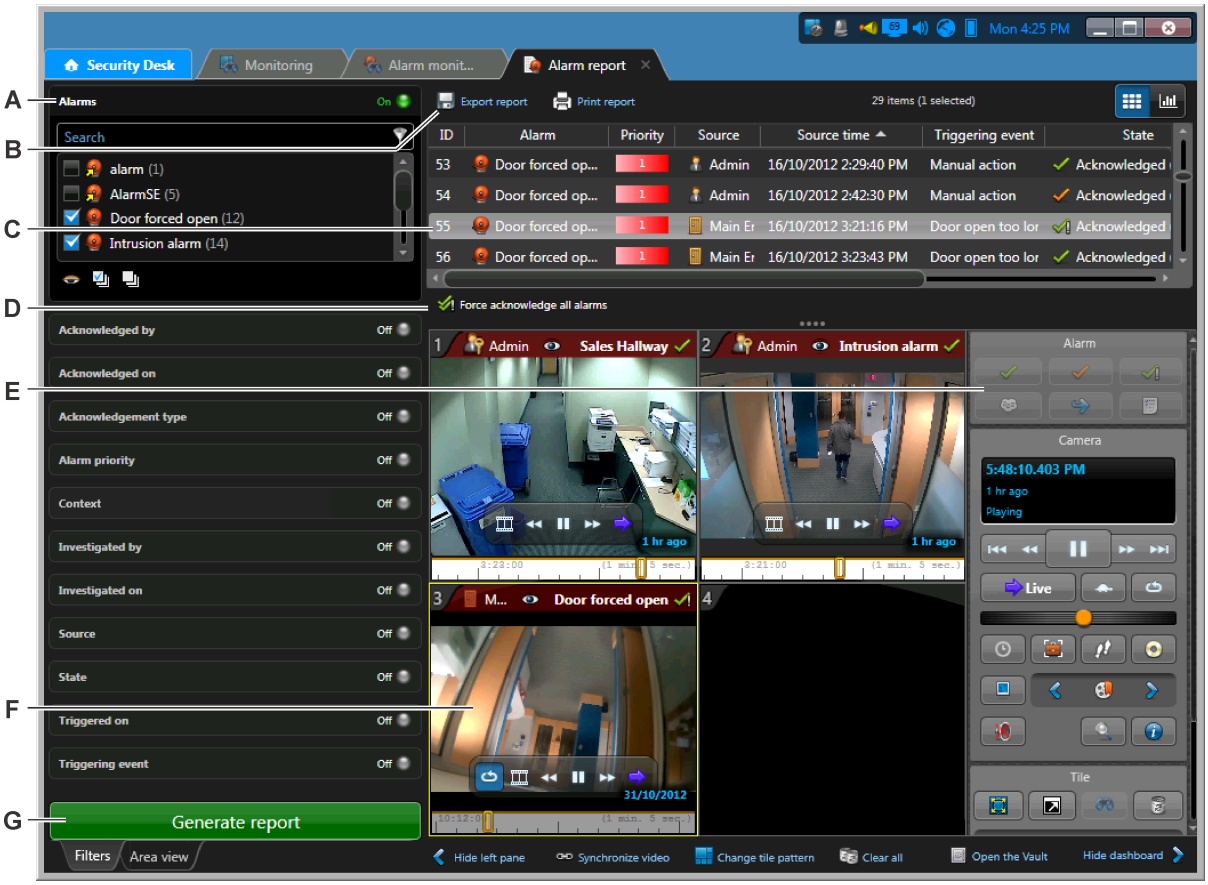
Related Topics

Acknowledging alarms on page 465

Overview of the Alarm report task

Use the *Alarm report* task to search for and investigate current and past alarms.

The following figure shows the *Alarm report* task.



A	Query filters.
B	Click to export or to print the report.
C	The alarm report results are listed in the report pane. Right-click an alarm to go to the configuration page of the alarm or its source entity.
D	Forcibly acknowledge all active alarms.
E	Alarm widget.
F	Video of an alarm in a tile.
G	Run the report.

Related Topics

Alarm widget on page 35
Exporting generated reports on page 74
Printing generated reports on page 74

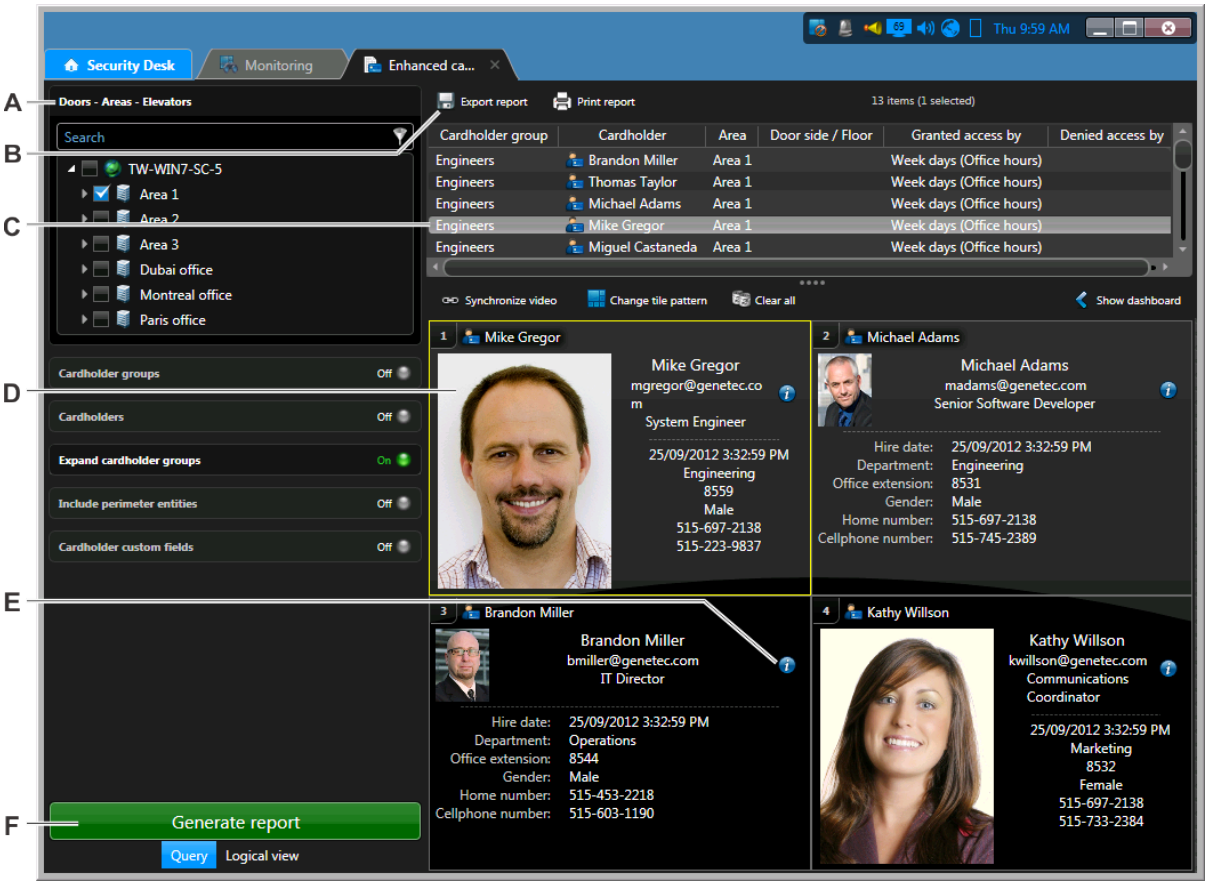
Investigating current and past alarms on page 474
How alarms are displayed in the Security Desk canvas on page 462

Overview of the Enhanced cardholder access rights task

You can find out which cardholders and cardholder groups are currently granted or denied access to selected areas, doors, and elevators, using the *Enhanced cardholder access rights* report.

This report is helpful, because it allows you to see where a cardholder can go, and when, and determine if their access rule properties need to be adjusted. You can also use this report to find members of a cardholder group.

TIP: Perform your query on one cardholder or cardholder group at a time, so your report is more specific.



A	Query filters. • **Cardholder groups:** Restict your search to specific cardholder groups. • **Cardholders:** Restrict your search to specific cardholders. • **Expand cardholder groups:** List the members of the selected cardholder groups in the report instead of the cardholder groups themselves. • **Include perimeter entities:** Include the perimeter entities of the selected areas in the report. • **Cardholder custom fields:** If custom fields are defined for the cardholders you are investigating, they can be included in this report.
B	Export or print the report.
C	All cardholders or cardholder groups that are granted or denied access at the selected areas and access points are listed in the report pane.
D	View cardholder properties in a tile.

E	- View additional cardholder details.
D	Run the report.

Related Topics

How cardholders are displayed in the Security Desk canvas on page 290

Enabling the Enhanced cardholder access rights task

To use the *Enhanced cardholder access rights* report, you must enable the report in Security Desk from the *SecurityDesk.plugins.xml* file.

To enable the Enhanced cardholder access rights task:

1. Open the *SecurityDesk.Modules.xml* file, located in *C:\Program files (x86)\Genetec Security Center 5.x* on a 64-bit computer, and in *C:\Program files\Genetec Security Center 5.x* on a 32-bit computer.
2. Set the **Genetec.AccessControl.Reporting.Casinos.dll** attribute to **true**.

   Example: <Report Assembly="Genetec.AccessControl.Reporting.Casinos.dll" Enabled="true" />
3. Save the XML file, and then restart Security Desk.

The next time you open Security Desk, the *Enhanced cardholder access rights* task is available.

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.
add-on	An add-on is a software package that adds tasks, tools, or specific configuration settings to Security Center systems.
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.
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 a user's response to an alarm. In Security Center, the default and the alternative

	acknowledgement are the two variants of alarm acknowledgements. 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	(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.
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.
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* 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*.
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.
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.
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.

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.

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™ 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.

AutoVu™ ALPR Processing Unit

AutoVu™ ALPR Processing Unit is the processing component of the SharpX system. The ALPR Processing Unit is available with two or four camera ports, with one dedicated processor per camera (if using SharpX) or per two cameras (if using SharpX VGA). This ensures maximum, per-camera, processing performance. The ALPR Processing Unit is sometimes referred to as the *trunk unit* because it is typically installed in a vehicle's trunk.

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.
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.
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)

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, A and B. A correlation exists between A and B if whenever event A occurs, event B is expected. For example, if whenever there is a large gathering of people, the number of new cases of COVID-19 increases in the following days, we can say that there is a correlation between large gatherings and the increase of the number of new cases of COVID-19.

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 Synergis™ 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. Only HID VertX interface modules can operate in degraded mode.
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	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.
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.
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 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 stored in Bosch units.
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™ Mobile	Official name of the map-based Security Center mobile application for Android and iOS devices.
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™ 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 media player that is used to view exported G64 and G64x video files from Security Desk, or on a computer that does not have Security Center 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.
georeferencing	Georeferencing is the process of using an object's geographic coordinates (latitude and longitude) to determine its position on a map.
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.
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 doors.

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.

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.

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.
Incidents	The *Incidents* task is an investigation task that you can use to search, review, and modify incident reports created by Security Desk users.
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).
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.
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 — The *long term* regulation is a parking regulation characterizing an overtime rule. This regulation uses the same principle as the *same position* regulation, but the parking period starts on one calendar date and ends on another calendar date. No more than one overtime rule can use the long term regulation in the entire system.

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.
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™, Genetec Mission Control™, or Record fusion, 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.
map view	A map view is a defined section of a 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.
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.
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*) .
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*.
Media Gateway	The Media Gateway role is used by Genetec™ Mobile and Web Client 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-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.
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.
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.
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.

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 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 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 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.
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.
patroller entity	A patroller entity in Security Center represents a patrol vehicle equipped with an in-vehicle computer running Genetec Patroller™ software.
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 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.

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 list. 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.

Plan Manager
(Obsolete) Plan Manager is a module of Security Center that provides interactive mapping functionality to better visualize your security environment. The Plan Manager module has been replaced by the Security Center role, Map Manager, since version 5.4 GA.

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 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.
Plugin	Plugin (with an uppercase, in singular) is the role template that serves to create specific plugin roles.
Plugins	The *Plugins* task is an administration task that you can use to configure plugin-specific roles and related entities.
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.
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.
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.
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)*.
Records	The *Records* task in an investigation task that you can use to query the *record providers* registered in Security Center and find relevant information based on known or suspected correlations.
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	The Reverse Tunnel role is used on the federated system to connect to the Federation™ host residing in the cloud. The connection is established using a keyfile generated from the cloud system. The keyfile can only be used once to ensure maximum security.
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.

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 and 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 any alternate server on standby intended to replace the primary server in the case the latter becomes unavailable.
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.
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).
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 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.

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.

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.

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.

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).

SharpV SharpV is a Sharp unit that is specialized for fixed installations and 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 (1.2MP) 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.
single sign-on	Single sign-on (SSO) is the use of a single user authentication for multiple IT systems or even organizations.
Software Development Kit	The Software Development Kit (SDK) is what end-users use to develop custom applications or custom application extensions for Security Center.
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.
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 SV 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	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 and PoE-enabled access control appliance of Genetec Inc. that supports a variety of third-party interface modules over IP and RS-485. Synergis™ Cloud Link is seamlessly integrated with Security Center and is capable of making access control decisions independently of the Access Manager.
Synergis™ Cloud Link clustering	Synergis™ Cloud Link clustering is a feature designed for large systems to optimize the way that cardholder synchronization is handled between Access Manager roles and Synergis™ Cloud Link units. When the feature is enabled, only active cardholders managed by the same Access Manager, based on access rules, are synchronized to the Synergis™ Cloud Link.
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 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	The *System* task is an administration task that you can use to configure roles, macros, schedules, and other system entities and settings.
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.
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 on supported video and access control 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 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	The *Video* task is an administration task that you can use to configure video management roles, units, analog monitors, and cameras.
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 Server	The Web Server role is used to configure Security Center Web Client, a web application that gives 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 Web Client and access information from Security Center.
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.
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.
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.

Additional resources

If you require additional resources other than the Genetec™ Technical Assistance Center, the following is available to you:

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss many topics, ranging from technical questions to technology tips. You can log on or sign up at https://gtapforum.genetec.com.
- **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.