Genetec™ Security Center.

Security Center Installation and Upgrade Guide 5.10.2.0

Click here for the most recent version of this document.

Document last updated: January 7, 2022

Genetec™

Legal notices

©2021 Genetec Inc. All rights reserved.

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

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

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

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

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

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

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

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

All specifications are subject to change without notice.

Document information

Document title: Security Center Installation and Upgrade Guide 5.10.2.0

Original document number: EN.500.002-V5.10.2.0(1)

Document number: EN.500.002-V5.10.2.0(1)

Document update date: January 7, 2022

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

About this guide

This guide explains how to install and upgrade Security Center components.

Notes and notices

The following notes and notices might appear in this guide:

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

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

Contents

Preface

Legal notices . . . ii
About this guide . . . iii

Chapter 1: Installing Security Center

Pre-installation checklist for Security Center . . . 2
Security Center 5.10.2.0 installation prerequisites . . . 4
Granting SQL Server permissions . . . 5
Activating the Media Foundation feature . . . 5
Security Center installation packages . . . 6
Reducing the package size for client installations . . . 7
Installing Security Center . . . 9
Ports used by core applications in Security Center . . . 9
Ports used by AutoVu™ applications in Security Center . . . 13
Ports used by Omnicast™ applications in Security Center . . . 15
Ports used by KiwiVision™ modules in Security Center . . . 23
Ports used by Synergis™ applications in Security Center . . . 25
Installing SQL Server independently of Security Center . . . 28
Installing the Security Center main server . . . 34
Activating Security Center license using the web . . . 46
Activating Security Center license manually . . . 49
Installing Security Center expansion servers . . . 54
Connecting expansion servers to the main server . . . 65
Installing Security Center Client Software . . . 68
Uninstalling Security Center . . . 76
Completing the installation process . . . 78

Chapter 2: Upgrading to Security Center 5.10

Supported upgrade paths to Security Center 5.10.2.0 . . . 82
Preparing to upgrade from an earlier release of Security Center 5.10 . . . 83
Upgrading from an earlier release of Security Center 5.10 . . . 84
Pre-upgrade checklist for upgrading from an earlier major version of Security Center . . . 85
Backward compatibility requirements for Security Center . . . 86
Backing up databases . . . 92
Backing up the Directory database . . . 92
Backing up role databases . . . 93
Upgrading Security Center 5.7, 5.8, or 5.9 to 5.10 . . . 95
Upgrading Security Center from 5.4, 5.5, or 5.6 to 5.10 . . . 96
Upgrading Directory failover systems from an earlier major version . . . 97
Reactivating Security Center license for Directory failover systems . . . 99
What Security Center client features are available when the Directory service is offline? . . . 104
Upgrading the Security Center main server . . . 105
Upgrading expansion servers in Security Center . . . 114
Upgrading Security Center Client . . . 118
Upgrading the Security Center Directory database . . . 119

Shrinking Security Center databases after an upgrade 120
Upgrading Security Center with Global Cardholder Synchronizer roles 122

Chapter 3: Automating Security Center installation

Silent installation of Security Center 124
Preparing to perform a silent installation 125
Silent installation options for Security Center 126
Security Center options 128
Sample Security Center Server installation commands 133
Sample Security Center Client installation commands 135
Uninstalling Security Center 5.10 in silent mode 136
Silent installation options for Security Center SDK 137

Chapter 4: Troubleshooting

Disabling the SQL Server telemetry service manually 139
Cameras stop working after installing Security Center with the default security options 140
Error when installing Microsoft .NET Framework, Return Code: 0x800f081f 141
Video stability and performance issues 142
Files remain blocked after unblocking them manually 143
One or more services failed to install 144

Glossary 146

Where to find product information 197
Technical support 198

1

Installing Security Center

This section includes the following topics:

- "Pre-installation checklist for Security Center" on page 2
- "Installing Security Center" on page 9
- "Installing SQL Server independently of Security Center" on page 28
- "Installing the Security Center main server" on page 34
- "Activating Security Center license using the web" on page 46
- "Activating Security Center license manually" on page 49
- "Installing Security Center expansion servers" on page 54
- "Installing Security Center Client Software" on page 68
- "Uninstalling Security Center" on page 76
- "Completing the installation process" on page 78

Pre-installation checklist for Security Center

To make sure that your Security Center installation goes smoothly, you must perform a series of pre-configuration steps.

CAUTION: Do not use the image of a configured machine to install Security Center Server on similar machines. Security Center installer creates unique IDs when it runs for the first time on a machine. These IDs are stored in configuration files and the Directory database. If these IDs are duplicated, it causes conflicts with the entities in the system that share the identifiers. This might make the system unusable.

Step	Task	Additional information
Review your system compatibility		
1	Read the release notes for any known issues, limitations, and other information about the release.	• *Security Center Release Notes*.
2	Review the system requirements to ensure that the minimum hardware (servers and workstations) and software requirements (Windows, web browser, and so on) are met.	• *Security Center System Requirements Guide*.
3	Read the installation prerequisites for your release. Security Center Installer automatically verifies and installs the software prerequisites on your system, but it is a good practice to know what they are beforehand.	• Security Center 5.10.2.0 installation prerequisites.
4	Read the best practices for configuring Windows to work with Security Center. To ensure the optimal performance of your system, you must follow these recommendations after installing Security Center	• Best practices for configuring Windows Firewall to work with Security Center. • If you are running Windows 8.1 or Windows Server 2012 R2, you must install Microsoft update 2919355 followed by 2999226.
Review your system components		
5	Create a list of the computers that will be part of your new system, and decide what software components need to be installed on each. **IMPORTANT:** Server names must be 15 characters or fewer. Security Center truncates all server names longer than 15 characters, causing errors when the system tries to access those servers.	Your system requires the following components: • Security Center Server (main or expansion server) • Security Center Client (Config Tool, Security Desk, or both) • SQL Server (Express, Standard, or Enterprise edition)
6	If you plan to use restricted cameras, do the following: 1. Contact your sales representative to obtain a special connection license for your restricted camera connections. 2. Sign the “Exclusion of Liability and Hold Harmless” waiver.	Cameras developed by some manufacturers have been restricted due to a higher cybersecurity risk profile. These cameras require a special connection license, in addition to the normal camera license. To view a list of manufacturers that require a restricted license, use the **Restricted** *License Type* filter on the Supported Device List.

Step	Task	Additional information
Verify your network connections		
7	Verify the network connections between your servers, workstations, and units.	Make sure that the ports required by Security Center are open and redirected for firewall and NAT purposes.
8	Verify the unicast and multicast network connections and settings.	Security Center does not modify your network infrastructure or how it works. Multicast works with Security Center out of the box automatically, as long as the network supports the necessary load. If multicast is the only protocol configured, Security Center will not switch to a different protocol if multicast is blocked, and video will not get recorded.
Verify your user permissions		
9	Make sure you have administrative privileges. If not, run the installation *setup.exe* as administrator.	You might need to be a Microsoft Windows Domain administrator to access databases and storage on the machines. Check with your IT administrator.
10	Grant the service users all necessary SQL Server permissions.	• Granting SQL Server permissions on page 5.
Set up additional software as needed		
11	If you are implementing role failover or VSS operation, install SQL Server yourself.	• Installing SQL Server independently of Security Center on page 28.
12	If you are running Windows Server 2012 or Windows Server 2016, activate the Media Foundation feature.	• Activating the Media Foundation feature on page 5.
Prepare your installation package		
13	Download the Security Center installation package.	• Security Center installation packages on page 6. • If you only want to install client applications, you can ease the download and distribution of Security Center to your remote sites by reducing the size of the installation package.
14	Unblock any blocked files.	• Unlocking downloaded files to avoid security warnings. • After downloading the Security Center installation package, compressed files might need to be unblocked before their contents are extracted.

Step	Task	Additional information
15	Have your system ID and password in hand to activate your license on the main server.	Your System ID and password are found in the *Security Center License Information* document. Genetec™ Inside Sales or Genetec™ Customer Service sends you this document when you purchase the product.
16	Install Security Center.	• Installing Security Center on page 9.

Security Center 5.10.2.0 installation prerequisites

The prerequisites for a successful Security Center installation are found in the Security Center installation package, in the *SC Packages* folder, in separate subfolders.

	32-bit Client	32-bit Server	64-bit Client	64-bit Server
ArcGIS Runtime 100	✓	✓	✓	✓
DirectX End-User Runtimes	✓	✓	✓	✓
Microsoft .NET Framework 4.8 Full	✓	✓	✓	✓
Microsoft CCR and DSS Runtime 2008 R2 Redistributable	✓	✓	✓	✓
Microsoft CCR and DSS Runtime 2008 R3 Redistributable	✓	✓	✓	✓
Microsoft Primary Interoperability Assemblies 2005[a]	✓	✓	✓	✓
Microsoft Report Viewer 2012	✓	✓	✓	✓
Microsoft SQL Server Management Studio - 18.5.1				✓
Microsoft System CLR Types for SQL Server 2014 v12.0.2402.11	✓	✓	✓	✓
Microsoft System CLR Types for SQL Server 2014 v12.0.2402.11 (x64)			✓	✓
Microsoft System CLR Types for SQL Server 2019 v.15.0.2000.5			✓	✓
Microsoft Visual C++ 2010 RTM Redistributable 10.0.30319.415	✓	✓	✓	✓
Microsoft Visual C++ 2010 SP1 Redistributable Package (x64)			✓	✓
Microsoft Visual C++ 2012 Update 4 Redistributable Package (x86)	✓	✓	✓	✓
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40660.0	✓	✓	✓	✓
Microsoft Visual C++ 2019 14.22.27821.0 Redistributable (x86)	✓	✓	✓	✓
Microsoft Visual C++ 2019 14.22.27821.0 Redistributable (x64)			✓	✓

	32-bit Client	32-bit Server	64-bit Client	64-bit Server
MSMQ 3.0 and up[b] (Windows Feature)	✓	✓	✓	✓
WinPcap 4.1.3[c]	✓	✓	✓	✓

[a] Only required if you are installing Omnicast™ Compatibility Packs.

[b] MSMQ version dependent on the system's version of Windows.

[c] Not mandatory.

Granting SQL Server permissions

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

What you should know

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

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

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

To grant SQL Server permissions:

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

After you finish

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

Activating the Media Foundation feature

If you want to install Security Center on a computer running Windows Server 2012, you have to manually activate the Media Foundation feature. It is not necessary for Windows Server 2016, but it is faster to activate the feature manually than to let the installer do it for you.

To activate the Media Foundation feature:

1 Open *Server Manager* and click **Add roles and features**.
2 If the **Before you begin** page is displayed, click **Next**.
3 Select **Role-based or feature-based installation** as the installation type and click **Next**.
4 Select the appropriate server, and click **Next**.

5 On the *Select server roles* page, click **Next**.
6 On the *Select features* page, select **Media Foundation** and click **Next** > **Install**.
7 Select the option **Restart the destination server automatically if required** for the server to automatically restart and apply changes after completing the installation.

Security Center installation packages

The Security Center installation packages contain the setup program that helps you to install everything you need to get the product working.

Downloadable packages

The Security Center installation packages are zip files that you can download from the GTAP *Product Download* page, at https://portal.genetec.com/support/SystemManagement/DownloadSection/. Note, you'll need a username and password to log on to GTAP.

- **SecurityCenterWebSetup.exe:** This is the web installer. The web installer is a small installation wizard that does not contain software packages. To retrieve the required software packages, the wizard connects to Genetec™ servers and downloads the components necessary for the features you choose to install.
- **Full installation package:** Download the full installation package if your computers do not have access to the Internet. This is a standalone package. You don't need anything else outside this package.

  The full installation package contains the following:

  - **setup.exe:** Found in the root folder, this is the AutoRun-enabled version of the standalone installer.
  - **Security Center Setup.exe:** Found in the *SC Packages* folder, this is the standalone installer.
  - **SC Packages:** This folder contains all the components (in separate subfolders) that you might need for your Security Center installation. All the Security Center installation prerequisites are found here.
  - **Documentation:** This folder contains the PDF versions of the *Security Center Installation and Upgrade Guide* along with the *Release Notes*.
- **Separate component installation packages:** The following installation packages are bundled in the full Security Center installation package, but can also be run separately.
  - **Security Center 5.10 Documentation:** This package is required to install the Security Center help (*.exe* files), accessible from Security Desk and Config Tool through the F1 button, and the *Security Center Hardening Guide* (PDF file) locally on your computer.
    - Every new version of Security Center comes with the latest documentation at the time of release.
    - The latest version of the documentation can be deployed using the Genetec™ Update Service.
    - Updated documentation can become available after the software is released to add new translations or to fix documentation bugs.
  - **Security Center Drivers 10.x.y:** This package is required to integrate video devices to Security Center.
    - Every new version of Security Center comes with the latest drivers at the time of release.
    - The latest version of the Drivers package can be deployed using the Genetec™ Update Service.
    - If you accidentally remove the Drivers package from *Programs and Features*, your video units will stop working and turn red in Config Tool. To reinstall it, execute *Genetec Security Center Drivers 10.x.y.msi* located in the *SC Packages* folder of your full Security Center installation package.
    - We do not recommend installing a Drivers package older than the one bundled with the Security Center package.
  - **Security Center 5.10.x.y SDK:** Use this package to install the Platform SDK and the Media SDK on computers where Security Center is not installed. If you want to install the Macro SDK, the Security Desk SDK, or the Web SDK, use the full installation package, because these SDKs require the Security Center core components. To learn more on the Security Center SDK, see the Security Center SDK Help on TechDoc Hub.

Installation modes

You can run the Security Center Installer in two modes:

- **Wizard mode:** The InstallShield Wizard for Security Center Installer is a user friendly interface that guides you through the installation steps through a series of questions and runs the installer for you with the options you selected. There are two versions of the installer:
  - **Web version:** Run the web version of the installer if your computer is connected to the Internet. To run the web installer, download the file *SecurityCenterWebSetup.exe* from GTAP and double-click it.
    At the beginning of the installation, you have the option to create a custom installation bundle that includes only the components that you need for your installation. This bundle is meant to replicate the current installation on computers with the same Windows setup.
    NOTE: To create the custom installation bundle, you must select this option while you are installing or upgrading Security Center. After the version you want has been installed, you cannot re-run the web setup to create the custom bundle.
  - **Standalone version:** Run the standalone version of the installer if your computer is not connected to the Internet. To run the standalone installer, download the full installation package from GTAP, copy the package to the target computer, and double-click *setup.exe* found in the root folder of the package.
- **Silent mode:** The silent mode is used to run the installer from the command line, without user intervention.

IMPORTANT: The Security Center Installer does not support using mapped drives in your path specifications.

Installer languages

The Security Center Installer is available in English and French, but the Security Center software can be installed in more than twenty different languages. The installer language is selected from the Security Center Installation startup screen.

Related Topics

Silent installation of Security Center on page 124

Reducing the package size for client installations

To ease the download and distribution of Security Center to your remote sites, you can greatly reduce the size of the installation package if you only want to install client applications.

What you should know

The full standalone Security Center installation package is roughly 4.6 GB. If you only need to install the client applications, Security Desk and Config Tool, you can eliminate the prerequisites that are only required for server installations, and reduce the size of the installation package by more than half.

TIP: You can use the web installer to create a custom installation bundle with only the components you need based on a first installation. However, the custom bundle can only be used to replicate the same installation on machines that have the same Windows setup as your first machine. If you plan on installing client applications on machines with different Windows setup, you must follow the current procedure.

To reduce the size of the installation package for client installations:

1 Download a copy of the full installation package from Genetec™ Portal (GTAP).

2 Unzip the package to a temporary folder.

3 Delete the *Documentation* folder.

This folder contains the *Security Center Installation and Upgrade Guide* and *Release Notes* in PDF format in multiple languages. You save roughly 21 MB.

TIP: If you need these documents later, you can download them individually from TechDoc Hub.

4 Open the *SC Packages* folder.

5 Delete the *SQLExpress* folder.

A client only installation does not require Microsoft SQL Server Express Edition. You save roughly 2.20 GB.

6 If you do not have an Omnicast™ Federation™, delete the Omnicast™ compatibility packs.

- *Genetec Omnicast 4.6 Compatibility Package* (~59 MB)
- *Genetec Omnicast 4.7 Compatibility Package* (~96 MB)
- *Genetec Omnicast 4.8 Compatibility Package* (~124 MB)

If no compatibility pack is required, then delete also *Microsoft Primary Interoperability Assemblies 2005*. Your save a total of roughly 280 MB.

7 If you do not need Genetec™ Video Player, delete the *Genetec Video Player* folder.

You save roughly 606 MB. If you need it later, you can download it separately from GTAP.

After you finish

Use the reduced package to install Security Center Client on other machines. Use the following sample silent installation commands:

- Install all client applications with Genetec™ Video Player:

```
"Security Center Setup.exe" /silent /language:1033 /ISFeatureInstall=Client /
debuglog"C:\DebugLog.log" /log"C:\" AGREETOLICENSE=Yes
```

- Install all client applications without Genetec™ Video Player:

```
"Security Center Setup.exe" /silent /language:1033 /ISFeatureInstall=Client /
debuglog"C:\DebugLog.log" /log"C:\" AGREETOLICENSE=Yes INSTALL_GVP=0
```

- Install Security Desk only with Genetec™ Video Player:

```
"Security Center Setup.exe" /silent /language:1033 /ISFeatureInstall=SecurityDesk /
debuglog"C:\DebugLog.log" /log"C:\" AGREETOLICENSE=Yes
```

Related Topics

Silent installation of Security Center on page 124

Installing Security Center

When you are ready to install Security Center, you must perform the following steps.

Before you begin

Go through the pre-installation checklist.

What you should know

IMPORTANT:

- If you need to install the Security Center Server on a computer after you have installed Security Center Client, always use the downloaded Security Center package. Using the *Change* option from *Programs and Features* does not install the SQL Server Express component.
- The Security Center Installer does not support the use of mapped drives in your path specifications.
- During the Security Center installation, you are given the option of allowing Security Center to create firewall rules for its applications. If you select this option, all Security Center applications are added as exceptions to the internal Windows firewall. However, you still must ensure that all the ports used by Security Center are open on your network.
- You can configure different port numbers than the ones that are used by default.
- If you are running Security Center 5.8 GA or earlier on a Windows machine that has *Federal Information Processing Standard (FIPS)* mode enabled, following the installation you must disable the machine's FIPS compliance checks for Security Center.

To install Security Center:

1. (Optional) Install SQL Server separately from Security Center.

   SQL Server Express is typically installed automatically with Security Center. Installing SQL Server separately depends on your deployment requirements.
2. Install Security Center components on the main server that will host the Directory role.
3. Activate your product license on the main server.
4. Make sure that all ports used by Security Center are open and redirected for firewall and network address translation purposes.
5. Configure Genetec™ Update Service (GUS).

   For more information, see the *Genetec™ Update Service User Guide*.
6. (Optional) Install Security Center components on expansion servers that will connect to the main server to add processing power to your Security Center system.
7. Install Security Center Client (Config Tool, Security Desk, or both).

After you finish

Go through the post-installation checklist.

Ports used by core applications in Security Center

The following table lists the default network ports that must be opened to allow proper communication between the core applications and services in Security Center.

For a visual representation of the ports, see the Security Center Network Diagram - Platform.

IMPORTANT: Exposing Security Center to the Internet is strongly discouraged without hardening your system first. Before exposing your system, implement the advanced security level described in the *Security Center Hardening Guide* to help protect your system from Internet threats. Alternatively, use a trusted VPN for remote connections.

Port usage	Inbound port	Outbound port	Protocol	Executable file
Directory				
Client and server connections	TCP 5500	TCP 5500	TLS 1.2	GenetecServer.exe
Config Tool				
Genetec™ Server/Directory communication		TCP 5500	TLS 1.2	GenetecServer.exe
Map download requests to Map Manager		TCP 8012	HTTPS	GenetecMapManager.exe
• Authentication role communication • Secured communication with the portal of the mobile credential provider • Communication with GTAP for Genetec™ Advantage validation and feedback		TCP 443	HTTPS TLS 1.2	ConfigTool.exe
Security Desk				
Genetec™ Server/Directory communication		TCP 5500	TLS 1.2	GenetecServer.exe
Map download requests to Map Manager		TCP 8012	HTTPS	GenetecMapManager.exe
• Authentication role communication • Secured communication with the portal of the mobile credential provider		TCP 443	HTTPS TLS 1.2	SecurityDesk.exe
SDK				
Genetec™ Server/Directory communication		TCP 5500	TLS 1.2	GenetecServer.exe
Map download requests to Map Manager		TCP 8012	HTTPS	GenetecMapManager.exe
All roles				

Port usage	Inbound port	Outbound port	Protocol	Executable file
Genetec™ Server/Directory communication **NOTE:** Previously port 4502. If port 4502 was the server port before upgrading from 5.3 or earlier, 4502 remains the server port after the upgrade.	TCP 5500	TCP 5500	Genetec Inc. proprietary protocol	GenetecServer.exe
REST/Server Admin communication[1]	TCP 80	TCP 80	HTTP	GenetecInterface.exe
Secured REST/Server Admin/Authentication role communication[1]	TCP 443	TCP 443	HTTPS	GenetecInterface.exe
Outgoing connections to the SQL Database Engine hosted on another server. Only required for roles that must connect to a database on another server. Not required if SQL Server is running on the same machine or if the role has no database.		TCP 1433	Microsoft Tabular Data Stream Protocol (TDS)	Role-dependent
Outgoing connections to the SQL Server Browser service for SQL Server connection information. Only required for roles that must connect to a named database instance on another server. Not required for roles configured to connect to their database using a specific port.		UDP 1434	Microsoft SQL Server Resolution Protocol (SSRP)	Role-dependent
Map Manager				
Requests for map download from client applications[1]	TCP 8012		HTTPS	GenetecMapManager.exe
Mobile Server				
Communication from mobile clients	TCP 443		HTTPS	GenetecMobileRole.exe GenetecMobileAgent.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Communication from Archiver for video streaming and storage	TCP 9000-10000		HTTP	GenetecMobileRole.exe GenetecMobileAgent.exe
Record Caching Service				
REST/Server Admin communication[1]	TCP 80	TCP 80	HTTP	GenetecIngestion.exe
Secured REST/Server Admin/Authentication role communication[1]	TCP 443	TCP 443	HTTPS	GenetecIngestion.exe
Unit Assistant				
Communication with Archiver roles	TCP 5500	TCP 5500	Genetec Inc. proprietary protocol	GenetecUnitAssistantRole.exe
Wearable Camera Manager				
Configurable in the UI		TCP 48830	Genetec Clearance™ protocol	GenetecBwcManagerRole.exe
Configurable in a config file		TCP 48831, 48832, 48833	Genetec Clearance™ protocol	GenetecBwcAgentService.exe
Web Server				
Initial connection between server hosting Web Server role and browser used for Web Client **NOTE:** Redirected to HTTPS port after initial connection.	TCP 80	TCP 80	HTTP	GenetecWebClient.exe
• Secured REST/Server Admin/Authentication role communication[1] • Connection between server hosting Web Server role and browser used for Web Client	TCP 443	TCP 443	HTTPS	GenetecWebClient.exe
Video requests to Media Gateway		TCP 443	HTTPS	GenetecWebClient.exe
Genetec™ Update Service (GUS)				

Port usage	Inbound port	Outbound port	Protocol	Executable file
Deprecated. Formerly used to access the GUS web page. Redirects to TCP 4595 in the latest GUS version[1]	TCP 4594		N/A	GenetecUpdateService.exe
Secure communication with the GUS web page, and other GUS servers[1]	TCP 4595	TCP 4595	HTTPS	GenetecUpdateService.exe
Communication with Azure and Genetec Inc.[1]	TCP 443	TCP 443	HTTPS	GenetecUpdateService.exe
SQL Server				
Incoming connections to the SQL Database Engine from roles on other servers	TCP 1433		Microsoft Tabular Data Stream Protocol (TDS)	sqlservr.exe
Incoming connections to the SQL Server Browser service for SQL Server connection information	UDP 1434		Microsoft SQL Server Resolution Protocol (SSRP)	sqlbrowser.exe
System Availability Monitor Agent (SAMA)				
Legacy port for communication with Security Center servers[1]		TCP 4592	HTTP	Genetec.HealthMonitor.Agent.exe
Communication with Security Center servers[1]		TCP 443	HTTPS	Genetec.HealthMonitor.Agent.exe
Connection to the Health Service in the Cloud[1]		TCP 443	HTTPS	Genetec.HealthMonitor.Agent.exe

[1] These ports use Windows System components to handle HTTP requests. Microsoft components using http.sys require the following rule: *dir="in" protocol="6" lport="<SPECIFY PORT USED HERE: CAN BE 80, 443, or CUSTOM>" binary="System"*.

Ports used by AutoVu™ applications in Security Center

The following tables lists the default network ports that must be opened to allow proper communication between Security Center and external AutoVu™ components when AutoVu™ is enabled in your system.

For a visual representation of the ports, see the Security Center Network Diagram - ALPR.

IMPORTANT: Exposing Security Center to the Internet is strongly discouraged without hardening your system first. Before exposing your system, implement the advanced security level described in the *Security Center Hardening Guide* to help protect your system from Internet threats. Alternatively, use a trusted VPN for remote connections.

Port usage	Inbound port	Outbound port	Protocol	Executable file
ALPR Manager				
Secure communication port for DataExporter		TCP 443	HTTPS	GenetecLicensePlate Manager.exe
Fixed Sharp unit discovery		UDP 5000	N/A	GenetecLicensePlate Manager.exe
Sharp control port (used for **Live** connections, not **LPM protocol** connections).		TCP 8001	HTTP	GenetecLicensePlate Manager.exe
Genetec Patroller™ communication and fixed Sharp units (not used for **LPM protocol** connections)	TCP 8731		HTTP	GenetecLicensePlate Manager.exe
LPM protocol listening port	TCP 10001		HTTPS	GenetecLicensePlate Manager.exe
Communication with Pay-by-Plate Sync plugin		TCP 8787	HTTP	GenetecLicensePlate Manager.exe
		TCP 8788	HTTPS	GenetecLicensePlate Manager.exe
Sharp unit (Plate Reader and Portal Server)				
Communication port (HTTP for SharpOS 12.7 and earlier)	TCP 80		HTTP	Sharp unit
Secure communication port for Web Portal, Sharp unit API, and MJPEG video streaming	TCP 443		HTTPS	Sharp unit
H.264 video streaming	TCP 554 UDP 554		RTSP	Sharp unit
Silverlight ports and image feed service (for Sharp models earlier than SharpV)	TCP 4502-4534		HTTP	Sharp unit
Control port (Mobile installation)	TCP 4545		HTTP	Sharp unit
Discovery port	UDP 5000		UDP	Sharp unit
Control port (Fixed installation)	TCP 8001		HTTP	Sharp unit
Sharp read events		TCP 8731	HTTP	Sharp unit

Port usage	Inbound port	Outbound port	Protocol	Executable file
LPM protocol communication port		TCP 10001	HTTPS	Sharp unit
FTP file upload. Only used when FTP extension is configured		TCP 21	FTP	Sharp unit
Genetec Patroller™ (in-vehicle computer)				
Communication with AutoVu™ cloud services		TCP 443	HTTPS	Patroller.exe
Communication with mobile Sharp units	TCP 4545	TCP 4545	HTTP	Patroller.exe
Time synchronization service for Sharp units	TCP 4546		SNTP	Patroller.exe
Sharp camera discovery		UDP 5000	UDP	Patroller.exe PatrollerConfigTool.exe
Communication with Simple Host	TCP 8001		HTTP	Patroller.exe
Communication with Pay-by-Plate Sync plugin	TCP 8787		HTTP	Patroller.exe
ALPR Manager connection		TCP 8731	HTTP and message-level encryption	Patroller.exe
Pay-by-Plate Sync				
Communication with AutoVu™ Free-Flow and Genetec Patroller™	TCP 8787		HTTP	GenetecPlugin.exe for Pay-by-Plate Sync
Secure communication with AutoVu™ Free-Flow	TCP 8788		HTTPS	GenetecPlugin.exe for Pay-by-Plate Sync

Ports used by Omnicast™ applications in Security Center

The following table lists the default network ports that must be opened to allow proper communication between Security Center and external IP video devices when Omnicast™ is enabled in your system.

For a visual representation of the ports, see the Security Center Network Diagram - Video.

IMPORTANT: Exposing Security Center to the Internet is strongly discouraged without hardening your system first. Before exposing your system, implement the advanced security level described in the *Security Center Hardening Guide* to help protect your system from Internet threats. Alternatively, use a trusted VPN for remote connections.

Port usage	Inbound port	Outbound port	Protocol	Executable file
Archiver				
Communication with Cloud storage		TCP 80[4], 443[4]	HTTPS TLS 1.2	GenetecArchiverAgent32.exe
Communication between the Archiver and the Media Router to announce content		TCP 554	RTSP over TLS when secure communication enabled	GenetecArchiverAgent32.exe
Live and playback stream requests	TCP 555[1]		RTSP over TLS when secure communication enabled	GenetecArchiverAgent32.exe
Edge playback stream requests	TCP 605[1]		RTSP	GenetecVideoUnit Control32.exe
Mobile device streaming through the Mobile Server		TCP 9000-10000	HTTP	GenetecVideoUnit Control32.exe
Communication between the primary Archiver and failover servers	TCP 5500	TCP 5500	TLS 1.2	GenetecArchiver.exe GenetecArchiverAgent32.exe GenetecVideoUnit Control32.exe
Telnet console connection requests	TCP 5602[1]		Telnet	GenetecArchiverAgent32.exe
Audio from client applications	UDP 6000-6500		RTP	GenetecVideoUnit Control32.exe
Live unicast streaming from IP cameras	UDP 15000–19999[2]		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecVideoUnit Control32.exe
Live video and audio multicast streaming	UDP 47806, 47807	UDP 47806, 47807	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecArchiverAgent32.exe GenetecVideoUnit Control32.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Vendor-specific ports for cameras	TCP & UDP	TCP Common ports include: • TCP 80 • TCP 443 • TCP 554 • TCP 322	• TCP 80: HTTP • TCP 443: HTTPS • TCP 554: RTSP • TCP 322: RTSP over TLS when secure communication enabled	GenetecVideoUnitControl32.exe
Redirector				
Live and playback stream requests	TCP 560		RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Communication with Media Router (Security Center Federation™)		TCP 554	RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Communication with Archiver		TCP 555	RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Communication with Auxiliary Archiver		TCP 558	RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Cloud playback requests		TCP 570[4]	RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Edge playback stream requests		TCP 605	RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Communication with Privacy Protector™		TCP 754	RTSP over TLS when secure communication enabled	GenetecRedirector.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Stream requests to other redirectors		TCP 560	RTSP over TLS when secure communication enabled	GenetecRedirector.exe
Media transmission to client applications	TCP 960[3]	UDP 6000-6500 TCP 960[3]	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecRedirector.exe
Media transmission to other redirectors	UDP 8000–12000	UDP 8000–12000	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecRedirector.exe
Live video and audio multicast streaming	UDP 47806, 47807	UDP 47806, 47807	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecRedirector.exe
Live video multicast streaming (Security Center Federation™)	UDP 65246	UDP 65246	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecRedirector.exe
Auxiliary Archiver				
Live and playback stream requests	TCP 558		RTSP over TLS when secure communication enabled	GenetecAuxiliaryArchiver.exe
Unicast media streams	UDP 6000-6500		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecAuxiliaryArchiver.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Live video and audio multicast streaming	UDP 47806, 47807		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecAuxiliaryArchiver.exe
Live video multicast streaming (Security Center Federation™)	UDP 65246		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecAuxiliaryArchiver.exe
Live stream requests		TCP 554, 555, 560	RTSP over TLS when secure communication enabled	GenetecAuxiliaryArchiver.exe
Media transmission		TCP 960[3]	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecAuxiliaryArchiver.exe
Cloud Playback				
Cloud playback requests	TCP 570		RTSP over TLS when secure communication enabled	GenetecCloudPlaybackRole.exe GenetecCloudPlaybackAgent.exe
Communication with Cloud storage		TCP 80, 443	TLS 1.2	GenetecCloudPlaybackRole.exe GenetecCloudPlaybackAgent.exe
Media Router				
Live and playback stream requests, and announce requests	TCP 554		RTSP over TLS when secure communication enabled	GenetecMediaRouter.exe
Federated Media Router stream requests		TCP 554	RTSP over TLS when secure communication enabled	GenetecMediaRouter.exe
Media Gateway				

Port usage	Inbound port	Outbound port	Protocol	Executable file
Live and playback stream requests from RTSP clients	TCP 654		RTSP over TLS when secure communication enabled	Genetec.MediaGateway.exe
Incoming stream requests from mobile and web clients	TCP 80, 443		• TCP 80: HTTP • TCP 443: HTTPS	Genetec.MediaGateway.exe
Communication between the Media Gateway agents and the Media Gateway role	TCP 5500	TCP 5500	TLS 1.2	Genetec.MediaGateway.exe
Live video unicast streams	UDP 6000-6500		SRTP when using encryption *in transit and at rest*	Genetec.Media Component32.exe
Live video and audio multicast streaming	UDP 47806, 47807	UDP 51914	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	Genetec.Media Component32.exe
Live video multicast streaming (Security Center Federation™)	UDP 65246		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	Genetec.Media Component32.exe
Live and playback video requests		TCP 554, 555, 558, 560, 605	RTSP over TLS when secure communication enabled	Genetec.Media Component32.exe
Media transmission		TCP 960[3]	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecAuxiliaryArchiver.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Cloud playback requests		TCP 570[4]	RTSP over TLS when secure communication enabled	Genetec.Media Component32.exe
Omnicast™ Federation™				
Connection to remote Omnicast™ 4.x systems.		TCP 5001-5002	TCP	GenetecOmnicast Federation32.exe
Security Center Federation™				
Connection to remote Security Center systems		TCP 5500	TLS 1.2	GenetecSecurityCenter Federation.exe
Security Desk				
Unicast media streams	UDP 6000–6200		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	SecurityDesk.exe Genetec.Media Component32.exe
Live video and audio multicast streaming	UDP 47806, 47807		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	SecurityDesk.exe Genetec.Media Component32.exe
Live video multicast streaming (Security Center Federation™)	UDP 65246		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	SecurityDesk.exe Genetec.Media Component32.exe
Live and playback video and audio requests		TCP 554, 555, 558, 560, 605	RTSP over TLS when secure communication enabled	SecurityDesk.exe Genetec.Media Component32.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Media transmission		TCP 960[3]	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	SecurityDesk.exe Genetec.Media Component32.exe
Cloud playback requests		TCP 570[4]	RTSP over TLS when secure communication enabled	SecurityDesk.exe Genetec.Media Component32.exe
Config Tool				
Unicast media streams	UDP 6000–6200		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	ConfigTool.exe Genetec.Media Component32.exe
Live video and audio multicast streaming	UDP 47806, 47807		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	ConfigTool.exe Genetec.Media Component32.exe
Live video multicast streaming (Security Center Federation™)	UDP 65246		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	ConfigTool.exe Genetec.Media Component32.exe
Live video and audio requests		TCP 554, 555, 560	RTSP over TLS when secure communication enabled	ConfigTool.exe Genetec.Media Component32.exe
Media transmission		TCP 960[3]	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	ConfigTool.exe Genetec.Media Component32.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Unit discovery with the Unit enrollment tool		Vendor-specific TCP and UDP ports	Vendor-specific	ConfigTool.exe Genetec.Media Component32.exe
Cloud storage reporting and configuration		TCP 80[4], 443[4]	HTTP	ConfigTool.exe

[1] Applies to servers hosting one Archiver role. If multiple Archiver roles are hosted on the same server, each additional role uses the next free port.

[2] You can have multiple Archiver agents on the same server. Each Archiver agent assigns a unique UDP port to each video unit it controls. To ensure that the UDP port assignment on a server is unique, each additional Archiver agent on the same server adds 5000 to its starting UDP port number. For example, the first Archiver agent uses ports 15000-19999, the second one uses ports 20000-24999, the third one uses ports 25000-29999, and so on.

NOTE: You can manually assign live streaming reception UDP ports from the **Resource** tab of the Archiver role.

[3] TCP port 960 applies to new installations of Security Center 5.8 and later. In Security Center 5.6 and 5.7, TCP port 5004 was used instead of TCP port 960. Therefore, any system upgraded to 5.10 through 5.6 or 5.7 continues to use TCP port 5004.

[4] In the context of Cloud storage, ports TCP 80, 443, and 570 are only used when Cloud storage is enabled.

Ports used by KiwiVision™ modules in Security Center

The following tables list the default network ports that must be opened to allow proper communication between Security Center and external IP video devices when KiwiVision™ is enabled in your system.

For a visual representation of the ports, see the Security Center Network Diagram - KiwiVision™.

IMPORTANT: Exposing Security Center to the Internet is strongly discouraged without hardening your system first. Before exposing your system, implement the advanced security level described in the *Security Center Hardening Guide* to help protect your system from Internet threats. Alternatively, use a trusted VPN for remote connections.

KiwiVision™ Privacy Protector™ and KiwiVision™ Camera Integrity Monitor modules

Port usage	Inbound port	Outbound port	Protocol	Executable file
Live video requests	TCP 754		RTSP over TLS when using Secure communication	Genetec.MediaProcessor.exe
Live video unicast streams	UDP 7000-7500		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	Genetec.MediaProcessor.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Live video multicast streaming	UDP 47806	UDP 47806	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	Genetec.MediaProcessor.exe
Live video multicast streaming (Security Center Federation™)	UDP 65246	UDP 65246	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	Genetec.MediaProcessor.exe
Live video requests		TCP 554, 555, 560	RTSP over TLS when using Secure communication	Genetec.MediaProcessor.exe
Media transmission		TCP 960[1]	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	Genetec.MediaProcessor.exe

KiwiVision™ Security video analytics and KiwiVision™ People Counter modules

Port usage	Inbound port	Outbound port	Protocol	Executable file
KiwiVision™ Manager				
Communication with KiwiVision™ Manager database		TCP 1433	Microsoft Tabular Data Stream Protocol (TDS)	GenetecPlugin.exe
		UDP 1434	Microsoft SQL Server Resolution Protocol (SSRP)	GenetecPlugin.exe
KiwiVision™ Analyzer				
Live video unicast streams	UDP 6000–6500		SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecPlugin.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Live video multicast streaming	UDP 47806	UDP 47806	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecPlugin.exe
Live video multicast streaming (Security Center Federation™)	UDP 65246	UDP 65246	SRTP when using encryption *in transit from Archiver* or *in transit and at rest*	GenetecPlugin.exe
Live and playback video requests		TCP 554, 560, 960[1]	RTSP over TLS when using Secure communication	GenetecPlugin.exe
Communication with KiwiVision™ Manager database		TCP 1433	Microsoft Tabular Data Stream Protocol (TDS)	GenetecPlugin.exe
		UDP 1434	Microsoft SQL Server Resolution Protocol (SSRP)	GenetecPlugin.exe

[1] TCP port 960 applies to new installations of Security Center 5.8 and later. In Security Center 5.6 and 5.7, TCP port 5004 was used instead of TCP port 960. Therefore, any system upgraded to 5.10 through 5.6 or 5.7 continues to use TCP port 5004.

Ports used by Synergis™ applications in Security Center

The following table lists the default network ports that must be opened to allow proper communication between Security Center and external IP access control devices when Synergis™ is enabled in your system.

For a visual representation of the ports, see the Security Center Network Diagram - Access control.

IMPORTANT: Exposing Security Center to the Internet is strongly discouraged without hardening your system first. Before exposing your system, implement the advanced security level described in the *Security Center Hardening Guide* to help protect your system from Internet threats. Alternatively, use a trusted VPN for remote connections.

Port usage	Inbound port	Outbound port	Protocol	Executable file
Access Manager				
Synergis™ extension - discovery		UDP 2000	Genetec Inc. proprietary protocol	GenetecAccessManager.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Secure communication with Synergis™ units and HID units		TCP 443	HTTPS TLS 1.2	GenetecAccessManager.exe
HID extension - FTP data and command[1]	TCP 20	TCP 21	FTP	GenetecAccessManager.exe
HID extension - SSH[1]		TCP 22	SSH	GenetecAccessManager.exe
HID extension - Telnet[1]		TCP 23	Telnet	GenetecAccessManager.exe
HID extension - HTTP communication		TCP 80	HTTP	GenetecAccessManager.exe
HID extension - VertX OPIN protocol		TCP 4050/4433[2]	• TCP 4050: Proprietary • TCP 4433: HTTPS TLS 1.2	GenetecAccessManager.exe
HID extension - VertX discovery[3]	UDP 4070	UDP 4070	N/A	GenetecAccessManager.exe
Remote syslog server[4]	UDP 514		N/A	GenetecAccessManager.exe
Security Desk and Config Tool				
Secured communication with the portal of the mobile credential provider Client needs access to the following URLs: https://api.origo.hidglobal.com For 5.10.0.0: https://portal.origo.hidglobal.com/ For 5.10.1.0 and later: https://ma.api.assaabloy.com/credential-management/		TCP 443	HTTPS TLS 1.2	SecurityDesk.exe ConfigTool.exe
Global Cardholder Synchronizer				
Connection to sharing host		TCP 5500	TLS 1.2	GenetecGlobal CardholderManagement.exe

Port usage	Inbound port	Outbound port	Protocol	Executable file
Mobile Credential Manager				
Secured communication with the portal of the mobile credential provider Mobile Credential Manager role needs access to the following URLs: https://api.origo.hidglobal.com For 5.10.0.0: https://portal.origo.hidglobal.com/ For 5.10.1.0 and later: https://ma.api.assaabloy.com/credential-management/		TCP 443	HTTPS TLS 1.2	GenetecMobileCredentialManager.exe

[1] Not used if HID units are configured with **Secure mode**. As a best practice, enable secure mode on all HID units.

[2] Legacy HID units or EVO units running a firmware version earlier than 3.7 use port 4050. HID EVO units running in secure mode with firmware 3.7 and later user port 4433.

[3] The discovery port of an HID unit is fixed at 4070. After it is discovered, the unit is assigned to an Access Manager that uses the ports shown in the previous table to control it.

For more information about initial HID hardware setup, download the documentation from http://www.HIDglobal.com.

[4] Starting in Security Center 5.10.1.0, this port is no longer enabled by default.

Installing SQL Server independently of Security Center

Depending on your deployment requirements, you might have to install SQL Server before you install Security Center. The most common reasons are to install SQL Server on a drive that is separate from the system drive (typically the C: drive), or on a server that is separate from all Security Center servers.

Before you begin

If you are installing SQL Server Standard or Enterprise edition, you must purchase it from Microsoft, and download the installation package. The installer for SQL Server Express is included in the Security Center installation package. SQL Server Express only works on 64-bit operating systems.

What you should know

There are many reasons why you must install SQL Server yourself. The most obvious one is when SQL Server Express does not satisfy your database requirements. Even when SQL Server Express is all you need, you might still have to install it yourself for the following reasons:

- You plan on setting up a role *failover*. In this case, install SQL Server on a server that is different from all servers hosting your role. For more information, see the *Security Center Administrator Guide*.
- Microsoft Volume Shadow Copy Service (VSS) is enabled on your server. In this case, install SQL Server on a drive that is separate from the system drive, and make sure that VSS only takes snapshots of the system drive.

  CAUTION: Do not disable VSS. Disabling VSS interferes with the operation of Windows System Restore.

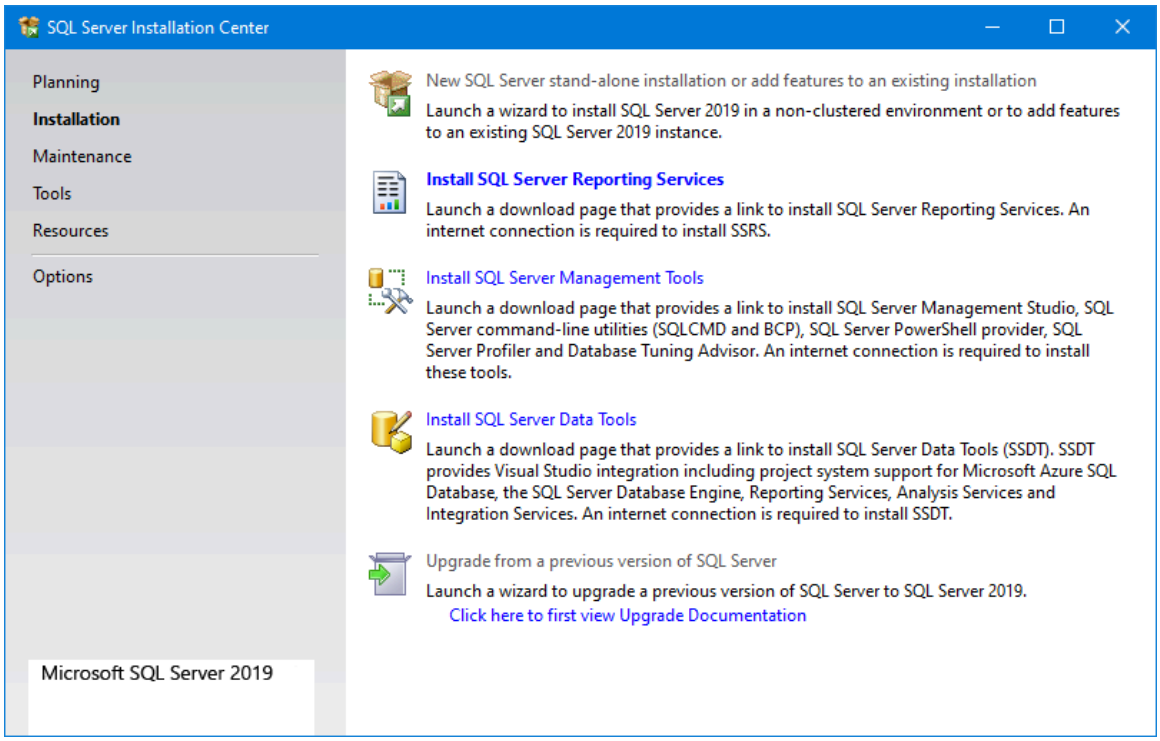
To install SQL Server yourself:

1 Do one of the following:

- If you are installing SQL Server Standard or Enterprise:
  a. In Windows, navigate to the SQL installation package folder.
  b. Double-click *Setup.exe*.
- If you are installing SQL Server Express:
  a. In Windows, navigate to the Security Center installation package folder.
  b. Open the folder *SC Packages\SQLExpress*.
  c. Double-click *SQLEXPRADV_x64_ENU.exe*.

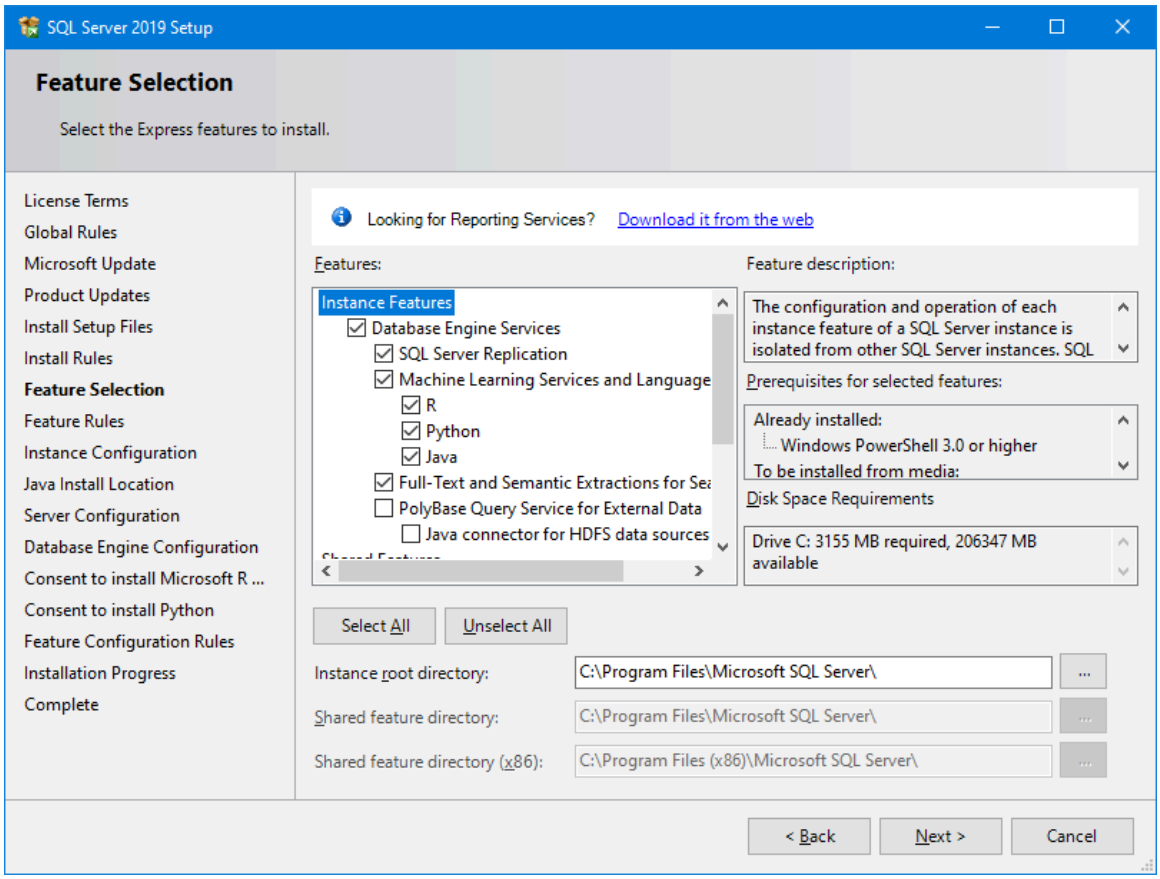
2 On the *SQL Server Installation Center* page, click **New SQL Server stand-alone installation or add features to an existing installation**.

NOTE: The screenshots shown in the following steps are for SQL Server 2019. The screens you see might look slightly different.



3 Read the software license terms, select **I accept the license terms**, and then click **Next**.

4 On the *Feature Selection* page, select *Database engine services* and any other features you want to install. For additional information on these features, consult the Microsoft SQL Server documentation.



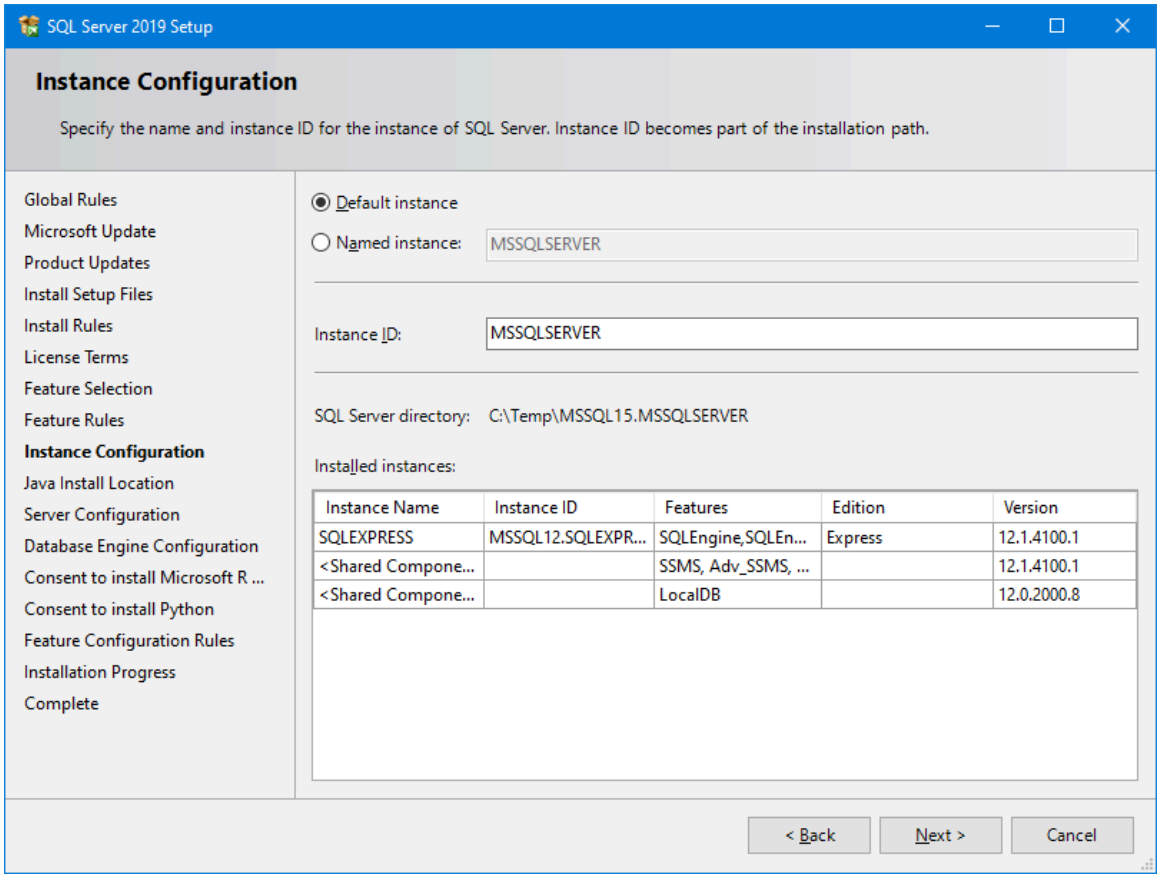
5 In the **Instance root directory** field, select where to install SQL Server and all role database files.

This is where you need to change the default path to C: drive if you want your databases to be stored on a different drive. You can type a path, or browse for a folder.

6 In the **Shared feature directory** field, select where to install the SQL Server shared features.

7 Click **Next**.

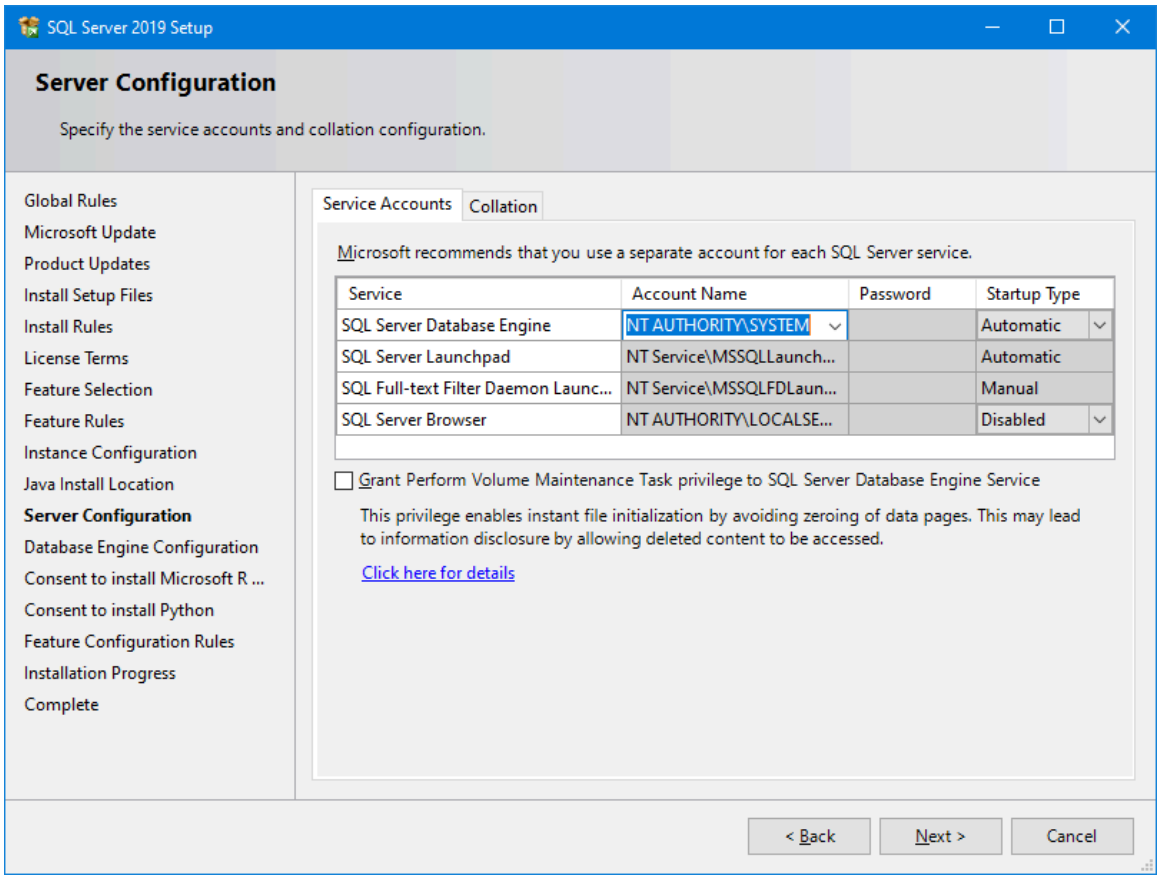
8 On the *Instance Configuration* page, select a name for the SQL Server.



NOTE: The database server name is not case-sensitive, but it must meet all of the following criteria:

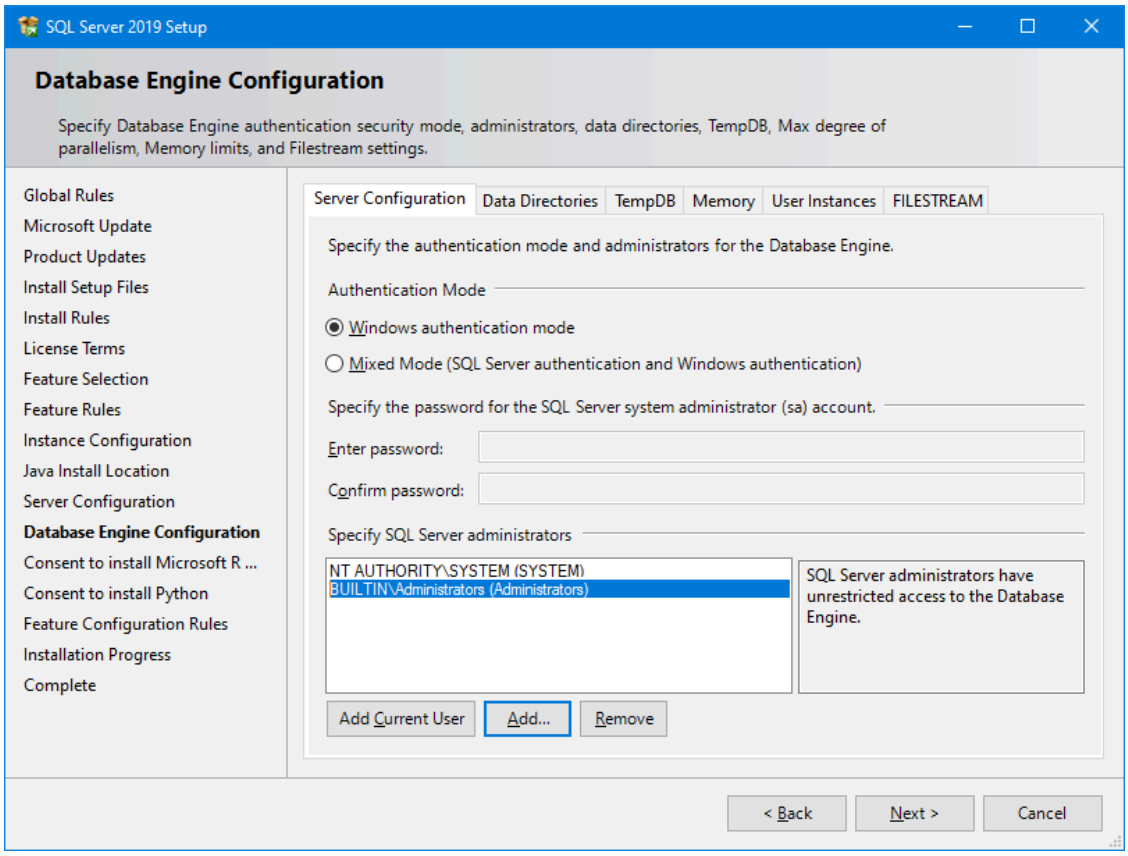
- It cannot be the same name as an existing SQL instance on your server.
- It cannot match any of the SQL Server reserved keywords, such as DEFAULT, PRIMARY, and so on.
- It cannot be longer than 16 characters.
- The first character of the instance name must be a letter or an underscore (_). Acceptable letters are defined by the Unicode Standard 2.0, including Latin characters a-z and A-Z, and letter characters from other languages.
- Subsequent characters can be letters defined by the Unicode Standard 2.0, decimal numbers from Basic Latin or other national scripts, the dollar sign ($), or an underscore (_).
- It cannot contain spaces or the following characters: \ , : ; ' & # @

9 On the *Server Configuration* page, select "NT AUTHORITY\SYSTEM" for the SQL Server Database Engine **Account Name**, unless your database administrator instructed you to do otherwise, and click **Next**.



10 On the *Database Engine Configuration* page, select the authentication mode for accessing the Database engine, and click **Next**.

- **Windows authentication mode:** Windows credentials. Specify "`NT AUTHORITY\SYSTEM`" plus any other account that must have permission to make configuration changes, such as the "`BUILTIN\Administrators`" user group.
- **Mixed mode:** Windows administrators can access the database engine using either their Windows credentials, or the password you specify here.



11 On the *Consent* pages, read the consent criteria and click **Accept** > **Next**.

12 Wait for the installation to complete. This can take several minutes.

13 Click **Close**.

SQL Server can now be used as your Security Center database server.

14 If you installed SQL Server Express, do the following:

a) Open the folder *SC Packages\Microsoft SQL Server Management Studio - 18.5.1*.

b) Double-click *SSMS-Setup-ENU.exe*.

After you finish

Install Security Center on the main server, and use the new SQL Server as your database server.

Related Topics

Preparing to perform a silent installation on page 125

Installing the Security Center main server

The main server in your Security Center system hosts the Directory role. You must install the main server first.

Before you begin

Prepare to install Security Center.

What you should know

A main server installation includes the following:

- The Genetec™ Server service with the Directory role.
  - Server Admin
  - Genetec™ Watchdog
- (Optional) Client applications: Config Tool, Security Desk, or both.
- (Optional) Omnicast™ compatibility packs to view video from federated Omnicast™ systems.

To install a Security Center main server:

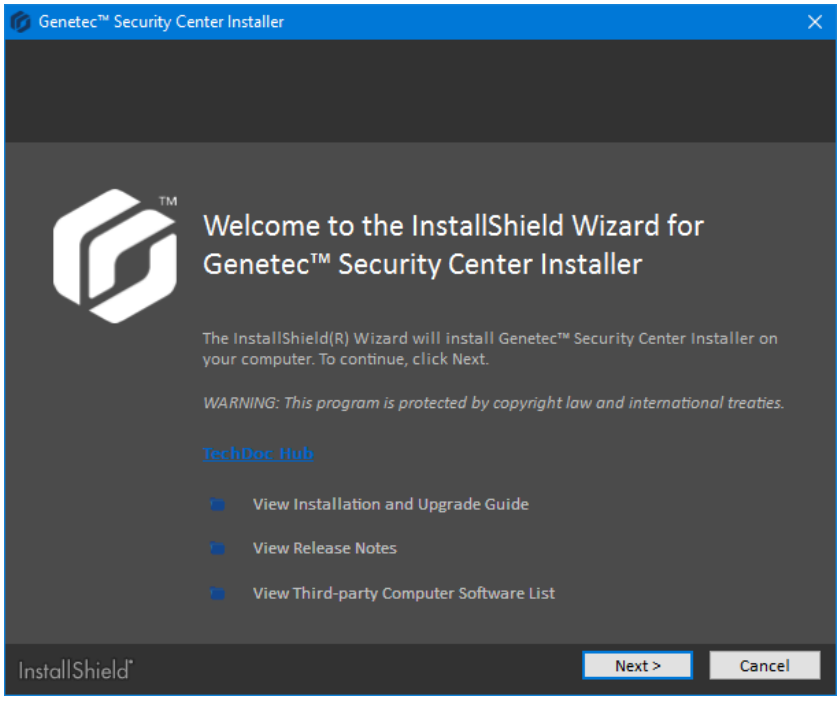
1 Right-click either *setup.exe* (standalone version) or *SecurityCenterWebSetup.exe* (web version), and click **Run as administrator**.

The InstallShield Wizard opens.

NOTE: Only the standalone installer is illustrated in this procedure.

2 On the *Choose Setup Language* page, select the language of the InstallShield Wizard, and click **Next**.

3 On the welcome page, click **Next**.

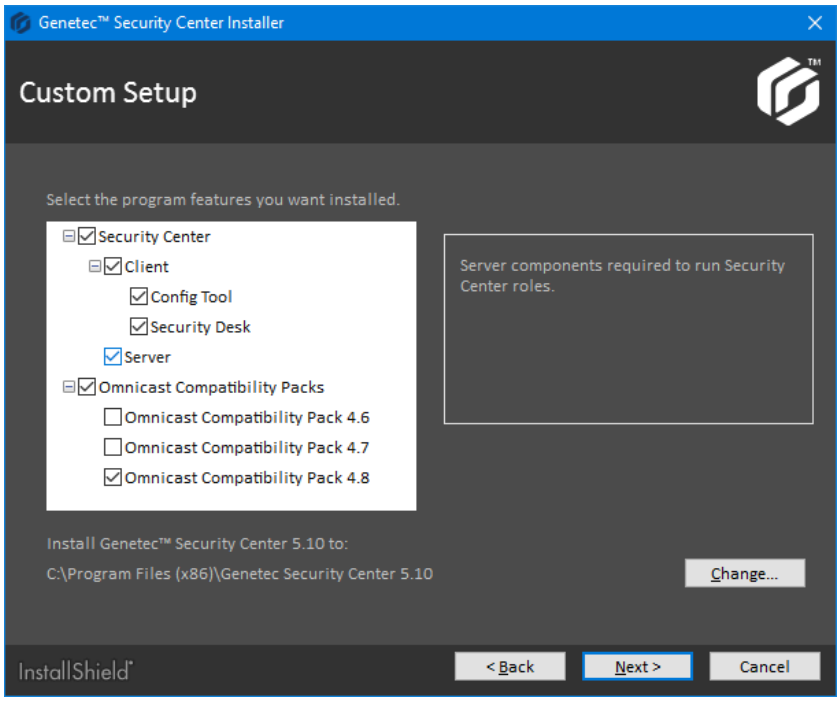


Links to relevant Security Center information are provided.

4 On the *License Agreement* page, read the terms in the *Software License Agreement*, select **I accept the terms in the license agreement**, and then click **Next**.

If you are upgrading from a previous version, a *Backward Compatibility* notice opens. Ensure that you understand the backward compatibility requirements before proceeding.

5 On the *Custom Setup* page, select the Security Center features to install, specify the destination folder, and then click **Next**.



You must select **Server** from the list. All other features are optional.

For the destination folder, you can only change the *root folder* where the *Genetec Security Center 5.10* folder is created. On a 64-bit machine, the default root folder is *C:\Program Files (x86)*.

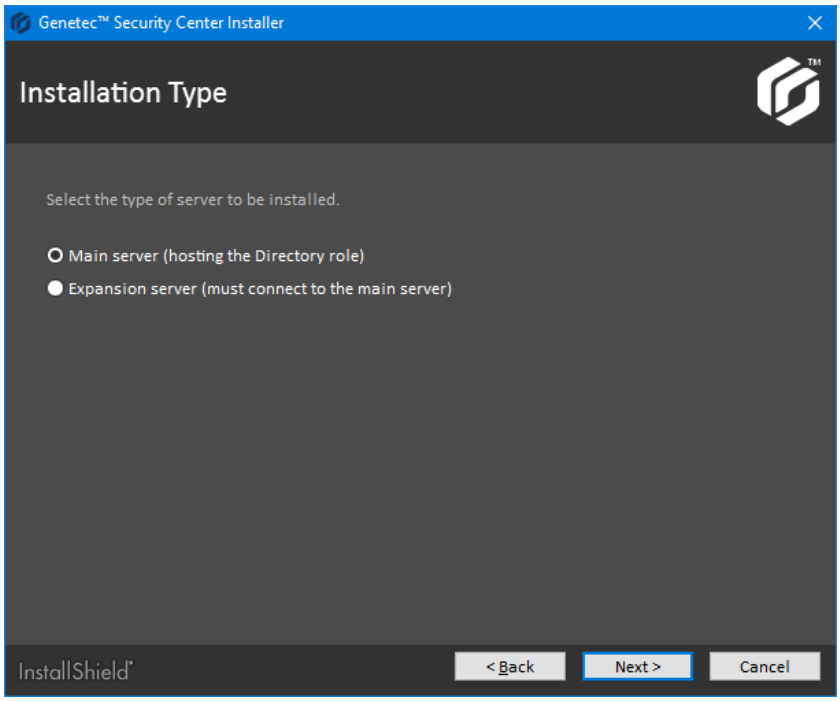
6 On the *Genetec™ Security Center Language Selection* page, select the user interface language for Security Center applications, and click **Next**.

NOTE: Online help for Security Center applications is not available in all languages. For language availability, see the *Security Center Release Notes*.

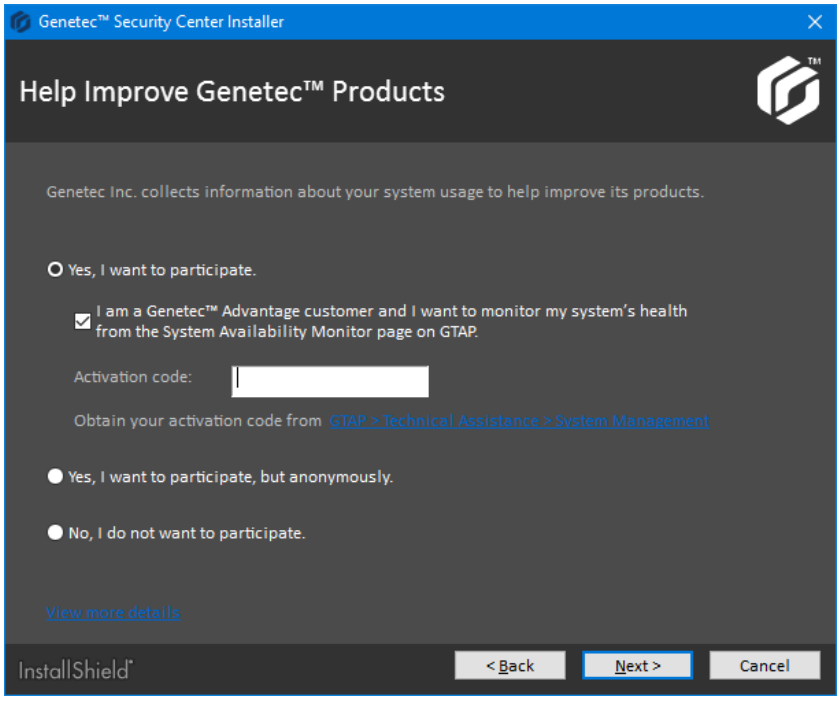
TIP: After installing Security Center, you can change the user interface language with the *Language Tool* found in the Genetec™ Security Center program group in the Start menu.

7 On the *Installation Type* page, select **Main server**, and click **Next**.

IMPORTANT: There must only be one **Main server** installation per system. If your Security Center license supports additional Directory servers, they must be installed as expansion servers. For more information, see the *Security Center Administrator Guide*.

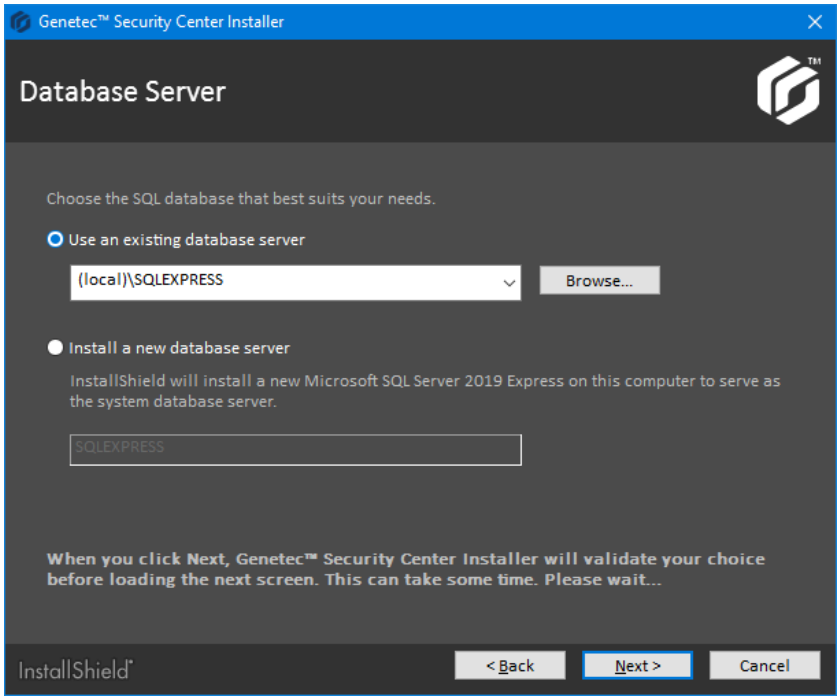


8 On the *Help Improve Genetec™ Products* page, select how much you want to participate in our data collection, and click **Next**.



A short description of each option and a link to our Global Privacy Policy are available by clicking **View more details**.

9 On the *Database Server* page, select an SQL database, and click **Next**.



The following options are available:

- **Use an existing database server:** Selects an existing Microsoft SQL Server instance on this machine, or another server.

  BEST PRACTICE: Replace (local) with either the computer name or hostname, and port, if required.

  For example: DB_SERVER.GENETEC.COM,1433\SQLEXPRESS

  You must use a computer name or hostname if you are configuring the Directory for load balancing. For more information on load balancing, see the *Security Center Administrator Guide*.

  If you are upgrading from a supported version of Security Center, the installer automatically upgrades all databases that your system requires.

  If you are using an old version of SQL Server Express, you get the option to upgrade your database server to SQL Server 2019 Express Edition if the following conditions are met:

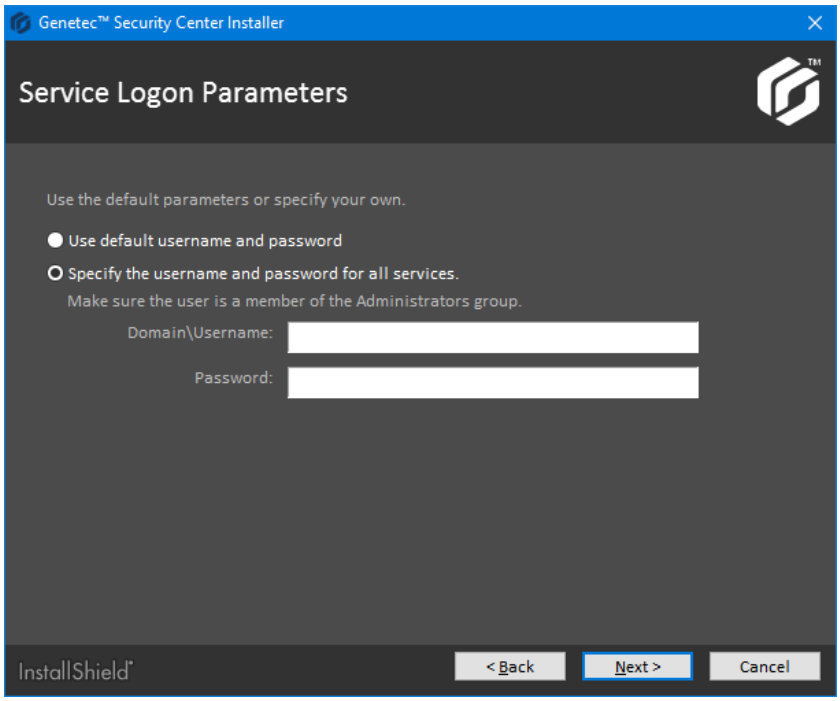
  - You are running a version of Windows that supports SQL Server 2019 Express Edition. This means the 64-bit version of Windows 10 or Windows Server 2016 or later.
  - Your current version of SQL Server is upgradable to SQL Server 2019 Express Edition. This means one of the following versions:
    - SQL Server 2012 SP4 Express, version 11.0.7001.0 or later
    - SQL Server 2014 SP2 Express, version 12.0.5000.0 or later
    - SQL Server 2016 Express, version 13.0.1601.5 or later
    - SQL Server 2017 Express, version 14.0.1000.169 or later
- **Install a new database server:** Installs Microsoft SQL Server 2019 Express Edition on this computer. You must choose a database server name. The default is SQLEXPRESS.

NOTE: The database server name is not case-sensitive, but it must meet all of the following criteria:

- It cannot be the same name as an existing SQL instance on your server.
- It cannot match any of the SQL Server reserved keywords, such as DEFAULT, PRIMARY, and so on.
- It cannot be longer than 16 characters.
- The first character of the instance name must be a letter or an underscore (_). Acceptable letters are defined by the Unicode Standard 2.0, including Latin characters a-z and A-Z, and letter characters from other languages.
- Subsequent characters can be letters defined by the Unicode Standard 2.0, decimal numbers from Basic Latin or other national scripts, the dollar sign ($), or an underscore (_).
- It cannot contain spaces or the following characters: \ , : ; ' & # @

NOTE: SQL Server 2019 Express is only supported on the 64-bit version of Windows 10 and Windows Server 2016 and later. If the version of Windows you are running is not one of these, quit the Security Center installation, download SQL Server 2014 Express SP3 from Microsoft Download Center, and install it first before installing Security Center.

10 On the *Service Logon Parameters* page, set the username and password used to run Security Center services.



a) Select one of the following options:

- **Use default name and password:** Select this option to use the LocalSystem account to run your Security Center services. The LocalSystem account has extensive privileges on the local computer, and acts as the computer on the network.
- **Specify the username and password for all services:** Select this option if you want to restrict the privileges granted to the service user. Enter a valid domain username and a strong password, and record them in a safe place. You must provide these credentials every time you upgrade your Security Center software. Use industry best practices for creating strong passwords.

  IMPORTANT: Make sure the service user is a local administrator and not a domain administrator. The service user must have sufficient rights to the local or remote database, and *Log on as service* user rights. If this server will host the Active Directory role, the specified user must also have read and write access to the Active Directory that you want the server to connect to.

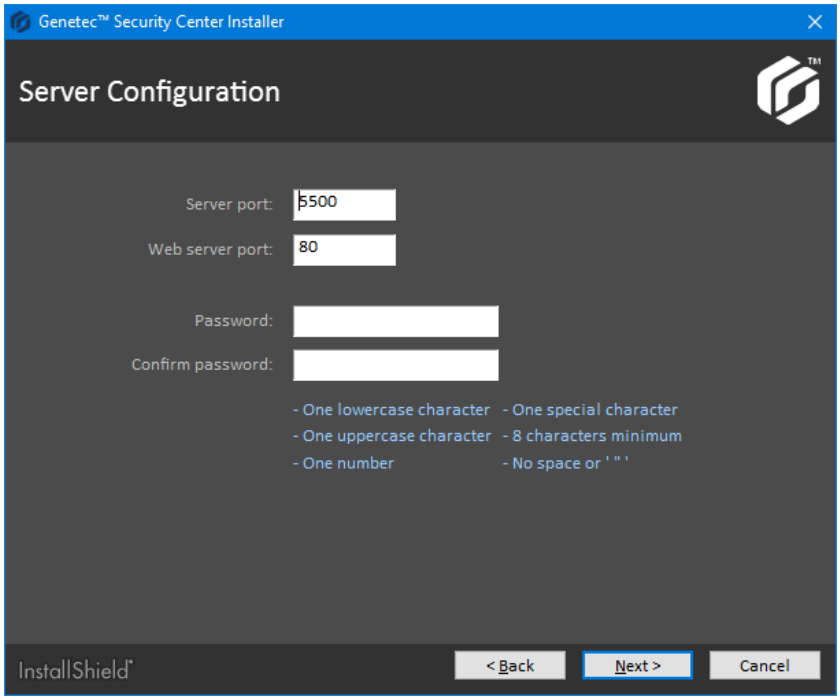
NOTE: The service user automatically creates all the necessary databases when the system is started for the first time. For this reason, the service user needs the SQL Server role, dbCreator, for its first run. After the databases are created, you can remove the dbCreator role.

To avoid having to grant the dbCreator role to the service user, you can create the databases required by the Security Center roles yourself, as empty databases. When the system is started for the first time, the service user only has to create the tables, without going through the database creations. For the list of Security Center roles that need a database and the minimum SQL Server roles they require, see "About connecting to SQL Server with an account that has administrative privileges" in the *Security Center Hardening Guide*.

You can also deny the service user the dbCreator role and create the databases later. In this case, the Security Center roles that require a database will fail at system startup. You must then create the databases and restart each role manually. You can also change the service user later from Microsoft Management Console.

b) Click **Next**.

11 On the *Server Configuration* page, set the server connection parameters.



a) Complete the following fields:

- **Server port:** The TCP port through which the servers in your system communicate.
- **Web server port:** The HTTP port that is used for the web-based Server Admin. If you change the default port, the Server Admin address must include the port number in the URL. For example, *http://computer:port/Genetec* instead of *http://computer/Genetec*. The link to Server Admin, accessible through Start menu, automatically includes this port.

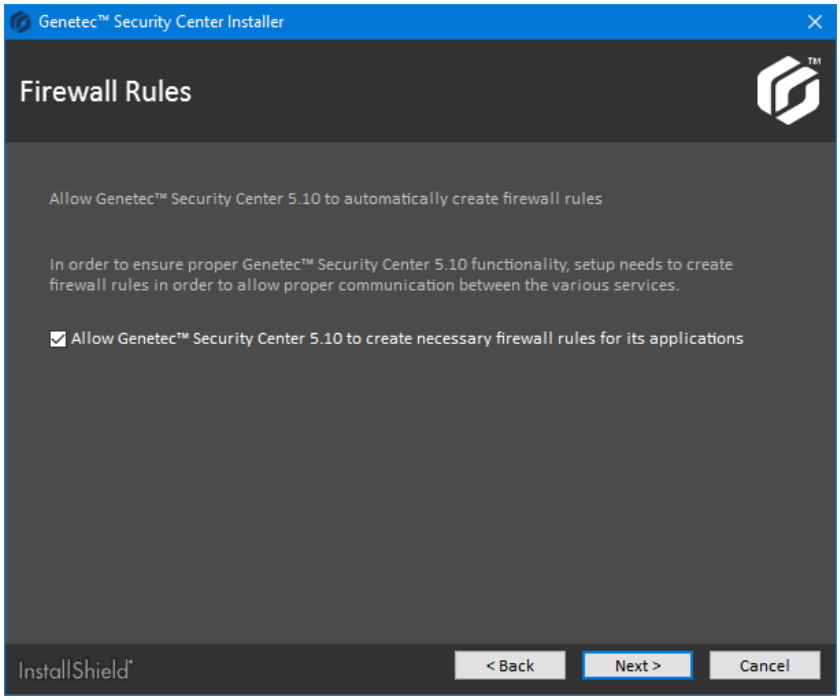
  CAUTION: Watch out for conflicts with other software, such as a Skype, running on the server that might use port 80.
- **Password/Confirm password:** Enter and confirm the password to open the web-based Server Admin.

  BEST PRACTICE: If you are upgrading your Security Center installation, the existing server password is kept by default. If you were using a blank password, we recommend that you enter a new one that contains at least one uppercase character, one lowercase character, one number and one special character.

IMPORTANT: If you lose the server password, call Genetec™ Technical Support to reset it.

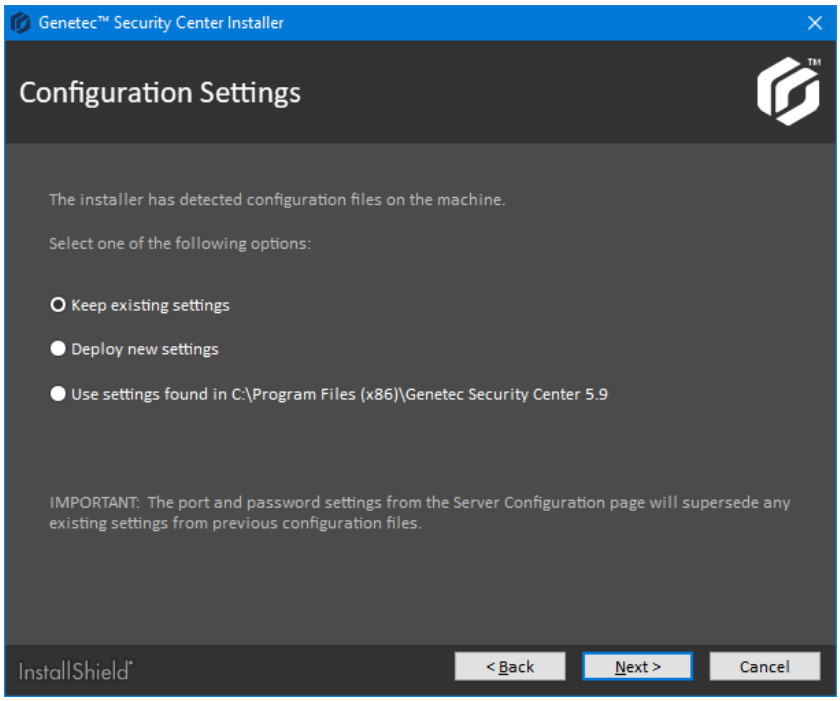
b) Click **Next**.

12 On the *Firewall Rules* page, grant the installer permission to automatically configure the Windows Firewall for Security Center, and click **Next**.



NOTE: This option only affects the Windows Firewall. After installation, you must also configure the required ports on other firewalls that control Security Center communication.

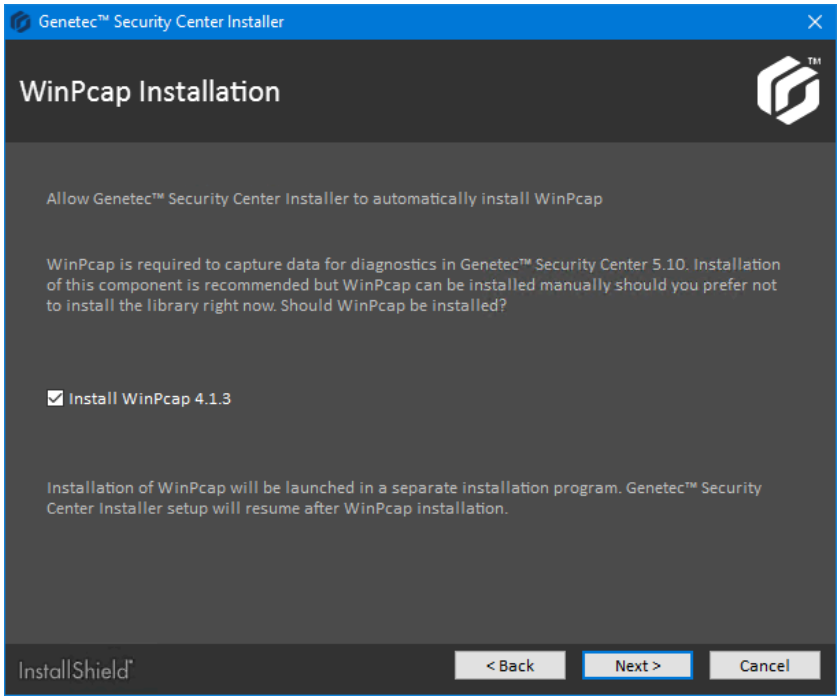
13 If old configuration files (*ConfigurationFiles*.gconfig*) are detected on your computer, you have the option to select which configuration to use. This step is skipped if you are upgrading your system.



- **Keep existing settings:** Use the existing configuration files detected for an older release of the current major version (5.10). This option is hidden if Security Center 5.10 was never installed on this computer.
- **Deploy new settings:** Disregard any existing configuration files you might have on your computer and install the default configuration files for the version you are installing.
- **Use settings found in <Security Center Installation Folder>:** Use the configuration files found in an older Security Center installation folder. This option is only available if an older major version of Security Center is detected.

- If WinPcap 4.1.3 is not installed, the *WinPcap Installation* page opens.
- If WinPcap 4.1.3 is already installed, the *Security Settings* page opens.

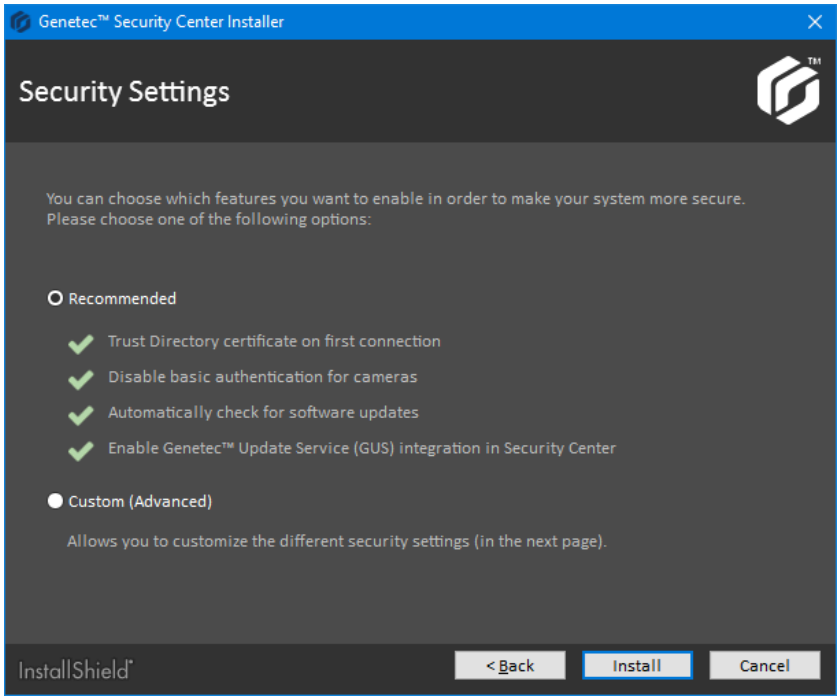
14 On the *WinPcap Installation* page, select **Install WinPcap**, if required, and click **Next**.



WinPcap captures diagnostic data for units and other services in Security Center. If you require assistance, this data can help Genetec™ technical support troubleshoot your issue.

WinPcap can be installed later.

15 On the *Security Settings* page, configure features to make your system more secure.

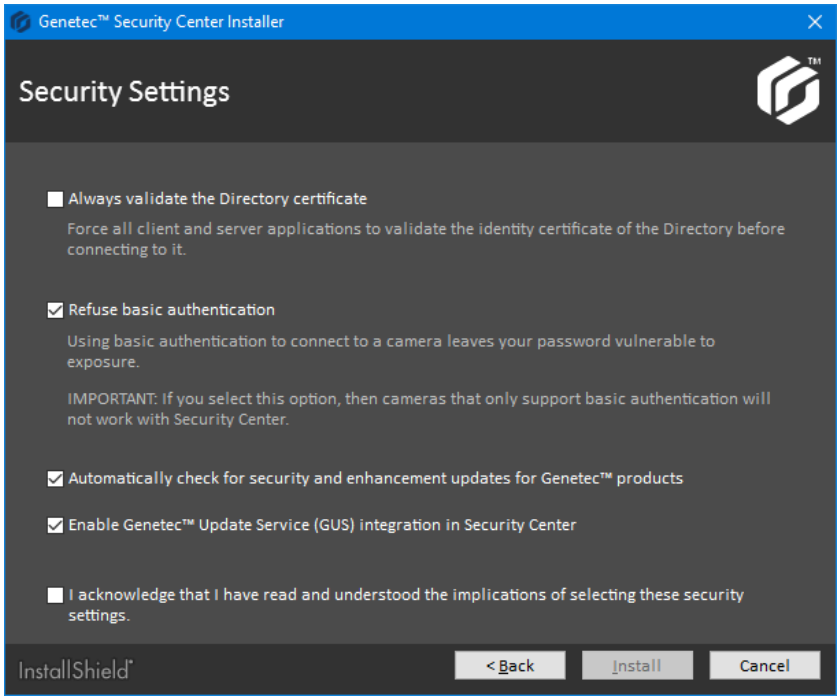


- Select **Recommended** to set the default security settings, and click **Install** to start the installation.

  The recommended security settings are:

  - If the certificate is self-signed, whitelist the *identity certificate* of the first Directory server this machine connects to.
  - Disable basic access authentication for cameras in favor of the more secure digest access authentication.
  - Automatically check for software updates.
  - Enable *Genetec™ Update Service (GUS)* integration in Security Center.
- Select **Custom (Advanced)** to configure the security settings, and click **Next**.

16 If you selected **Custom (Advanced)**, configure the security settings.



a) Configure the following settings:

- **Always validate the Directory certificate:** Select this option to force all client and server applications on the current machine to validate the identity certificate of the Directory before connecting to it.

  BEST PRACTICE: If you enable *Directory authentication*, it is best to use a certificate issued by a trusted certificate authority (CA). Otherwise, the first time this computer connects to the Directory, the user is prompted to confirm the identity of the Directory server.

  For more information on Directory authentication, see the *Security Center Administrator Guide*.
- **Turn off basic authentication:** Basic access authentication for cameras is turned off by default to prevent camera credentials from being compromised when the Archiver connects to a video unit.

  IMPORTANT: When this option is selected, cameras that only support basic access authentication will not work.

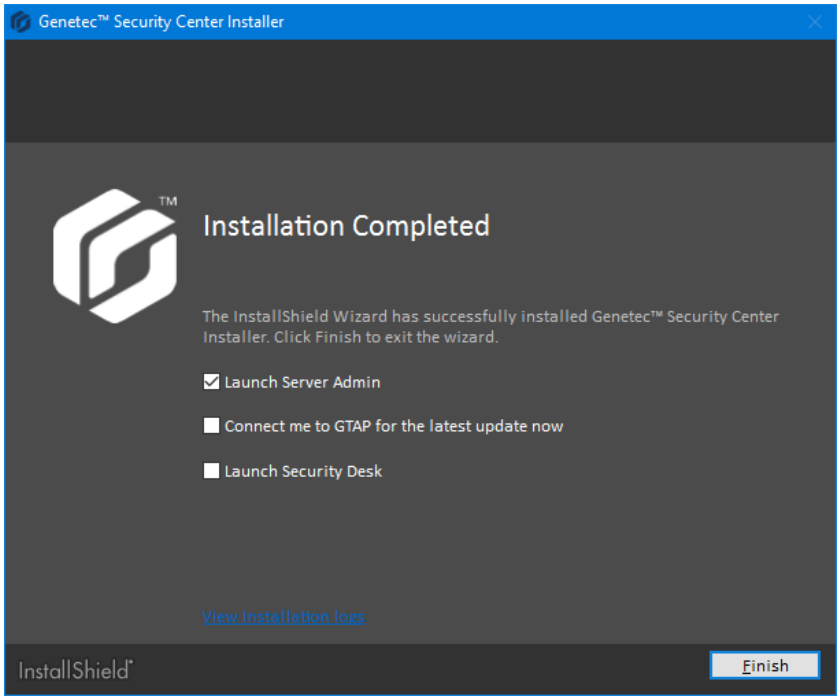
  TIP: Most recent video unit models support digest access authentication. If you are not sure whether your cameras support *digest* or not, leave the default setting as is. After installation, if some cameras do not work, you can always turn basic access authentication on again.
- **Automatically check for security and enhancement updates for Genetec™ products:** Select this option to allow GUS to automatically check for updates of all installed Genetec™ products.
- **Enable Genetec™ Update Service (GUS) integration in Security Center:** Enable this option to make GUS available in Config Tool.

b) Select **I acknowledge that I have read and understood the implications of selecting these security settings**, and click **Install** to start the installation.

17 If you chose to install WinPcap 4.1.3, follow the *WinPcap 4.1.3 Setup Wizard* that opens.

a) On the *Installation options* page, select **Automatically start the WinPcap driver at boot time**.
b) Click **Install**.

18 On *Installation Completed* page, select the required post-installation options, and click **Finish**.



If you selected **Launch Server Admin**, Server Admin opens in a browser window. Before using Security Center, you must connect to Server Admin and activate your product license.

If you selected **Connect me to GTAP for the latest updates now** and your machine has Internet access, you are connected to the Genetec™ *Product Download* page on GTAP. You need a username and a password to log in.

If you selected **Launch Security Desk**, Security Desk opens automatically. However, you cannot log on to the Directory until your product license is activated.

If you get a message asking you to restart your computer, click **Yes**.

If you get a warning message that the SQL Server 2019 telemetry service cannot be disabled, disable it manually.

The Security Center main server is now installed.

After you finish

Do the following:

- Activate your product license from the Server Admin.
- Configure Genetec™ Update Service.

  For more information, see the *Genetec™ Update Service User Guide*.
- If required, install Security Center on expansion servers.

Related Topics

Activating Security Center license using the web on page 46
Activating Security Center license manually on page 49
Installing Security Center expansion servers on page 54
Installing SQL Server independently of Security Center on page 28

Activating Security Center license using the web

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

To activate your Security Center license using web activation:

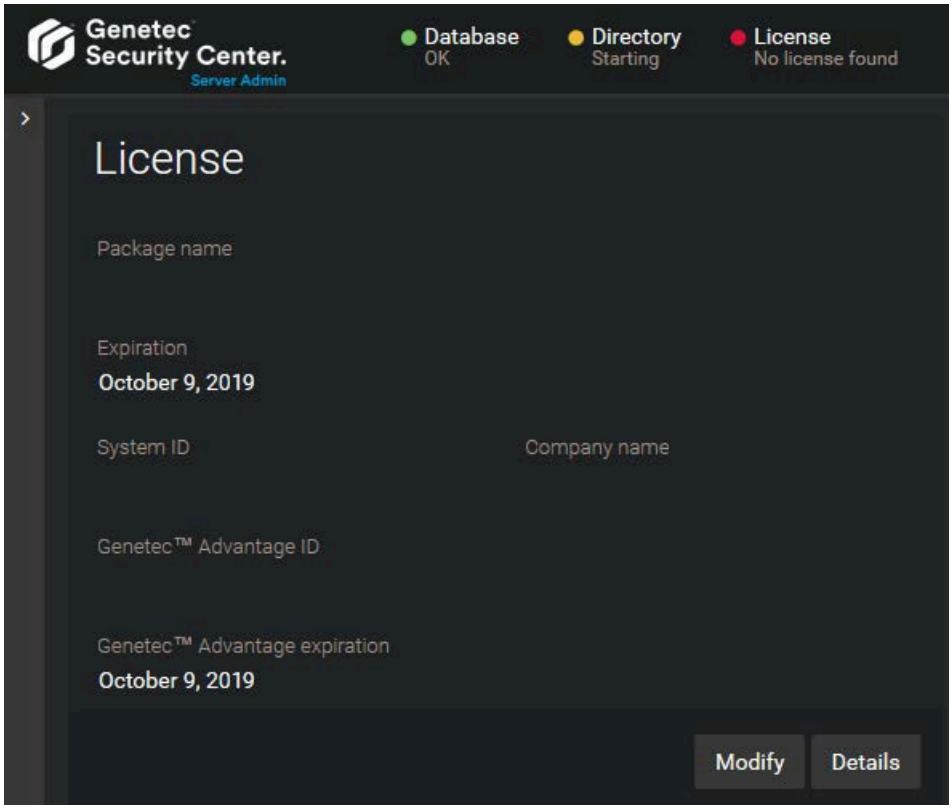
1 Open the Server Admin web page by doing one of the following:

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

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

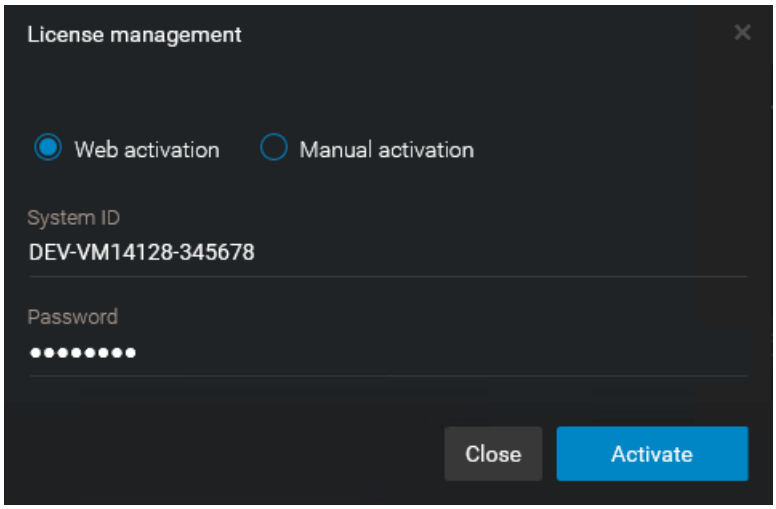
The Server Admin *Overview* page opens.

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

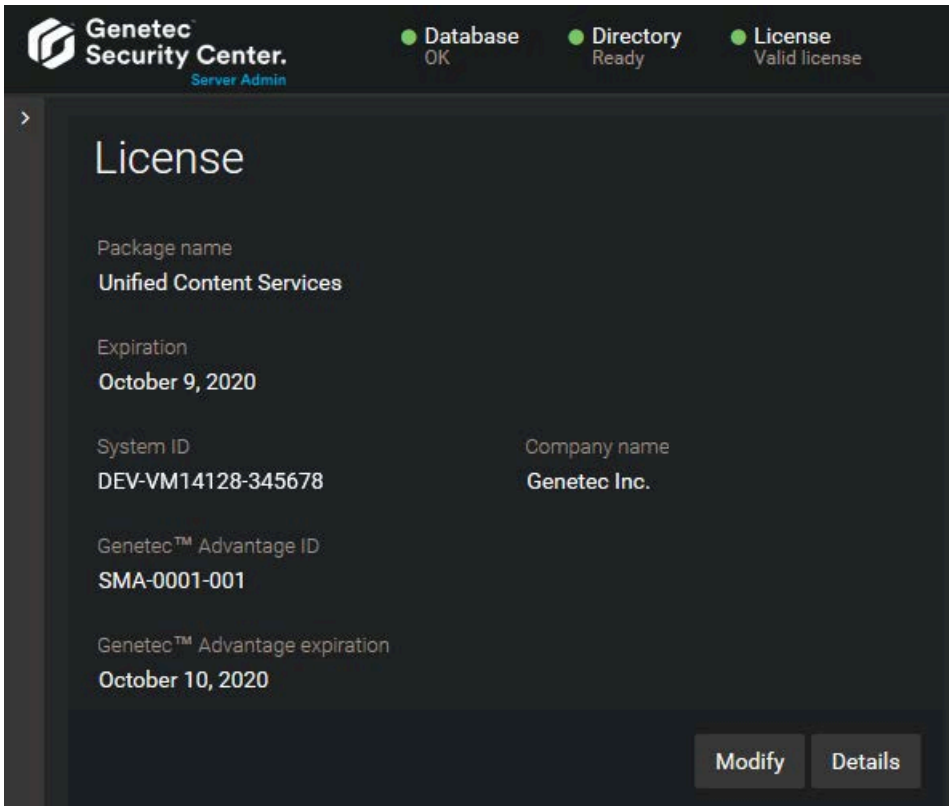


4 In the *License management* dialog box, click **Web activation** and enter your **System ID** and **Password**.

Your system ID and password are specified in the *Security Center License Information* document. Our Customer Service team sends you this document when you purchase the product.



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



Activating Security Center license manually

After you install Security Center on the main server or promote an expansion server to a main server, you must activate your Security Center license on the main server. If you do not have Internet access, you can activate your Security Center license using *manual activation* from Server Admin and GTAP.

To activate your Security Center license manually:

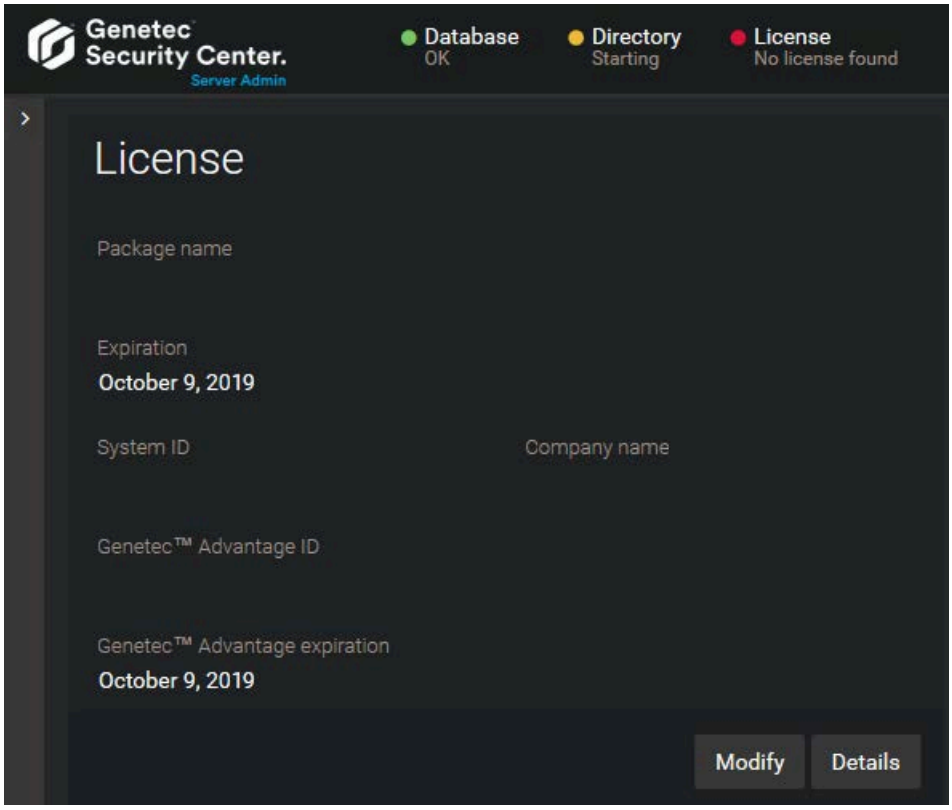
1 Open the Server Admin web page by doing one of the following:

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

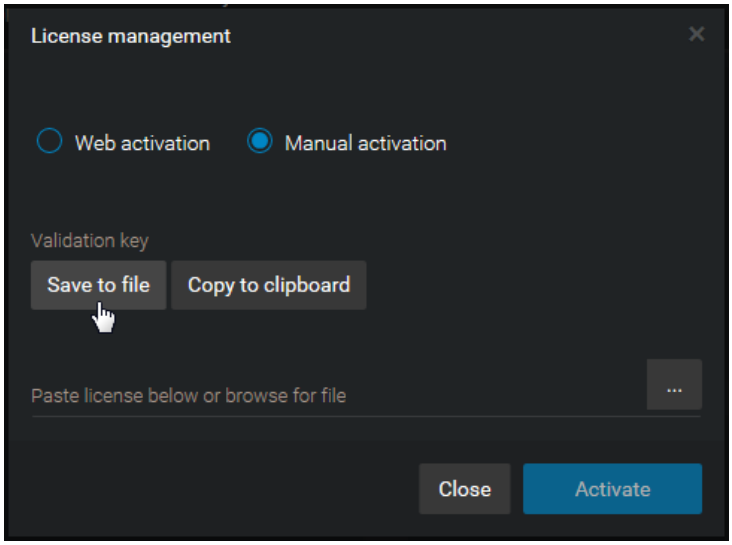
2 Enter the server password that you set during the server installation, and click **Log on**.

The Server Admin *Overview* page opens.

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



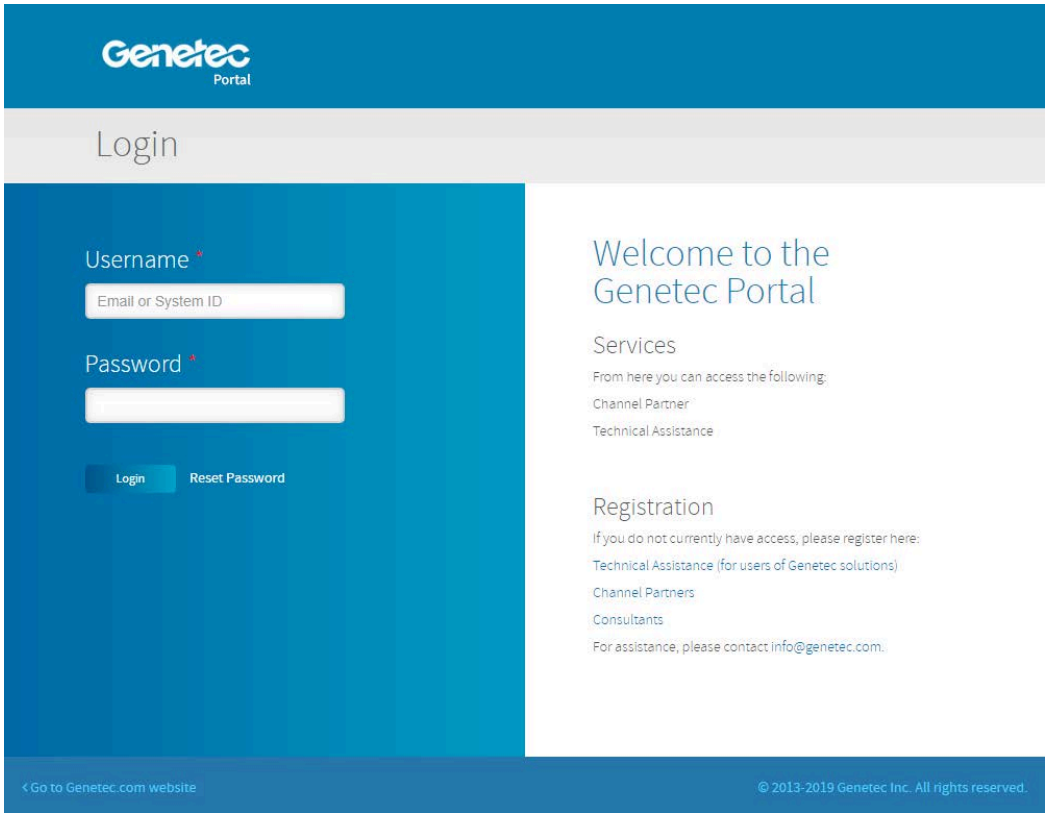
4 In the *License management* dialog box, click **Manual activation**, and then under *Validation key*, click **Save to file**.



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

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

5 From a computer with internet access, open the Genetec™ Technical Assistance Portal (GTAP) at: https://portal.genetec.com/support.



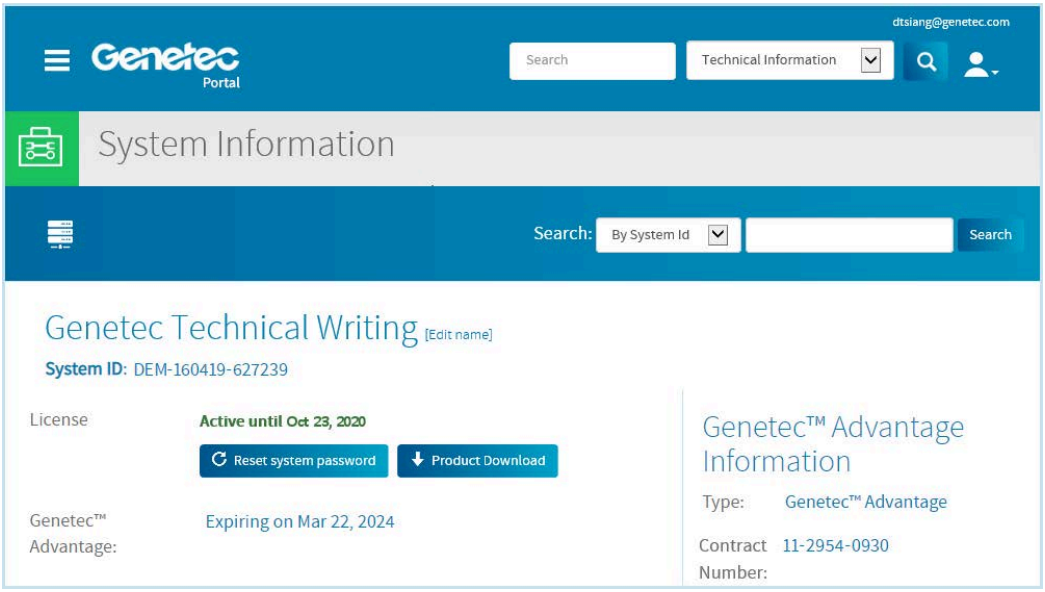
6 On the *Login* page, do one of the following:

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

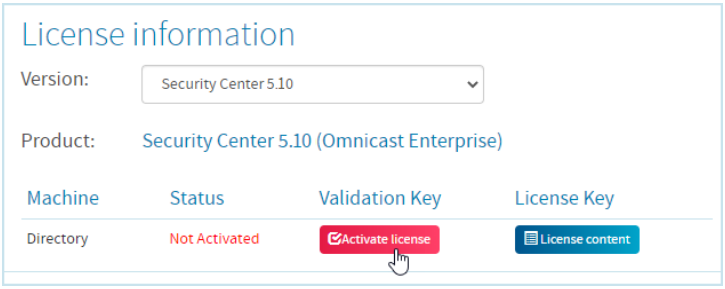
  Your system ID and password are specified in the *Security Center License Information* document. Our Customer Service team sends you this document when you purchase the product.
- Enter the email address for your GTAP user account and password, and then click **Login**

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

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



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



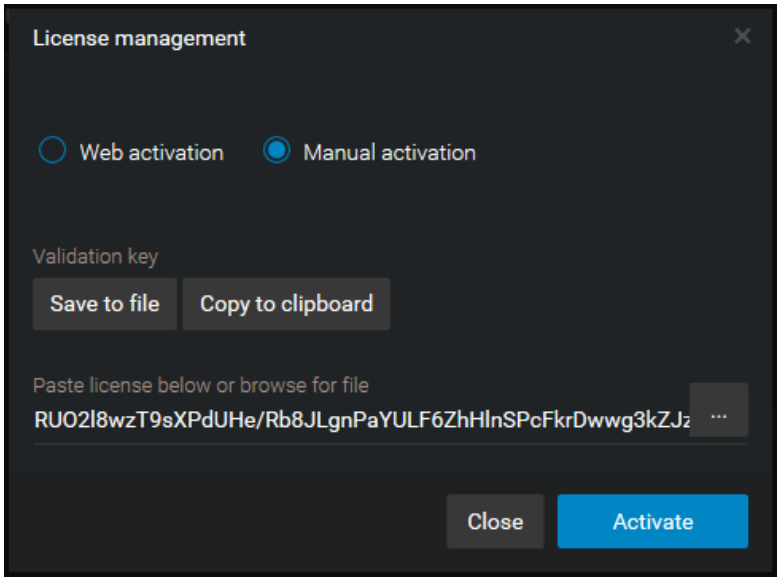
10 In the dialog box that opens, browse to your validation key (.vk file), and click **Submit**.

11 When you receive the License activation successful message, click **Download** under *License Key* and save the license key to a file.
The default file name is your system ID, followed by *_Directory_License.lic*.

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

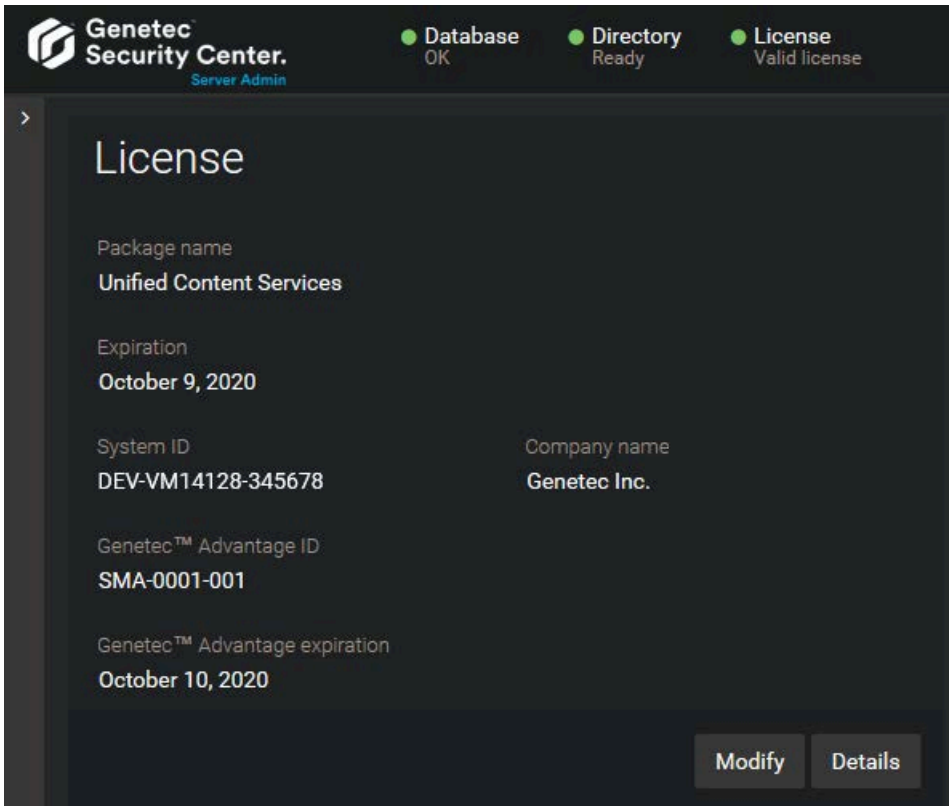
13 In the *License management* dialog box, do one of the following:

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



14 Click **Activate**.

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



Installing Security Center expansion servers

To add processing power to your Security Center system, you can install expansion servers and connect them to the main server.

Before you begin

- Prepare to install Security Center.
- Install the Security Center main server, and ensure that it is up and running.

What you should know

An expansion server installation includes the following:

- The Genetec™ Server service without the Directory role.
  - Server Admin
  - Genetec™ Watchdog
- (Optional) Client applications: Config Tool, Security Desk, or both.
- (Optional) Omnicast™ compatibility packs to view video from federated Omnicast™ systems.

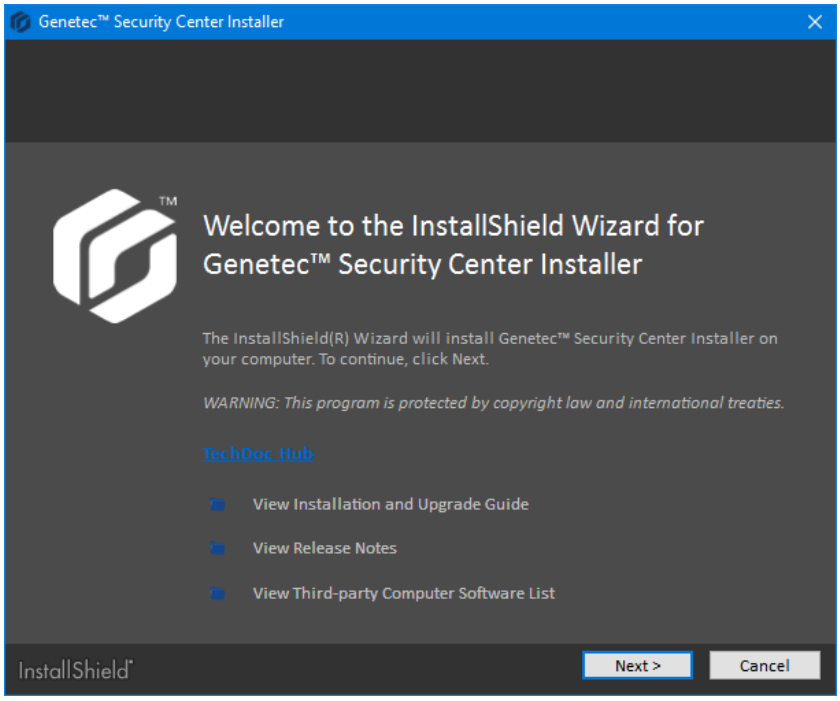
To install a Security Center expansion server:

1 Right-click either *setup.exe* (standalone version) or *SecurityCenterWebSetup.exe* (web version), and click **Run as administrator**.
The InstallShield Wizard opens.

NOTE: Only the standalone installer is illustrated in this procedure.

2 On the *Choose Setup Language* page, select the language of the InstallShield Wizard, and click **Next**.

3 On the welcome page, click **Next**.

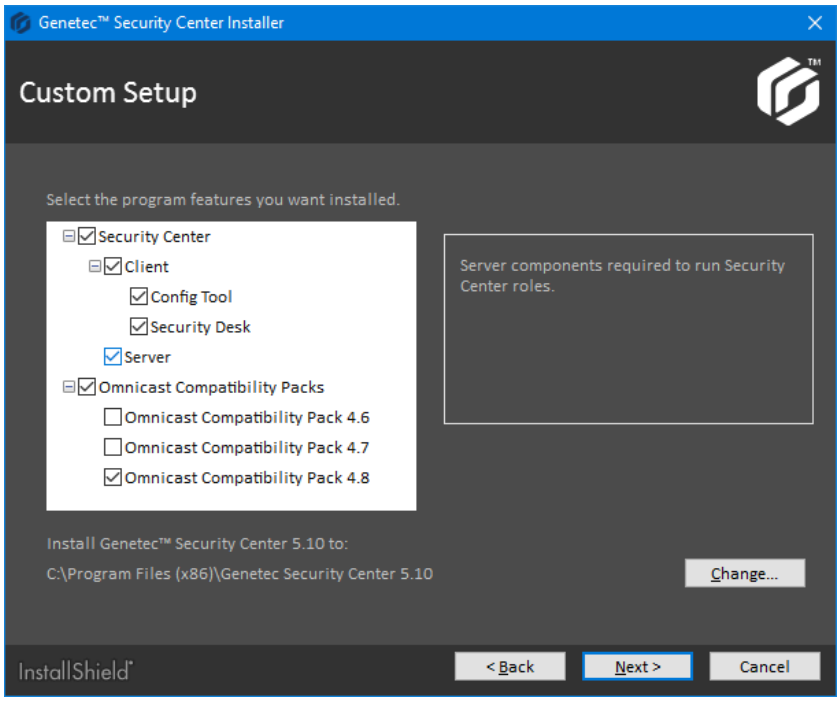


Links to relevant Security Center information are provided.

4 On the *License Agreement* page, read the terms in the *Software License Agreement*, select **I accept the terms in the license agreement**, and then click **Next**.

If you are upgrading from a previous version, a *Backward Compatibility* notice opens. Ensure that you understand the backward compatibility requirements before proceeding.

5 On the *Custom Setup* page, select the Security Center features to install, specify the destination folder, and then click **Next**.



You must select **Server** from the list. All other features are optional.

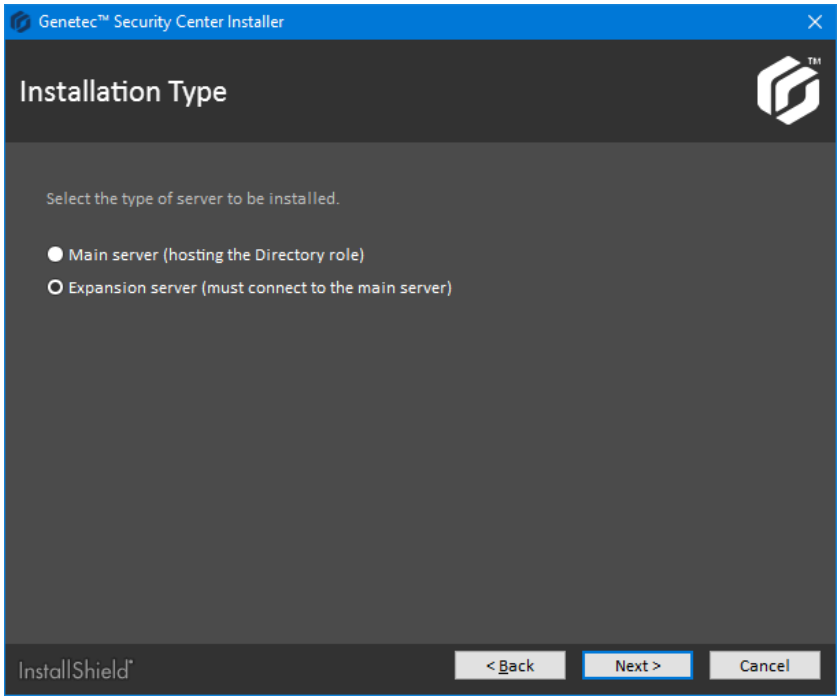
For the destination folder, you can only change the *root folder* where the *Genetec Security Center 5.10* folder is created. On a 64-bit machine, the default root folder is *C:\Program Files (x86)*.

6 On the *Genetec™ Security Center Language Selection* page, select the user interface language for Security Center applications, and click **Next**.

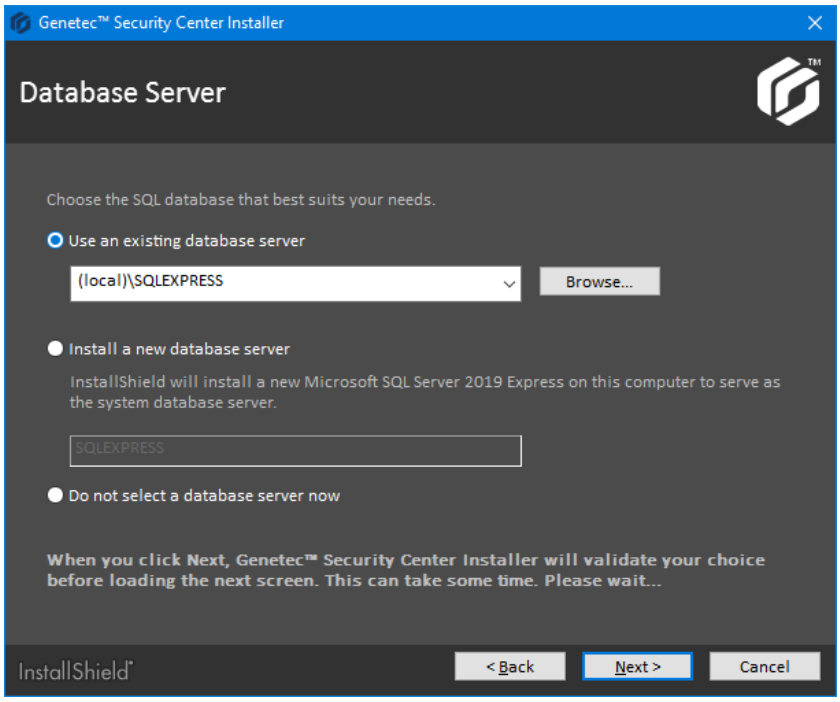
NOTE: Online help for Security Center applications is not available in all languages. For language availability, see the *Security Center Release Notes*.

TIP: After installing Security Center, you can change the user interface language with the *Language Tool* found in the Genetec™ Security Center program group in the Start menu.

7 On the *Installation Type* page, select **Expansion server**, and click **Next**.



8 On the *Database Server* page, select an SQL database, if required, and click **Next**.



The following options are available:

- **Use an existing database server:** Selects an existing Microsoft SQL Server instance on this machine, or another server.

BEST PRACTICE: Replace (local) with either the computer name or hostname, and port, if required.

For example: DB_SERVER.GENETEC.COM,1433\SQLEXPRESS

You must use a computer name or hostname if you are configuring the Directory for load balancing. For more information on load balancing, see the *Security Center Administrator Guide*.

If you are upgrading from a supported version of Security Center, the installer automatically upgrades all databases that your system requires.

If you are using an old version of SQL Server Express, you get the option to upgrade your database server to SQL Server 2019 Express Edition if the following conditions are met:

- You are running a version of Windows that supports SQL Server 2019 Express Edition. This means the 64-bit version of Windows 10 or Windows Server 2016 or later.
- Your current version of SQL Server is upgradable to SQL Server 2019 Express Edition. This means one of the following versions:
  - SQL Server 2012 SP4 Express, version 11.0.7001.0 or later
  - SQL Server 2014 SP2 Express, version 12.0.5000.0 or later
  - SQL Server 2016 Express, version 13.0.1601.5 or later
  - SQL Server 2017 Express, version 14.0.1000.169 or later

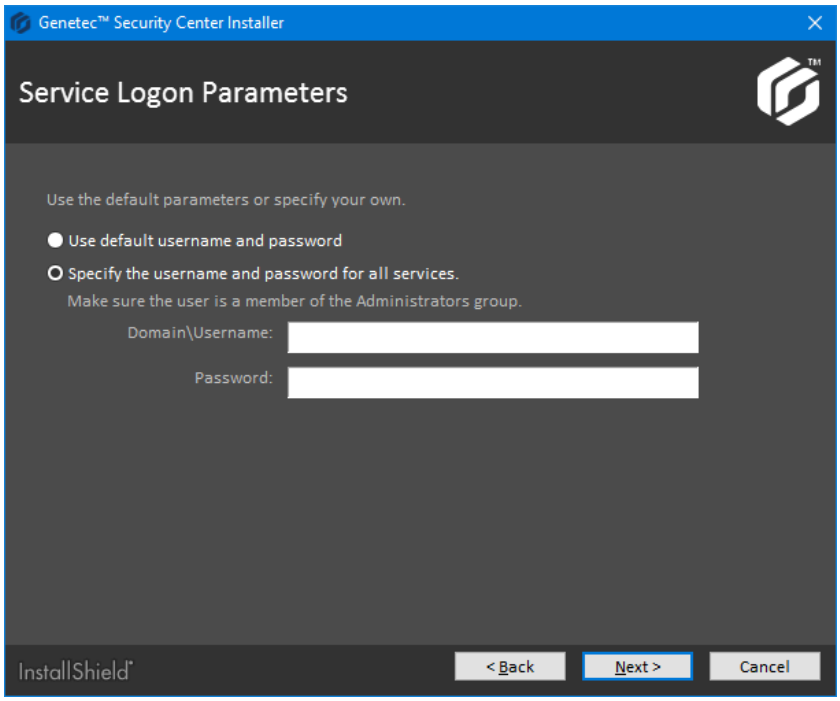
- **Install a new database server:** Installs Microsoft SQL Server 2019 Express Edition on this computer. You must choose a database server name. The default is SQLEXPRESS.

  NOTE: The database server name is not case-sensitive, but it must meet all of the following criteria:

  - It cannot be the same name as an existing SQL instance on your server.
  - It cannot match any of the SQL Server reserved keywords, such as DEFAULT, PRIMARY, and so on.
  - It cannot be longer than 16 characters.
  - The first character of the instance name must be a letter or an underscore (_). Acceptable letters are defined by the Unicode Standard 2.0, including Latin characters a-z and A-Z, and letter characters from other languages.
  - Subsequent characters can be letters defined by the Unicode Standard 2.0, decimal numbers from Basic Latin or other national scripts, the dollar sign ($), or an underscore (_).
  - It cannot contain spaces or the following characters: \ , : ; ' & # @

  NOTE: SQL Server 2019 Express is only supported on the 64-bit version of Windows 10 and Windows Server 2016 and later. If the version of Windows you are running is not one of these, quit the Security Center installation, download SQL Server 2014 Express SP3 from Microsoft Download Center, and install it first before installing Security Center.
- **Do not select a database server now:** Install this expansion server without a database. Roles that need a database cannot be hosted on this server. A SQL database can be added later.

9 On the *Service Logon Parameters* page, set the username and password used to run Security Center services.



a) Select one of the following options:

- **Use default name and password:** Select this option to use the LocalSystem account to run your Security Center services. The LocalSystem account has extensive privileges on the local computer, and acts as the computer on the network.
- **Specify the username and password for all services:** Select this option if you want to restrict the privileges granted to the service user. Enter a valid domain username and a strong password, and record them in a safe place. You must provide these credentials every time you upgrade your Security Center software. Use industry best practices for creating strong passwords.

  IMPORTANT: Make sure the service user is a local administrator and not a domain administrator. The service user must have sufficient rights to the local or remote database, and *Log on as service* user rights. If this server will host the Active Directory role, the specified user must also have read and write access to the Active Directory that you want the server to connect to.

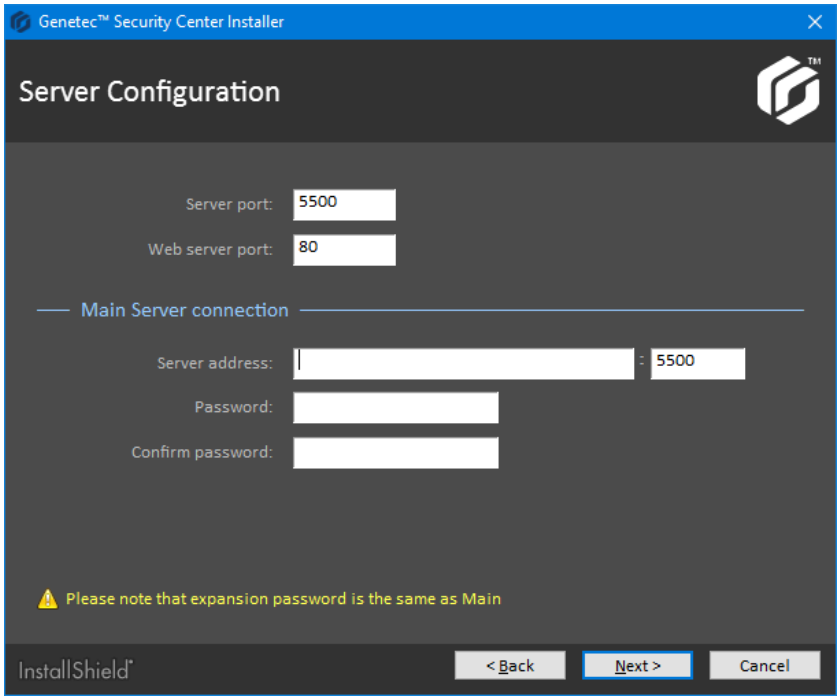
  NOTE: The service user automatically creates all the necessary databases when the system is started for the first time. For this reason, the service user needs the SQL Server role, dbCreator, for its first run. After the databases are created, you can remove the dbCreator role.

  To avoid having to grant the dbCreator role to the service user, you can create the databases required by the Security Center roles yourself, as empty databases. When the system is started for the first time, the service user only has to create the tables, without going through the database creations. For the list of Security Center roles that need a database and the minimum SQL Server roles they require, see "About connecting to SQL Server with an account that has administrative privileges" in the *Security Center Hardening Guide*.

  You can also deny the service user the dbCreator role and create the databases later. In this case, the Security Center roles that require a database will fail at system startup. You must then create the databases and restart each role manually. You can also change the service user later from Microsoft Management Console.

b) Click **Next**.

10 On the *Server Configuration* page, set the server connection parameters.



a) Complete the following fields:

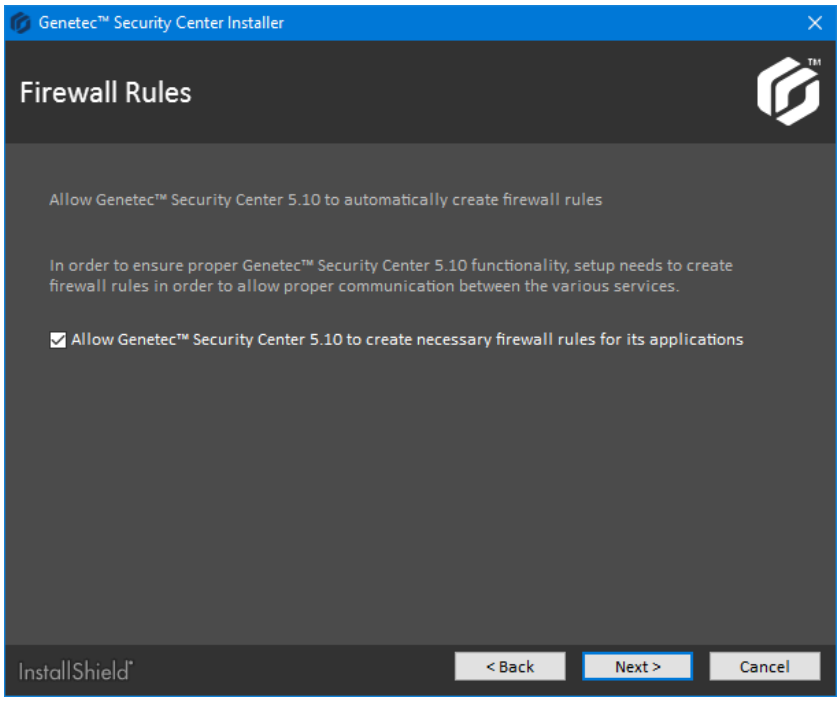
- **Server port:** The TCP port through which the servers in your system communicate.
- **Web server port:** The HTTP port that is used for the web-based Server Admin. If you change the default port, the Server Admin address must include the port number in the URL. For example, *http://computer:port/Genetec* instead of *http://computer/Genetec*. The link to Server Admin, accessible through Start menu, automatically includes this port.

  CAUTION: Watch out for conflicts with other software, such as a Skype, running on the server that might use port 80.
- **Server address:** The hostname or IP address and port used to connect to the main server.

  If you changed the default port number (5500) of the main server, enter the correct number here.
- **Password/Confirm password:** Enter and confirm the main server password.

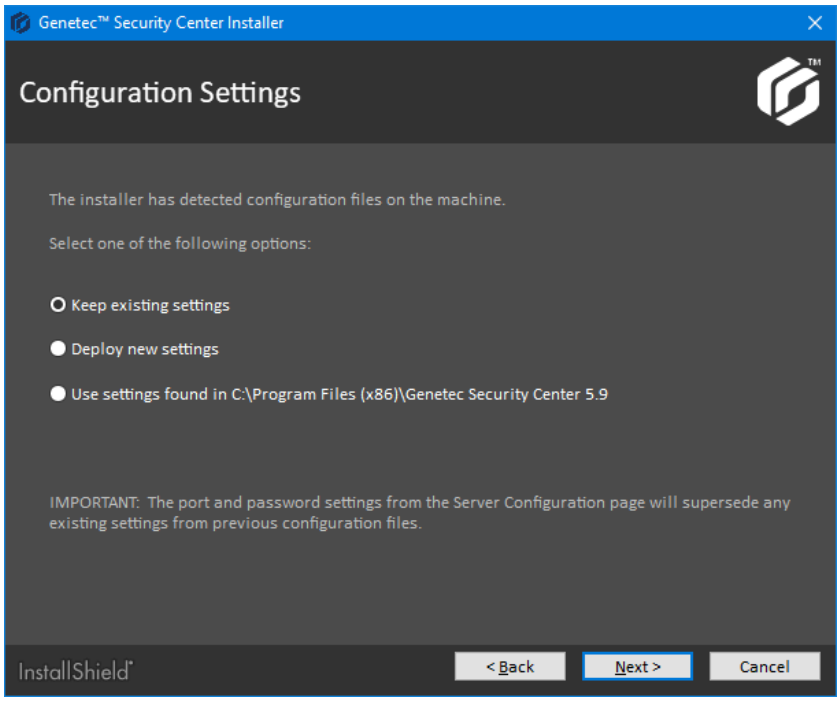
b) Click **Next**.

11 On the *Firewall Rules* page, grant the installer permission to automatically configure the Windows Firewall for Security Center, and click **Next**.



NOTE: This option only affects the Windows Firewall. After installation, you must also configure the required ports on other firewalls that control Security Center communication.

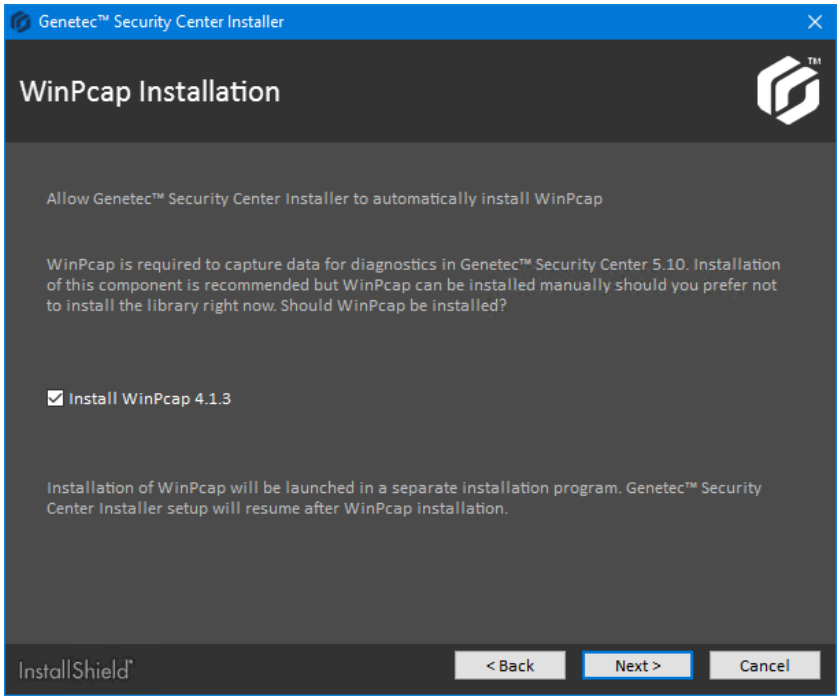
12 If old configuration files (*ConfigurationFiles*.gconfig*) are detected on your computer, you have the option to select which configuration to use. This step is skipped if you are upgrading your system.



- **Keep existing settings:** Use the existing configuration files detected for an older release of the current major version (5.10). This option is hidden if Security Center 5.10 was never installed on this computer.
- **Deploy new settings:** Disregard any existing configuration files you might have on your computer and install the default configuration files for the version you are installing.
- **Use settings found in <Security Center Installation Folder>:** Use the configuration files found in an older Security Center installation folder. This option is only available if an older major version of Security Center is detected.

- If WinPcap 4.1.3 is not installed, the *WinPcap Installation* page opens.
- If WinPcap 4.1.3 is already installed, the *Security Settings* page opens.

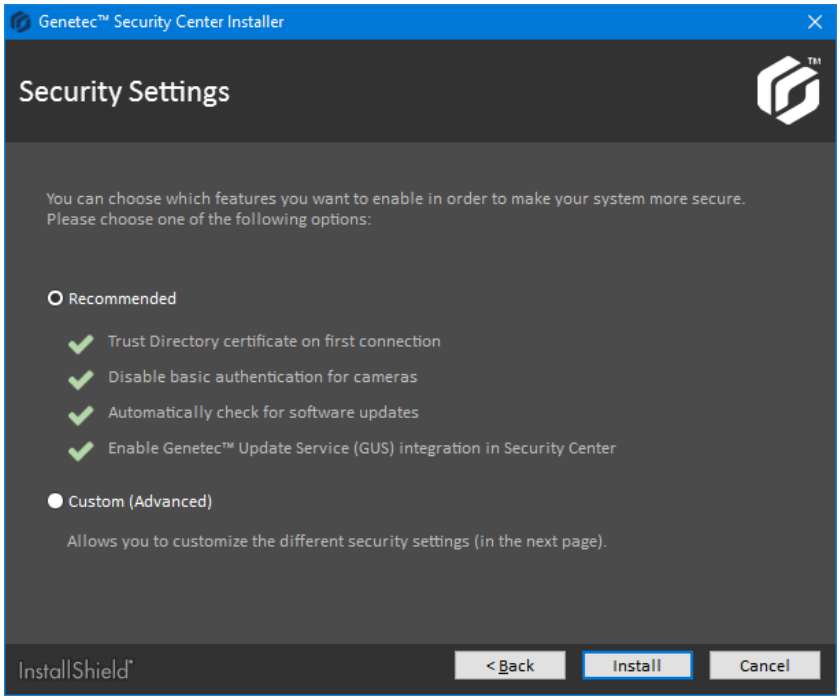
13 On the *WinPcap Installation* page, select **Install WinPcap**, if required, and click **Next**.



WinPcap captures diagnostic data for units and other services in Security Center. If you require assistance, this data can help Genetec™ technical support troubleshoot your issue.

WinPcap can be installed later.

14 On the *Security Settings* page, configure features to make your system more secure.

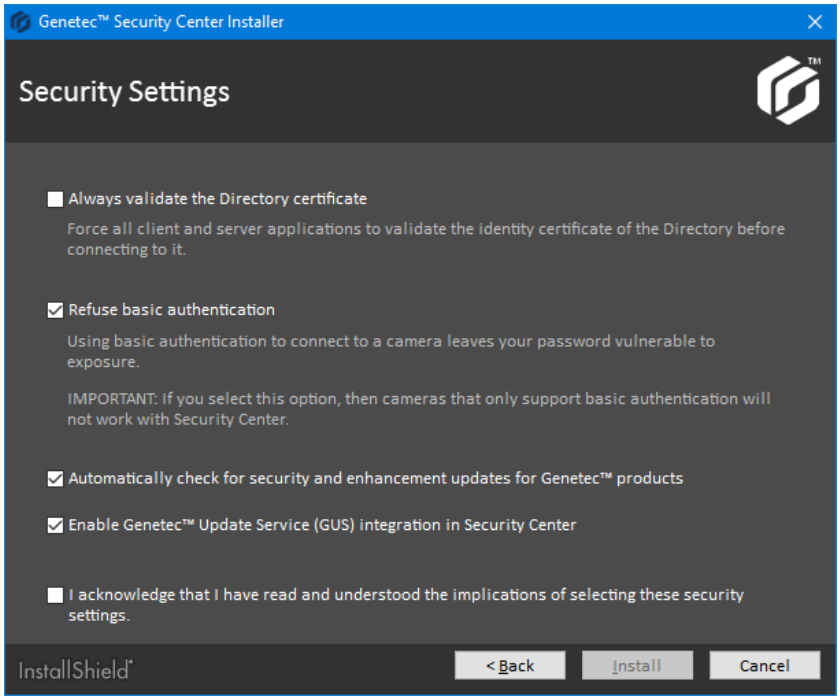


- Select **Recommended** to set the default security settings, and click **Install** to start the installation.

  The recommended security settings are:

  - If the certificate is self-signed, whitelist the *identity certificate* of the first Directory server this machine connects to.
  - Disable basic access authentication for cameras in favor of the more secure digest access authentication.
  - Automatically check for software updates.
  - Enable *Genetec™ Update Service (GUS)* integration in Security Center.
- Select **Custom (Advanced)** to configure the security settings, and click **Next**.

15 If you selected **Custom (Advanced)**, configure the security settings.



a) Configure the following settings:

- **Always validate the Directory certificate:** Select this option to force all client and server applications on the current machine to validate the identity certificate of the Directory before connecting to it.

  BEST PRACTICE: If you enable *Directory authentication*, it is best to use a certificate issued by a trusted certificate authority (CA). Otherwise, the first time this computer connects to the Directory, the user is prompted to confirm the identity of the Directory server.

  For more information on Directory authentication, see the *Security Center Administrator Guide*.
- **Turn off basic authentication:** Basic access authentication for cameras is turned off by default to prevent camera credentials from being compromised when the Archiver connects to a video unit.

  IMPORTANT: When this option is selected, cameras that only support basic access authentication will not work.

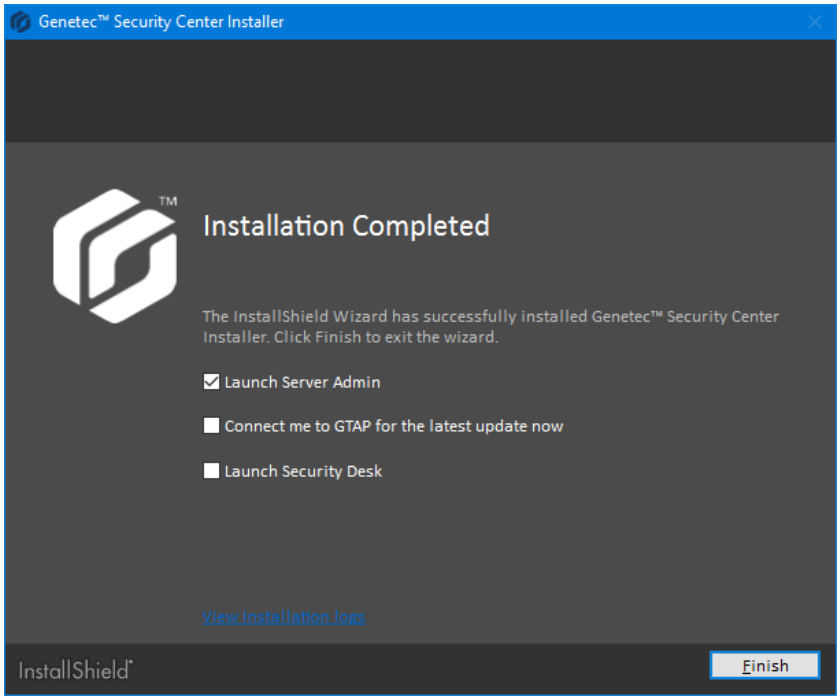
  TIP: Most recent video unit models support digest access authentication. If you are not sure whether your cameras support *digest* or not, leave the default setting as is. After installation, if some cameras do not work, you can always turn basic access authentication on again.
- **Automatically check for security and enhancement updates for Genetec™ products:** Select this option to allow GUS to automatically check for updates of all installed Genetec™ products.
- **Enable Genetec™ Update Service (GUS) integration in Security Center:** Enable this option to make GUS available in Config Tool.

b) Select **I acknowledge that I have read and understood the implications of selecting these security settings**, and click **Install** to start the installation.

16 If you chose to install WinPcap 4.1.3, follow the *WinPcap 4.1.3 Setup Wizard* that opens.

a) On the *Installation options* page, select **Automatically start the WinPcap driver at boot time**.
b) Click **Install**.

17 On *Installation Completed* page, select the required post-installation options, and click **Finish**.



If you selected **Launch Server Admin**, Server Admin opens in a browser window. Before using Security Center, you must connect to Server Admin and activate your product license.

If you selected **Connect me to GTAP for the latest updates now** and your machine has Internet access, you are connected to the Genetec™ *Product Download* page on GTAP. You need a username and a password to log in.

If you selected **Launch Security Desk**, Security Desk opens automatically. However, you cannot log on to the Directory until your product license is activated.

If you get a message asking you to restart your computer, click **Yes**.

If you get a warning message that the SQL Server 2019 telemetry service cannot be disabled, disable it manually.

The Security Center expansion server is now installed.

After you finish

Connect the expansion server to the main server.

Related Topics

Installing SQL Server independently of Security Center on page 28

Connecting expansion servers to the main server

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

Before you begin

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

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

To connect an expansion server to the main server:

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

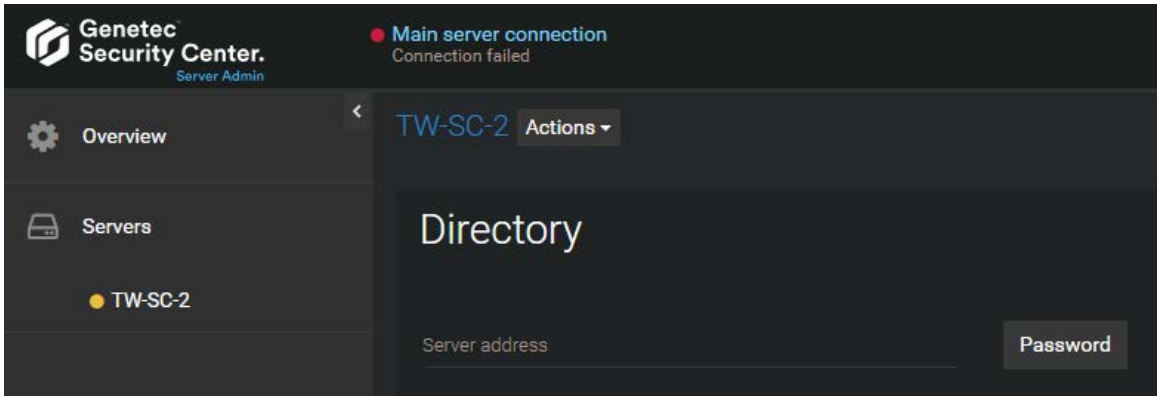
- In the address bar of your web browser, type http://computer:port/Genetec, where computer is the hostname or the IP address of your expansion server, and port is the web server port specified during the Security Center Server installation.

  You can omit the web server port if you are using the default value (80).
- If connecting to Server Admin from the local host, double-click **Genetec™Server Admin** ( ) in the *Genetec Security Center* folder in the Windows Start menu.

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

The Server Admin *Overview* page appears.

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



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

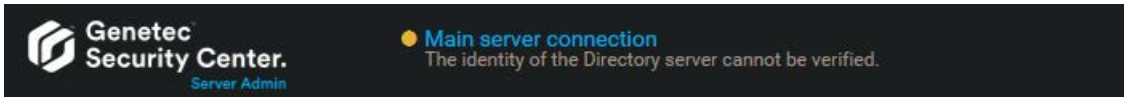
5 When prompted to restart the service, click **Yes**.

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

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

The main server is connected.

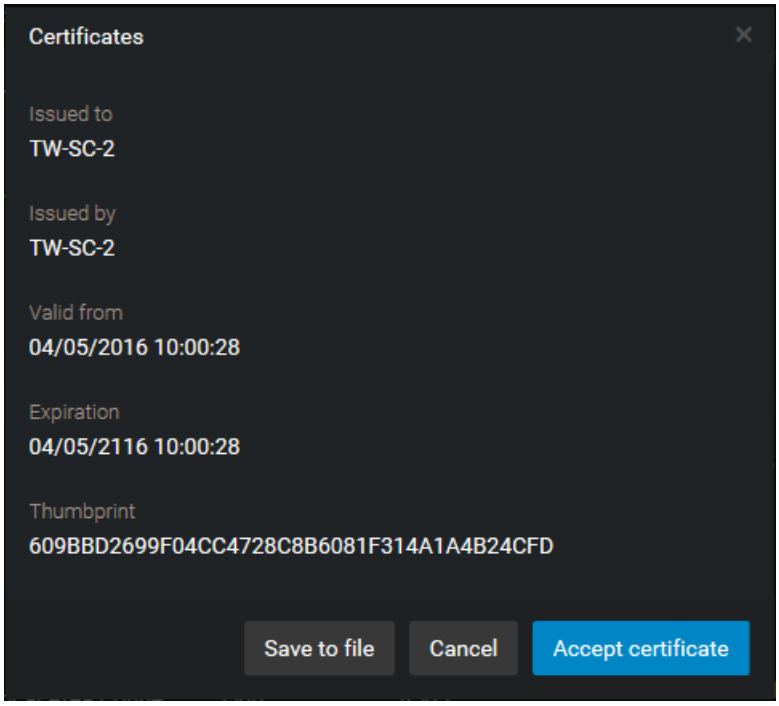
If **Always validate the Directory certificate** is set, you might see a message that the identity of the Directory server cannot be verified.



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

a) Click **Main server connection**.

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



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

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

c) Click **Save**.

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

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

The expansion server is now connected to the main server. The two servers remain connected, even when you change the certificate, on one or both of the servers, as long as the two servers are connected while the change is made.

Installing Security Center Client Software

When Security Center is up and running, you require client software to configure and use the system. A client installation includes Config Tool and Security Desk by default.

Before you begin

- Install the Security Center main server, and ensure that it is up and running.

To install Security Center client software:

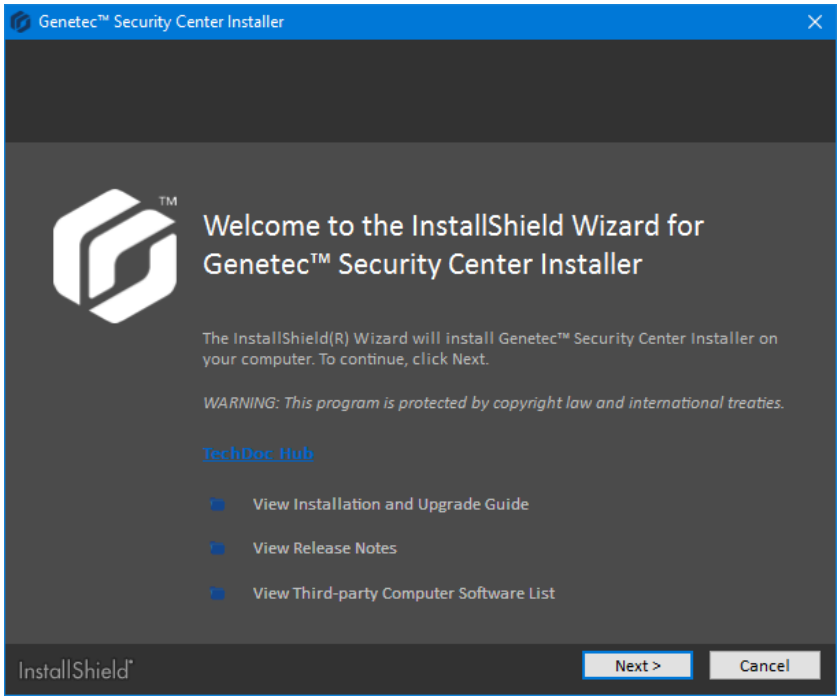
1 Right-click either *setup.exe* (standalone version) or *SecurityCenterWebSetup.exe* (web version), and click **Run as administrator**.

The InstallShield Wizard opens.

NOTE: Only the standalone installer is illustrated in this procedure.

2 On the *Choose Setup Language* page, select the language of the InstallShield Wizard, and click **Next**.

3 On the welcome page, click **Next**.

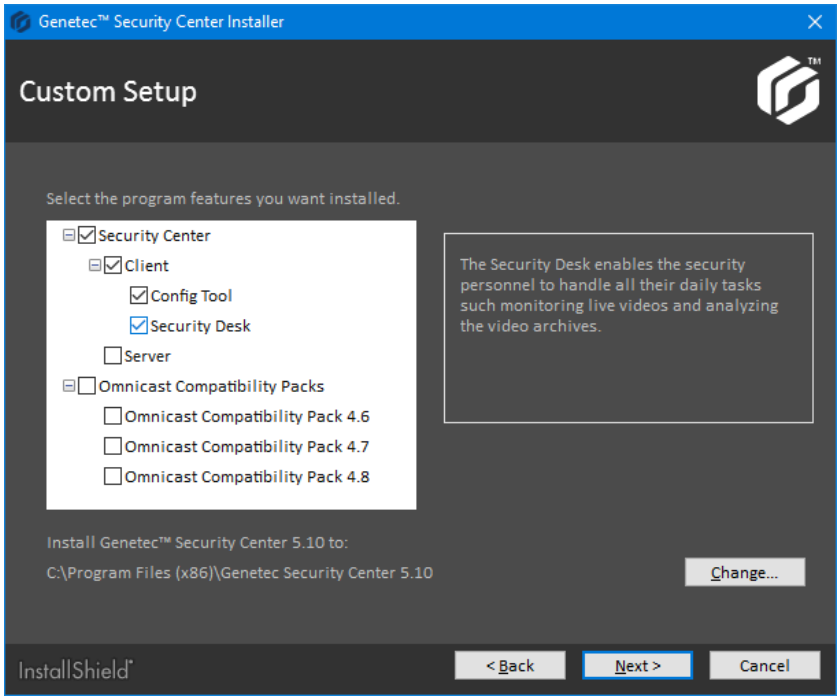


Links to relevant Security Center information are provided.

4 On the *License Agreement* page, read the terms in the *Software License Agreement*, select **I accept the terms in the license agreement**, and then click **Next**.

If you are upgrading from a previous version, a *Backward Compatibility* notice opens. Ensure that you understand the backward compatibility requirements before proceeding.

5 On the *Custom Setup* page, select the Security Center features to install, specify the destination folder, and then click **Next**.



You must select **Config Tool**, **Security Desk**, or both from the list. All other features are optional.

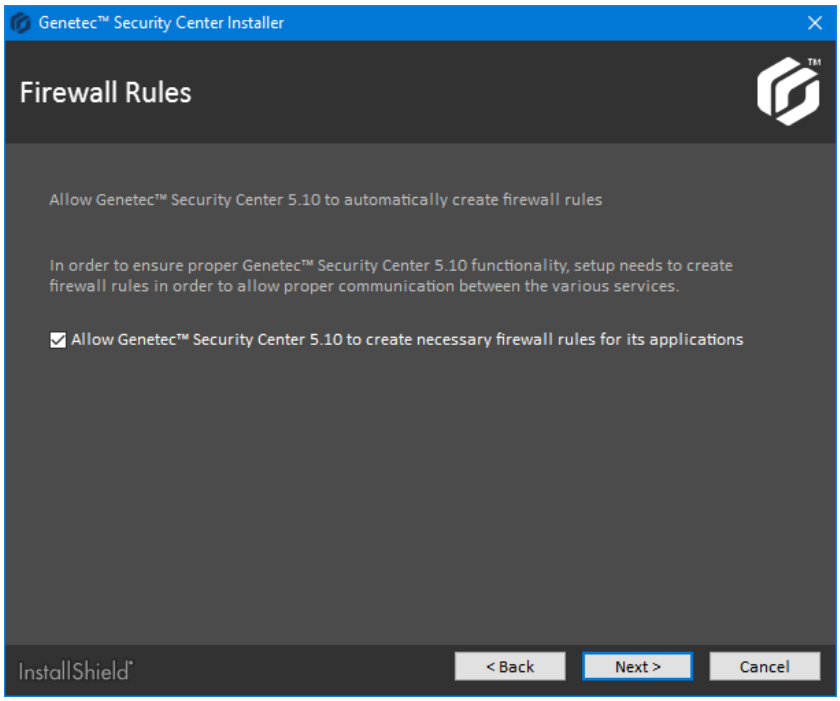
For the destination folder, you can only change the *root folder* where the *Genetec Security Center 5.10* folder is created. On a 64-bit machine, the default root folder is *C:\Program Files (x86)*.

6 On the *Genetec™ Security Center Language Selection* page, select the user interface language for Security Center applications, and click **Next**.

NOTE: Online help for Security Center applications is not available in all languages. For language availability, see the *Security Center Release Notes*.

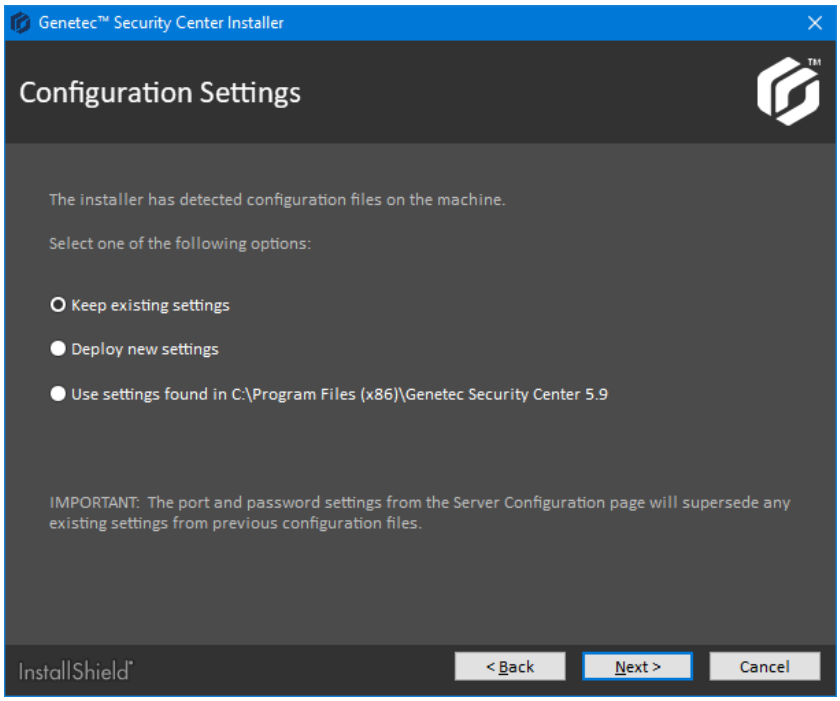
TIP: After installing Security Center, you can change the user interface language with the *Language Tool* found in the Genetec™ Security Center program group in the Start menu.

7 On the *Firewall Rules* page, grant the installer permission to automatically configure the Windows Firewall for Security Center, and click **Next**.



NOTE: This option only affects the Windows Firewall. After installation, you must also configure the required ports on other firewalls that control Security Center communication.

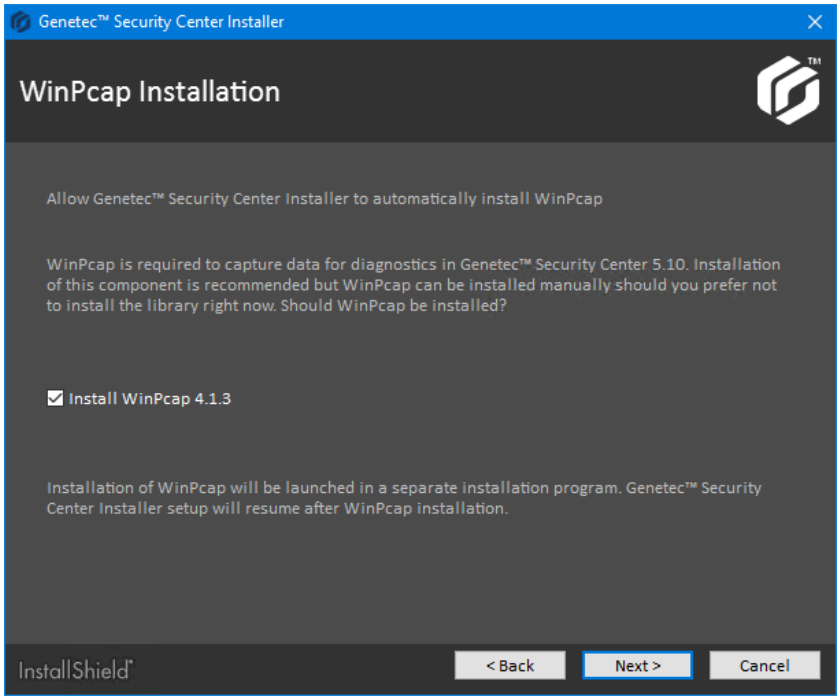
8 If old configuration files (*ConfigurationFiles*.gconfig*) are detected on your computer, you have the option to select which configuration to use. This step is skipped if you are upgrading your system.



- **Keep existing settings:** Use the existing configuration files detected for an older release of the current major version (5.10). This option is hidden if Security Center 5.10 was never installed on this computer.
- **Deploy new settings:** Disregard any existing configuration files you might have on your computer and install the default configuration files for the version you are installing.
- **Use settings found in <Security Center Installation Folder>:** Use the configuration files found in an older Security Center installation folder. This option is only available if an older major version of Security Center is detected.

- If WinPcap 4.1.3 is not installed, the *WinPcap Installation* page opens.
- If WinPcap 4.1.3 is already installed, the *Security Settings* page opens.

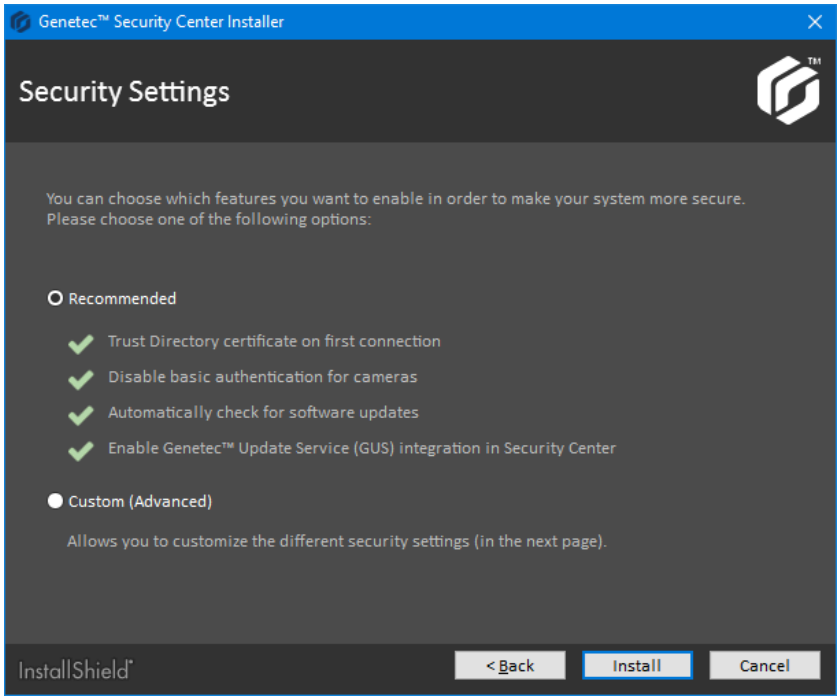
9 On the *WinPcap Installation* page, select **Install WinPcap**, if required, and click **Next**.



WinPcap captures diagnostic data for units and other services in Security Center. If you require assistance, this data can help Genetec™ technical support troubleshoot your issue.

WinPcap can be installed later.

10 On the *Security Settings* page, configure features to make your system more secure.

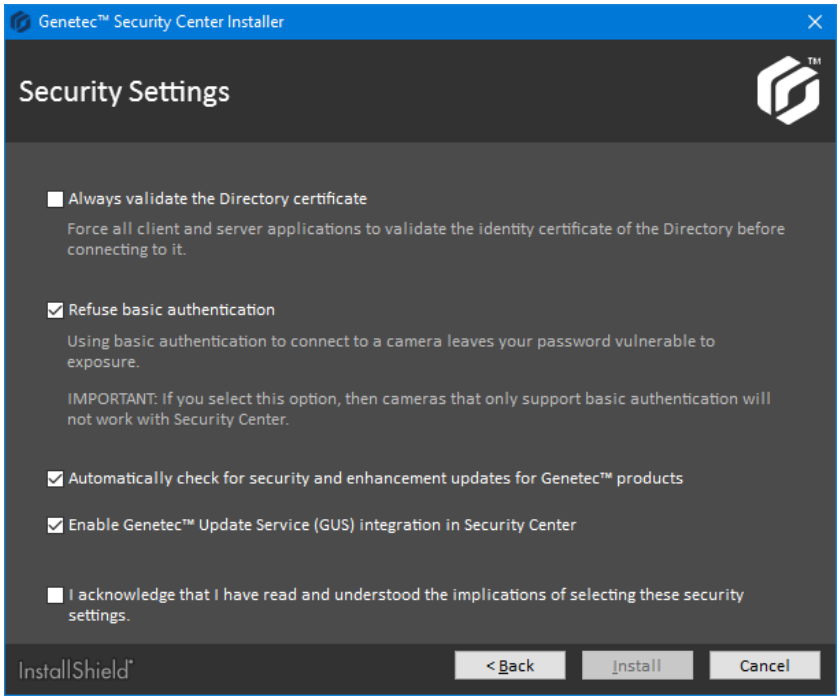


- Select **Recommended** to set the default security settings, and click **Install** to start the installation.

  The recommended security settings are:

  - If the certificate is self-signed, whitelist the *identity certificate* of the first Directory server this machine connects to.
  - Disable basic access authentication for cameras in favor of the more secure digest access authentication.
  - Automatically check for software updates.
  - Enable *Genetec™ Update Service (GUS)* integration in Security Center.
- Select **Custom (Advanced)** to configure the security settings, and click **Next**.

11 If you selected **Custom (Advanced)**, configure the security settings.



a) Configure the following settings:

- **Always validate the Directory certificate:** Select this option to force all client and server applications on the current machine to validate the identity certificate of the Directory before connecting to it.

  BEST PRACTICE: If you enable *Directory authentication*, it is best to use a certificate issued by a trusted certificate authority (CA). Otherwise, the first time this computer connects to the Directory, the user is prompted to confirm the identity of the Directory server.

  For more information on Directory authentication, see the *Security Center Administrator Guide*.
- **Turn off basic authentication:** Basic access authentication for cameras is turned off by default to prevent camera credentials from being compromised when the Archiver connects to a video unit.

  IMPORTANT: When this option is selected, cameras that only support basic access authentication will not work.

  TIP: Most recent video unit models support digest access authentication. If you are not sure whether your cameras support *digest* or not, leave the default setting as is. After installation, if some cameras do not work, you can always turn basic access authentication on again.
- **Automatically check for security and enhancement updates for Genetec™ products:** Select this option to allow GUS to automatically check for updates of all installed Genetec™ products.
- **Enable Genetec™ Update Service (GUS) integration in Security Center:** Enable this option to make GUS available in Config Tool.

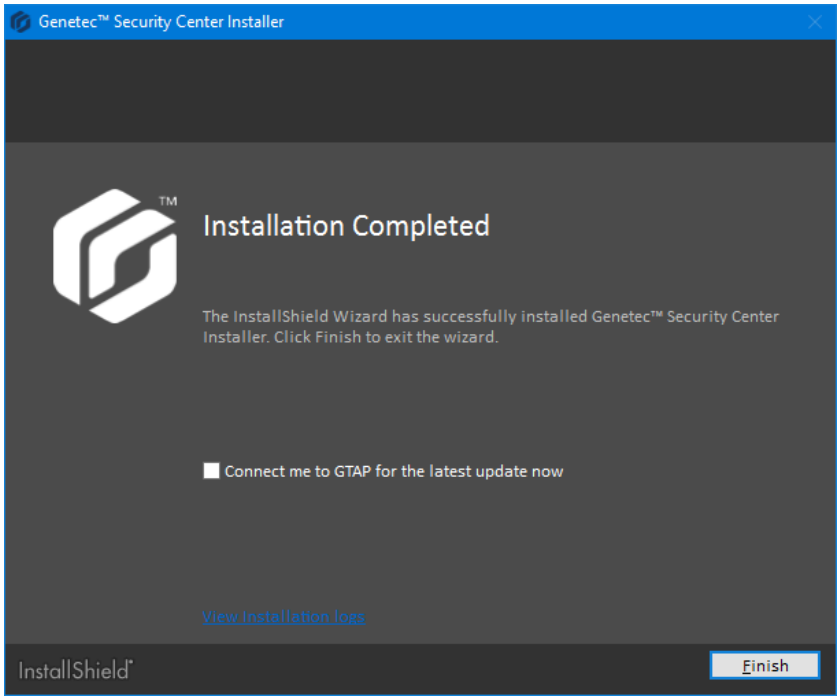
b) Select **I acknowledge that I have read and understood the implications of selecting these security settings**, and click **Install** to start the installation.

12 If you chose to install WinPcap 4.1.3, follow the *WinPcap 4.1.3 Setup Wizard* that opens.

a) On the *Installation options* page, select **Automatically start the WinPcap driver at boot time**.

b) Click **Install**.

13 On *Installation Completed* page, select the required post-installation options, and click **Finish**.



Uninstalling Security Center

If you need to completely remove Security Center from your system, including all data, configuration settings, and video archives, prior to re-installing it, you must perform a series of steps.

What you should know

CAUTION: If you are uninstalling a previous version of Security Center Client and a Security Center 5.10 Server is installed on the same computer, the server component is also uninstalled. You will need to reinstall the Security Center Server.

To uninstall Security Center from your system:

1 Take note of the following:

- The service logon username and password for all your servers.
- The name of the database server used to manage the Directory database.

2 In Server Admin, backup the Directory database by clicking **Backup/Restore** under the Database section in the **Directory** tab.

3 Backup the database of each role configured in the system.

4 Close all Security Center applications (Security Desk, Config Tool, and Server Admin).

5 Run *services.msc* in Windows, and stop the Genetec™ Server service.

6 From the Windows Control Panel, open the *Programs and Features* applet.

7 In the *Programs and Features* window, right-click **Genetec System Availability Monitor Agent**, and then click **Uninstall** > **Yes**.

8 Right-click **Genetec Update Service**, and then click **Uninstall** > **Yes**.

9 Right-click **Genetec Security Center Installer**, and then click **Uninstall**.

10 In the *Remove the Program* dialog box, click **Remove**.

11 When the message **Uninstallation Completed** appears, click **Finish**.

Genetec™Security Center 5.10, the installer program, and all Omnicast™ Compatibility Packs, are removed.

12 (Optional) If you do not want to keep database information, including video archives, uninstall the SQL Server.

13 In the Windows **Start** menu, type `regedit`, and then press **ENTER**.

14 In the *Registry Editor*, export the following keys to keep them for future reference, and then delete them from the registry.

- On 32-bit systems: *HKEY_LOCAL_MACHINE\SOFTWARE\Genetec*
- On 64-bit systems: *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Genetec*

15 Delete the cache data.

- C:\ProgramData\Genetec Update Service\SharedGpacks
- C:\Users\<username>\AppData\Local\Genetec Security Center 5.10\VideoCache

16 Make a copy of the following folders if you want to keep them for future reference, and then delete them.

- On 32-bit systems: C:\Program Files\Genetec Security Center 5.10
- On 64-bit systems: C:\Program Files (x86)\Genetec Security Center 5.10
- On all systems:
  - C:\ProgramData\Genetec Security Center
  - C:\ProgramData\Genetec Security Center 5.10
  - C:\ProgramData\Genetec Update Service
  - C:\ProgramData\AppData\Local\Genetec Security Center 5.10
  - C:\Users\<username>\AppData\Local\Genetec Inc
  - C:\Users\<username>\AppData\Local\Genetec Security Center 5.10
  - C:\Users\<username>\AppData\Local\IsolatedStorage

    NOTE: You cannot delete this folder if other applications are using it.

17 (Optional) Delete the video archives (G64 files) created by the Archiver.

IMPORTANT: Do not delete the video archives if you keep the Archiver database.

Completing the installation process

After you install Security Center, there is a series of steps you can take to check the status of your system.

Before you begin

Install Security Center.

To complete the installation process:

1 If you chose to create the databases yourself, create them now.

If you use default database names, the service user can connect to them automatically. The default database names are the roles name without the spaces, with the following exceptions:

- The default database name for the ALPR Manager role is LPRManager.
- The default database name for the Record Caching Service role is RecordCache.

If your database names are different from the default ones, you must change the setting in Server Admin for the Directory database and in the roles' *Resources* page in Config Tool for the role databases.

IMPORTANT: Delete the default databases before creating new ones. Use a different database name for each role to avoid confusion.

2 Log on to Server Admin, click **Overview**, and check the following:

- ☐ Directory database is connected ( ).
- ☐ Directory is ready ( ).
- ☐ License is valid ( ) and all required features are present.
- ☐ All installed servers are connected ( ).
- ☐ SMA contract number is confirmed with expiration date.
- ☐ Mail server (SMTP) is configured.
- ☐ Genetec™ Watchdog is configured for email notifications and recipients.

3 Under *Servers* ( ), click the main server ( ), and check the following:

- ☐ Automatic Directory database backup is enabled and configured.

  NOTE: If the database is local to the Directory server, check under **Database properties** ( ). If the database is hosted on an external machine, confirm that automatic backup is configured on that machine.
- ☐ Retention periods for various types of data are properly configured.

  NOTE: Keep in mind the database size when SQL Express is being used. A long retention period might cause database size issues if your system generates a lot of events.
- ☐ Data collection policy is properly configured.
- ☐ Correct network interface card (NIC) is selected.
- ☐ Server authentication certificate is configured.

4 Under *Servers* ( ), click each expansion server, and check the following:

- ☐ Correct NIC is selected.
- ☐ Server authentication certificate is configured.

5 Log on to Security Center through Config Tool, open the *Network view* task, and check the following:

- ☐ All servers are online with no health issues.
- ☐ Proper network protocol is in use based on network capabilities.
- ☐ Public addresses are configured properly where needed.
- ☐ Network address and subnet mask correspond to the actual network.

For more information, see "About the Network view" in the *Security Center Administrator Guide*.

6 Open the *System* task, click **Roles**, and check the following:

- ☐ Roles are online with no health issues (not displayed in a yellow warning state).
- ☐ Roles are connected to their database (when applicable).
- ☐ Automatic backup is configured for role databases (if required).

  NOTE: If a database is local to the server that hosts the role, check under **Resources** > **Backup/ Restore** (). If the database is hosted on an external machine, confirm that automatic backup is configured on that machine.
- ☐ NIC is selected for each role, and in the case of the Media Router, for each redirector.
- ☐ Whenever role failover is configured for roles other than the Archiver and the Directory, the role database is hosted on a third computer.

7 Open the *User management* task, and ensure that the *Admin* user has a password.

8 Check that you can log on to Security Center through Security Desk.

If that doesn't work, you can troubleshoot the main server.

9 On all Security Center servers, check the following:

- ☐ Unused NICs are disabled.
- ☐ NIC binding order is properly configured.

  For more information, see "Network cards order and prioritization" in Best practices for configuring network cards on your servers for Security Center.
- ☐ Server is not a domain controller.
- ☐ Windows update is set to not automatically install.
- ☐ Windows clock is synchronized to a time source.

  For more information, read our online articles on time synchronization.
- ☐ No unwanted application is running.
- ☐ System drive has sufficient free space.
- ☐ CPU memory and usage are under acceptable thresholds.

  Recommended CPU usage is under 85%. Refer to Microsoft documentation for memory usage thresholds.
- ☐ Windows storage indexing is disabled on all drives used for video archiving.
- ☐ Windows Event Viewer is free of critical errors or restarts.
- ☐ Antivirus software is configured properly and all exclusions are made.

  For more information, see Best practices for configuring antivirus software for Security Center.

After you finish

- Read and follow our Best practices for configuring Windows and Security Center.

- Depending on your deployment requirements, complete your system configuration for:
  - User management (users, user groups, and partitions)
  - Schedules (follow our best practices for naming conventions)
  - Video surveillance and management
  - Access control
  - License Plate Recognition

For more information about deploying your system, see the *Security Center Administrator Guide*.

For information about how to enhance the security of your Genetec™ Security Center system, see the Security Center Hardening Guide.

2

Upgrading to Security Center 5.10

This section includes the following topics:

- "Supported upgrade paths to Security Center 5.10.2.0" on page 82
- "Preparing to upgrade from an earlier release of Security Center 5.10" on page 83
- "Upgrading from an earlier release of Security Center 5.10" on page 84
- "Pre-upgrade checklist for upgrading from an earlier major version of Security Center" on page 85
- "Backing up databases" on page 92
- "Upgrading Security Center 5.7, 5.8, or 5.9 to 5.10" on page 95
- "Upgrading Security Center from 5.4, 5.5, or 5.6 to 5.10" on page 96
- "Upgrading Directory failover systems from an earlier major version" on page 97
- "What Security Center client features are available when the Directory service is offline?" on page 104
- "Upgrading the Security Center main server" on page 105
- "Upgrading expansion servers in Security Center" on page 114
- "Upgrading Security Center Client" on page 118
- "Upgrading the Security Center Directory database" on page 119
- "Upgrading Security Center with Global Cardholder Synchronizer roles" on page 122

Supported upgrade paths to Security Center 5.10.2.0

Security Center supports direct upgrades and two-step upgrades to the latest software version. When upgrading, it is important to know your required upgrade path.

Direct upgrades

A direct upgrade to Security Center 5.10.2.0 is supported from the following software versions:

- Security Center 5.9.x.y
- Security Center 5.8 GA and 5.8.1.x
- Security Center 5.7 GA and all SRs

Two-step upgrades

A two-step upgrade to Security Center 5.10.2.0 is supported from the following software versions:

- Security Center 5.6 GA and all SRs
- Security Center 5.5 GA and all SRs
- Security Center 5.4 GA and all SRs

To maintain backward compatibility during a two-step upgrade, supported systems are first upgraded to the latest release of Security Center 5.7 and then directly upgraded to Security Center 5.10.2.0.

Older version upgrades

To upgrade Security Center 5.3 and earlier, contact your representative of Genetec Inc..

Omnicast™ 4.x

To upgrade Omnicast™ 4.x systems, follow a three-step procedure:

- Omnicast™ 4.8 SR8 → Security Center 5.5 SR5 CU15 → Security Center 5.8 (latest) → Security Center 5.10.2.0

If you are using a version of Omnicast™ earlier than 4.8 SR8, upgrade your system to version 4.8 SR8 first. For more information, see the Omnicast™ Migration Guide 5.5.

More information

For more information, see our Product Lifecycle page on GTAP.

Preparing to upgrade from an earlier release of Security Center 5.10

If you need to upgrade from an earlier release of Security Center 5.10 to 5.10.2.0, you must prepare the following.

What you should know

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.

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.

To prepare to upgrade from an earlier release of Security Center 5.10:

- Make sure you have the following information:
  - The service logon username and password for all your servers.
  - The name of the database server used to manage the Directory database.

  You'll have to re-enter the same values when you install Security Center Server 5.10.2.0.

Upgrading from an earlier release of Security Center 5.10

To have the latest release of Security Center 5.10, you can upgrade from an earlier minor version of 5.10 to 5.10.2.0 after you have completed the preparation steps.

Before you begin

- Understand the things you need to know and do before you upgrade.
- Back up your Directory database, and all role databases.

What you should know

You do not need to change your license when you upgrade from an earlier *minor version* of 5.10 to 5.10.2.0 because they share the same *major version*.

Previous installation choices, such as language and installation types are preserved, and the InstallShield Wizard will not ask for them again.

To upgrade from an earlier release of Security Center 5.10 to 5.10.2.0:

1. Upgrade your main server to Security Center 5.10.2.0.
2. Upgrade your expansion servers to Security Center 5.10.2.0, according to your priorities.
3. Upgrade your client workstations to Security Center 5.10.2.0, according to your priorities.

After you finish

If the file *AllowedSynchronizationConfiguration.xml* was used to set the synchronization times of your HID VertX units, the settings must be re-applied manually from Config Tool after the upgrade.

TIP: Configure one unit with the required synchronization settings, then use the copy configuration tool to set the same settings on multiple units.

Pre-upgrade checklist for upgrading from an earlier major version of Security Center

To upgrade your Security Center system from an earlier major version to 5.10.2.0, you must go through a series of preparatory steps.

- 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.
- Different versions of the Security Center clients can coexist on the same machine, but different versions of Security Center Server cannot. Not all current settings are kept if you uninstall your current software version before installing the new one.
- If the Active Directory role is on a different domain than the Active Directory it is synchronizing with, you must set up a domain trust relationship. For more information on setting up domain trust relationships, see your Microsoft documentation.

Step	Task	Additional information
Understand prerequisites and key issues		
1	Read the release notes for any known issues, limitations, and other information about the release.	• *Security Center Release Notes*.
2	Review the backward compatibility requirements for Security Center.	• Backward compatibility requirements for Security Center on page 86.
3	Make sure you have the following information: • The service logon username and password for all your servers. • The name of the database server used to manage the Directory database.	
Prepare		
4	Back up your Directory and role-specific databases to a secure location that is separate from your main server.	• Backing up databases on page 92.
5	Close all applications related to Microsoft Management Console (MMC), such as Services, Event Viewer, and so on.	These applications might lock the Security Center services and prevent them from being updated.

Step	Task	Additional information
Set up additional software and configuration as needed		
6	If you have an Active Directory role in your current system, make sure that the Windows user configured to connect to the Windows Active Directory has Read access to the *accountExpires* attribute. **CAUTION:** If the Windows user does not have Read access to the *accountExpires* attribute, all cardholders and credentials previously imported from the Windows Active Directory are deleted the next time you synchronize Security Center with your Windows Active Directory after the upgrade.	When you import users and cardholders to Security Center from a Windows Active Directory, you can set an expiration date for the imported entities by importing the standard attribute *accountExpires*. The status of the imported entity automatically changes to inactive after the specified date.

Backward compatibility requirements for Security Center

Security Center 5.10.2.0 is backward compatible with many Security Center components from the three previous major versions.

IMPORTANT: Security Center 5.10.2.0 is compatible with the three previous *major versions*. A server or workstation that is three major versions behind can connect to the 5.10.2.0 Directory, but one that is four major versions behind cannot. To retain backward compatibility when upgrading your system in stages, no part of Security Center can be more than three major versions apart. For systems that are four to six major versions behind, upgrade in two steps to maintain backward compatibility.

IMPORTANT: Adding backward compatible connections slows down the performance of the Directory. It is only recommended as a temporary solution before you are able to upgrade all servers and workstations.

The requirements for Security Center backward compatibility are as follows:

- **Upgrading to the latest version:** When upgrading, you must always upgrade the main server hosting the Directory role and Config Tool. Always upgrade each expansion server hosting a role type that is not backward compatible.
- **Using new features:** To use the new features introduced in version 5.10.2.0, upgrade your Security Center servers.
- **Role assigned to multiple servers:** If a role is assigned to multiple servers, such as in a failover configuration, all of its servers must be running the same version of Security Center.
- **Directory assigned to multiple servers:** All Directory servers must use the exact same version, meaning that all four digits of their version numbers must be the same. For example, if you upgrade to Security Center 5.10.2.0, you must upgrade all Directory servers to 5.10.2.0.

Backward compatibility between Security Center roles

Each new version of Security Center includes new role features that might not be compatible with earlier versions. The Security Center roles that are backward compatible are outlined in the following table.

IMPORTANT: All expansion servers hosting a non-backward compatible role must be upgraded to the same version as the main server hosting the Directory.

5.10 role	Backward compatible with 5.7, 5.8 and 5.9	
	Yes	No
Access Manager	✓	

5.10 role	Backward compatible with 5.7, 5.8 and 5.9	
	Yes	No
Active Directory	✓ (5.9 and later)	
ALPR Manager Formerly LPR Manager (5.9.2.0 and earlier)	✓	
Archiver	✓	
Authentication Service (OpenID & SAML2)		✓ (introduced in 5.9.2.0)
Authentication Service (WS-Federation) Formerly Active Directory Federation Services		✓
Authentication Service (WS-Trust) Formerly Active Directory Federation Services		✓
Auxiliary Archiver	✓	
Camera Integrity Monitor (hidden)	✓ (introduced in 5.8)	
Cloud Playback		✓ (introduced in 5.10.0.0)
Directory Manager		✓
Global Cardholder Synchronizer (GCS)		✓
Health Monitor		✓
Intrusion Manager	✓	
Map Manager	✓	
Media Gateway	✓	
Media Router		✓
Mobile Credential Manager		✓ (introduced in 5.10.0.0)
Mobile Server	✓ (introduced in 5.8)	
Omnicast™ Federation™	✓	
Plugin (all instances)		✓
Point of Sale		✓
Privacy Protector™ (hidden)	✓ (introduced in 5.7 SR1)	
Record Caching Service		✓ (introduced in 5.10.0.0)
Record Fusion Service		✓ (introduced in 5.10.0.0)

5.10 role	Backward compatible with 5.7, 5.8 and 5.9	
	Yes	No
Report Manager		✓
Reverse Tunnel	✓ (introduced in 5.8)	
Reverse Tunnel Server	✓ (introduced in 5.8)	
Security Center Federation™	✓	
Unit Assistant		✓ (introduced in 5.9.1.0)
Wearable Camera Manager		✓ (introduced in 5.7 SR2)
Web Server	✓	
Web-based SDK	✓	
Zone Manager	✓	

Backward compatibility with Security Center tasks

The Security Center 5.10 tasks that are backward compatible with Security Desk 5.7, 5.8 and 5.9 are summarized in the following table:

Task category	Task type	Backward compatible with Security Desk 5.7, 5.8 and 5.9	
		Yes	No
Operation	Monitoring (live and playback video)	✓	
	Maps	✓	
	Dashboards	✓ (introduced in 5.8)	
	Health dashboard	✓ (introduced in 5.8.1.0)	
	Remote		✓
	Cardholder management	✓[1]	
	Credential management	✓[1]	
	Visitor management	✓[1]	
	People counting	✓	
	Hotlist and permit editor	✓	
	Inventory management	✓	
	Mustering	✓ (introduced in 5.9.0.0)	

Task category	Task type	Backward compatible with Security Desk 5.7, 5.8 and 5.9	
		Yes	No
Alarm management	Alarm monitoring	✓	
	Alarm report	✓	
Investigation	Incidents	✓	
	Transactions		✓
	Zone activities	✓	
Investigation > Access control	Area activities	✓	
	Door activities	✓	
	Cardholder activities	✓	
	Visitor activities	✓	
	Area presence	✓	
	Time and attendance	✓	
	Credential activities	✓	
	Credential request history	✓	
	Elevator activities	✓	
	Visit details	✓[1]	
Investigation > Asset management	Asset activities		✓
	Asset inventory		✓
Investigation > ALPR	Hits	✓	
	Hits (Mutli-region)	✓	
	Reads	✓	
	Reads (Mutli-region)	✓	
	Patrol vehicle tracking	✓	
	Inventory report	✓	
	Daily usage per patrol vehicle	✓	
	Logons per patrol vehicle	✓	
	Reads/hits per day	✓	
	Reads/hits per zone	✓	

Task category	Task type	Backward compatible with Security Desk 5.7, 5.8 and 5.9	
		Yes	No
	Zone occupancy	✓	
	Parking sessions	✓	
	Parking zone activities	✓	
Investigation > Intrusion detection	Intrusion detection area activities	✓	
Investigation > Record fusion	Records		✓ (introduced in 5.10.0.0)
Investigation > Video	Archives	✓	
	Bookmarks	✓	
	Camera events	✓	
	Motion search	✓	
	Video file explorer	✓	
	Forensic search	✓	
	Security video analytics	✓ (introduced in 5.7 SR2, renamed from *KiwiVision intrusion detector* in 5.7 SR5)	
Maintenance	System status	✓	
	Audit trails	✓	
	Activity trails	✓	
	Health history	✓	
	Health statistics	✓	
	Hardware inventory	✓	
Maintenance > Access control	Access control health history	✓	
	Access control unit events	✓	
	Cardholder access rights	✓	
	Door troubleshooter	✓	
	Access rule configuration	✓	
	Cardholder configuration	✓[1]	
	Credential configuration	✓	

Task category	Task type	Backward compatible with Security Desk 5.7, 5.8 and 5.9	
		Yes	No
	I/O configuration	✓	
Maintenance > Intrusion detection	Intrusion detection unit events	✓	
Maintenance > Video	Camera configuration	✓	
	Archiver events	✓	
	Archiver statistics	✓ (introduced in 5.8)	
	Archive storage details	✓	
	Wearable camera evidence	✓ (introduced in 5.8)	

[1] Saved reports that use filters with **During the next** time intervals are not compatible with Security Desk 5.8 and earlier.

Backing up databases

You can protect your Security Center system data by regularly backing up its databases to a secure location that is separate from your main server. It is best practice to back up your databases before an upgrade.

What you should know

WARNING: Do not use virtual machine snapshots to back up your Security Center databases. During the snapshot process, all I/Os on the virtual machine are suspended, which can affect the stability and the performance of your system. We strongly recommend that you follow the procedure described below.

Depending on which role database you want to back up, the procedure can be different.

To back up a database:

1. For the Directory database without failover, perform the backup from Server Admin.
2. For the Directory database with failover, see "Backing up the Directory database with failover" in the *Security Center Administrator Guide*.
3. For any other Security Center role database, perform the backup from Config Tool, on the Resources page of the role.
4. For the Archiver and Auxiliary Archiver roles, after backing up the database, also back up the video files. For more information, see "Transferring video archives on demand" in the *Security Center Administrator Guide*.

Backing up the Directory database

You back up the Directory database from Server Admin.

Before you begin

- For non-Directory databases, see Backing up role databases on page 93.
- If the *Backup and restore* failover mode is enabled, see "Backing up the Directory database with failover" in the *Security Center Administrator Guide*.

What you should know

There are restrictions regarding the backup and restore of the Directory database when the *Mirroring* failover mode is enabled. For more information, refer to the Microsoft SQL Server Database Mirroring documentation.

To back up the Directory database:

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

   The Server Admin - *Main server* page is displayed.
3. Click **Database properties** ( ) and configure the backup settings:
   - **Destination folder:** Path to the backup folder relative to the server performing the backup. By default, databases are backed up to *C:\SecurityCenterBackup* on the database server, and configuration files are backed up to the same folder on the server hosting the role. If the folder does not exist, it will be created. To save your backups on a shared network drive, enter the path manually, and ensure that both the Genetec™ Server service user and the SQL Server service user have write access to that location.
   - **Compress backup file:** (Optional) Select this option to create a ZIP file instead of a BAK file. If you select this option, you need to unzip the backup file before you can restore it.

IMPORTANT: The **Compress backup file** option only works if the database is local to the server hosting the role.

- **Enable automatic backup:** (Optional but recommended) Select this option to enable automatic backup on a schedule. Specify the frequency and time of the backup, and how many backup files you want to keep.

  NOTE: Backup files you create manually are not counted in the number of retained backup files.

4 Click **OK** > **Save**

5 Click **Backup/Restore** ( ) and then click **Backup now**.

The backup starts and the progress is shown in the dialog box.

6 When the task is completed, click **OK**.

A backup file is created in the backup folder with the file extension BAK (or ZIP if the **Compress backup file** option was selected). The name of the file is the database name, followed by "_ManualBackup_", and the current date and time.

Backing up role databases

You back up a role database from Config Tool, from the role's *Resources* page.

Before you begin

For the Directory database, see Backing up the Directory database on page 92.

What you should know

You protect the data managed by a role by backing up its database. For the Archiver and Auxiliary Archiver roles, you also need to back up the video archive because the associated video files are not stored in the database. For more information, see "Transferring video archives on demand" in the *Security Center Administrator Guide*.

To back up a role database:

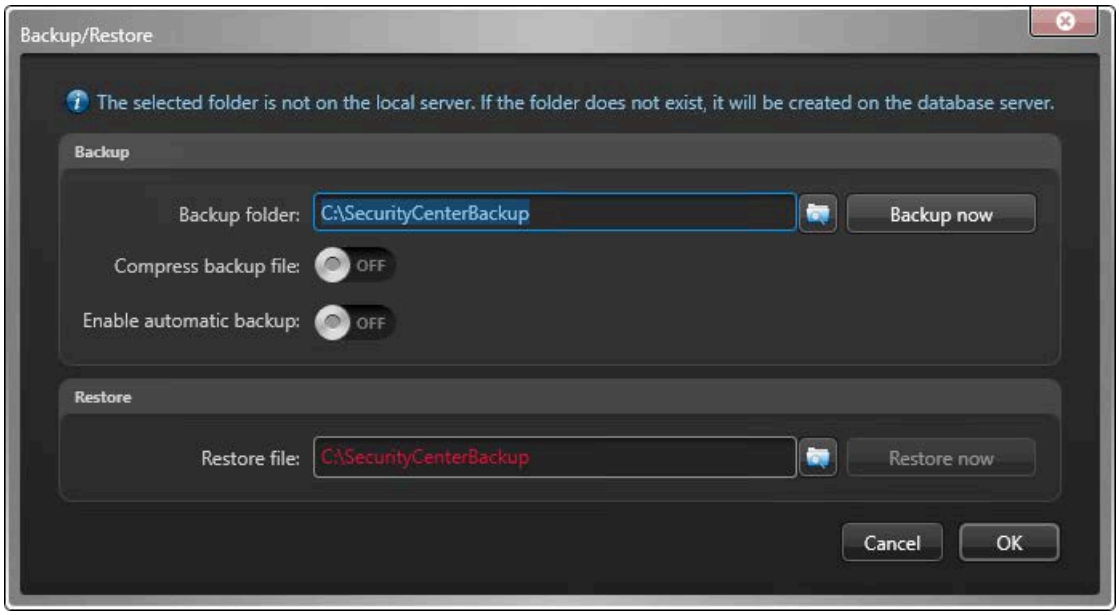
1 From the Config Tool home page, open the *System* task, and click the **Roles** view.

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

3 Click **Backup/Restore** ( ).

4 In the *Backup/Restore* dialog box, beside the **Backup folder** field, click **Select folder** (), and select the folder where you want to save the backup file.

IMPORTANT: Make sure you select a separate and secure location to store your backups.



NOTE: The location of the **Backup folder** is relative to the server performing the backup. By default, databases are backed up to *C:\SecurityCenterBackup* on the database server, and configuration files are backed up to the same folder on the server hosting the role. If the folder does not exist, it will be created. To save your backups on a shared network drive, enter the path manually, and ensure that both the Genetec™ Server service user and the SQL Server service user have write access to that location.

5 (Optional) Turn on the **Compress backup file** option to create a ZIP file instead of a BAK file.

If you select this option, you need to unzip the backup file before you can restore it.

IMPORTANT: The **Compress backup file** option only works if the database is local to the server hosting the role.

6 Click **Backup now**.

A backup file is created in the backup folder with the file extension BAK. The name of the file is the database name, followed by "_ManualBackup_", and the current date and time.

Upgrading Security Center 5.7, 5.8, or 5.9 to 5.10

To have the latest release of Security Center, you can upgrade directly from the previous three major versions to 5.10.

Before you begin

Understand the things you need to know and do before you upgrade.

What you should know

Not all tasks and roles work in backward compatibility mode. If you plan to upgrade your system in stages, make sure that the features that are essential to your operation are supported. See Backward compatibility requirements for Security Center on page 86.

NOTE: A role is upgraded only if you upgrade the server hosting the role. If you only upgrade the main server, the roles hosted on the expansion servers that are not yet upgraded work in backward compatibility mode.

IMPORTANT: If you upgrade the ALPR Manager, the Archiver it is linked to must also be upgraded. The upgraded ALPR Manager would not work if the Archiver is working in backward compatibility mode.

To upgrade from Security Center 5.7, 5.8, or 5.9 to 5.10:

1 If Omnicast™ systems were federated to your previous Security Center system, uninstall the Omnicast™ compatibility packs.

2 Do one of the following:

- If you have multiple Directory system, upgrade all your Directory servers at the same time.
- If you have a single Directory system, upgrade your main server.

3 Upgrade the rest of your system according to your priorities and schedule.

- Upgrade your expansion servers.

  IMPORTANT: If role failover is configured, upgrade all servers assigned to the same role at the same time. Failing to do so breaks your failover configuration.
- Upgrade your client workstations.

If both Security Center Client and Server are installed on the same machine, upgrade them together.

IMPORTANT: Make sure to note and apply the same settings used for your previous installation: passwords, databases, ports, general properties, and so on.

After you finish

If the file *AllowedSynchronizationConfiguration.xml* was used to set the synchronization times of your HID VertX units, the settings must be re-applied manually from Config Tool after the upgrade.

TIP: Configure one unit with the required synchronization settings, then use the copy configuration tool to set the same settings on multiple units.

Related Topics

One or more services failed to install on page 144

Upgrading Security Center from 5.4, 5.5, or 5.6 to 5.10

To maintain backward compatibility while upgrading Security Center 5.4, 5.5, or 5.6 to 5.10, you must follow a two-step upgrade process.

Before you begin

Understand the things you need to know and do before you upgrade

What you should know

Security Center 5.10.2.0 is compatible with the three previous *major versions*. A server or workstation that is three major versions behind can connect to the 5.10.2.0 Directory, but one that is four major versions behind cannot. To retain backward compatibility when upgrading your system in stages, no part of Security Center can be more than three major versions apart. For systems that are four to six major versions behind, upgrade in two steps to maintain backward compatibility.

To upgrade from Security Center 5.4, 5.5, or 5.6 to 5.10:

1 Upgrade your system to the latest Security Center 5.7 release.

You need a temporary license and the latest Security Center installation package. Ask one of our representatives.

CAUTION: There is a known issue in Security Center 5.6 where the Archiver might loose some ALPR images from the ALPR Manager. For this reason, if you have an ALPR Manager in your system and you are upgrading from Security Center 5.4 or later, upgrade to Security Center 5.7 instead of 5.6 as your first step. If you are upgrading from Security Center 5.3, after the upgrade to 5.6, continue immediately with the upgrade to 5.9 without turning your system on. If you cannot afford the downtime to perform the two-step upgrade back-to-back, contact Genetec™ Technical Assistance Center (GTAC).

a) Upgrade your main server to Security Center 5.7.

Follow the upgrade instructions found in the *Security Center Installation and Upgrade Guide 5.7 SRx*.

b) Turn your system on.

All servers and workstations that are not yet upgraded run in backward compatibility mode. This is the first stage.

c) Upgrade the rest of your system (servers and workstations) to the latest 5.7 release.

Your entire system runs in version 5.7. This is the second stage. You can split this step into as many stages as needed, depending on the number of machines you need to upgrade.

2 Upgrade your system to Security Center 5.10.

Related Topics

One or more services failed to install on page 144

Upgrading Directory failover systems from an earlier major version

Directory servers are not backward-compatible. Perform this procedure if you are upgrading Security Center with multiple Directory servers to the latest version or release.

Before you begin

- Read the *Security Center Release Notes* for important information when upgrading to Security Center 5.10.
- You need a maintenance window to upgrade all the Directory servers. This period should be scheduled at a time when it is acceptable to run the system with a minimum set of features.
- Back up the Directory database, all role databases, and configuration files.
- Make sure to note and apply the same settings in the InstallShield that you used for your previous installation: passwords, database, ports, general properties, and so on.
- The Config Tool and the Directory must be of the same version.
- If Config Tool and the Directory are on different machines, upgrade the Config Tool before you upgrade the Directory.
- Do not change the Directory failover configuration before upgrading; that is, do not remove the secondary Directory servers from the list of Directory servers.

What you should know

- During the upgrade, the Directory role is stopped. Consequently, Config Tool and most Security Desk features are not available. However, video that is displayed before the Directory service goes offline continues to be streamed in the Security Desk *Monitoring* task and saved to the Archiver. For example, video walls continue to display video streams. Access control continues to work as well, but operators are unable to use Security Desk to manually open doors, and so on.
- During the upgrade, each Directory server is upgraded separately. Consequently, the failover feature is not available.
- License upgrades are only necessary for major version upgrades (for example, from version 5.x to 5.10). It is not necessary to upgrade the license for minor version upgrades (for example, from 5.10.x.0 to 5.10.y.0).

To upgrade a multiple Directory server system:

1 On each of the secondary Directory servers in the Directory server list, stop the Genetec™ Watchdog service from the Microsoft Management Console (MMC) Service window.

The secondary Directory servers are indicated with the expansion server icon ( ). Do not stop the main server ( ).

The Genetec™ Server service is stopped on the secondary Directory servers. All roles that only run on secondary Directory servers are offline. Usually each Directory server is responsible for an equal share of the role and client connections. After the secondary Directory servers are stopped, any roles or clients previously connected to one of the secondary Directory servers are forced to reconnect to the primary Directory server. The clients briefly show the "Connection is lost..." message during this process. The roles and their entities appear as offline until they are reconnected.

2 Upgrade the primary Directory server as the main server.

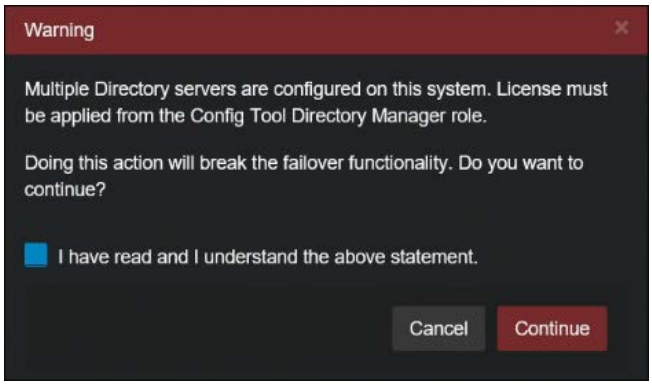
The primary Directory server, also known as the main server ( ), is the only server that is still active before you start the upgrade process. While the main server is being upgraded, no Directory service is available on the system. Only some features remain functional.

Security Center Installer automatically stops the Genetec™ Server service on the main server, and restarts it after the upgrade.

3 (Only applies to major version upgrades) Activate your Security Center 5.10 license by doing one of the following:

- If you have Internet access, use web activation.
- If you do not have Internet access, use manual activation.

During the license activation, a message warning you that the failover functionality will be broken, is displayed.



Do not worry. The failover functionality will be restored later. Click **I have read and I understand the above statement** and click **Continue**.

The Directory service is online. All expansion servers (except the secondary Directory servers) and client workstations that are not yet upgraded run in backward compatibility mode. Directory failover and load balancing are not yet available.

4 From Config Tool, connect to the main server. Check that all roles, servers, and units are running as expected.

The secondary Directory servers are still stopped (in red). Any roles that only run on the secondary Directory servers are still offline.

5 Upgrade the rest of the Directory servers as expansion servers.

Security Center Installer restarts the Genetec™ Server service after each upgrade. Directory failover and load balancing are still unavailable.

6 (Only applies to major version upgrades) Reactivate the Security Center 5.10 license for all your Directory servers.

Directory failover and load balancing are now available.

After you finish

Upgrade the rest of your system according to your priorities and schedule.

IMPORTANT: Adding backward compatible connections slows down the performance of the Directory. It is only recommended as a temporary solution before you are able to upgrade all servers and workstations.

Related Topics

Backward compatibility requirements for Security Center on page 86
One or more services failed to install on page 144

Reactivating Security Center license for Directory failover systems

Every time you add, remove, or change the servers in the Directory failover list, you must generate a new validation key and reactivate your Security Center license from Config Tool.

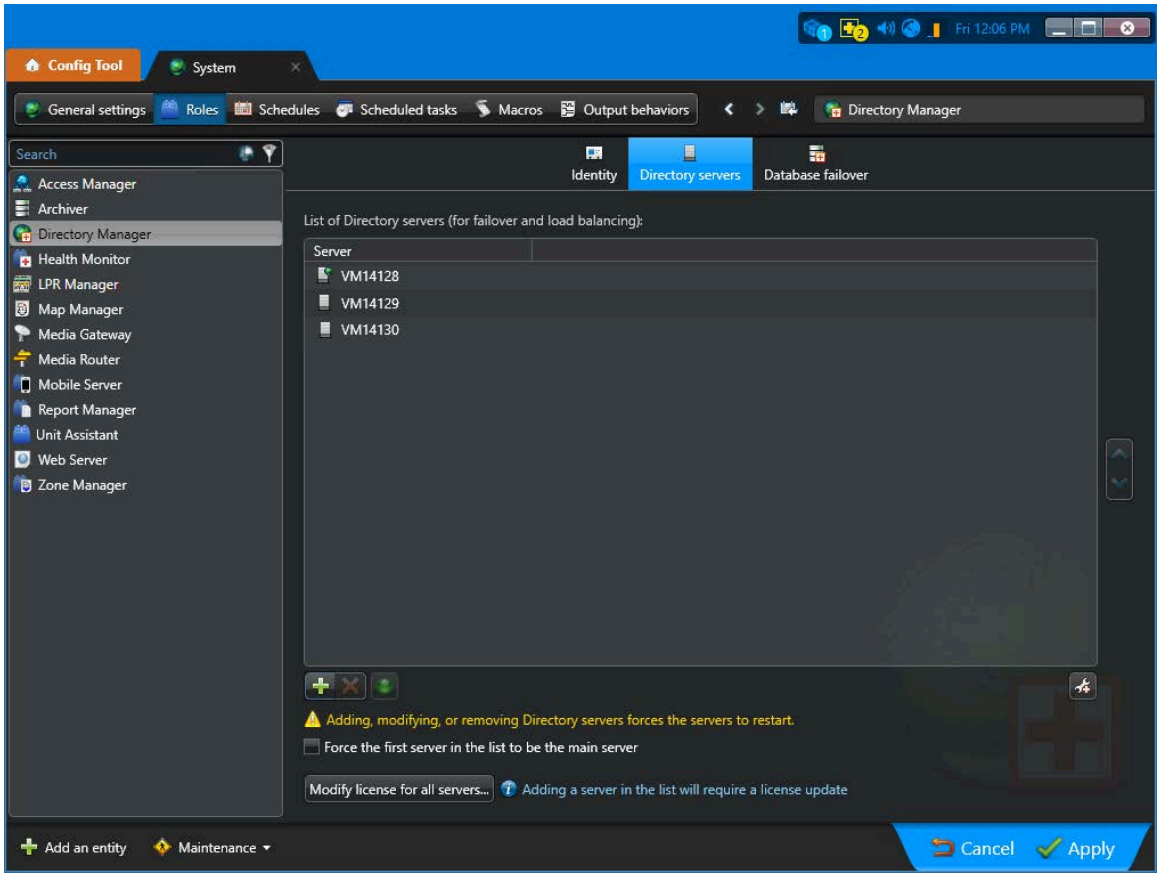
What you should know

IMPORTANT: When you have multiple Directory servers configured for failover, you must generate the validation key and apply the license key from Config Tool instead of Server Admin. All Directory servers must be up and running for the license update to work.

To reactivate the Security Center license for a multiple Directory server system:

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

2 Select the **Directory Manager** ( ) role, and click the **Directory servers** tab.



3 Click **Modify license for all servers**.

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

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

Your system ID and password are specified in the *Security Center License Information* document. Our Customer Service team sends you this document when you purchase the product.

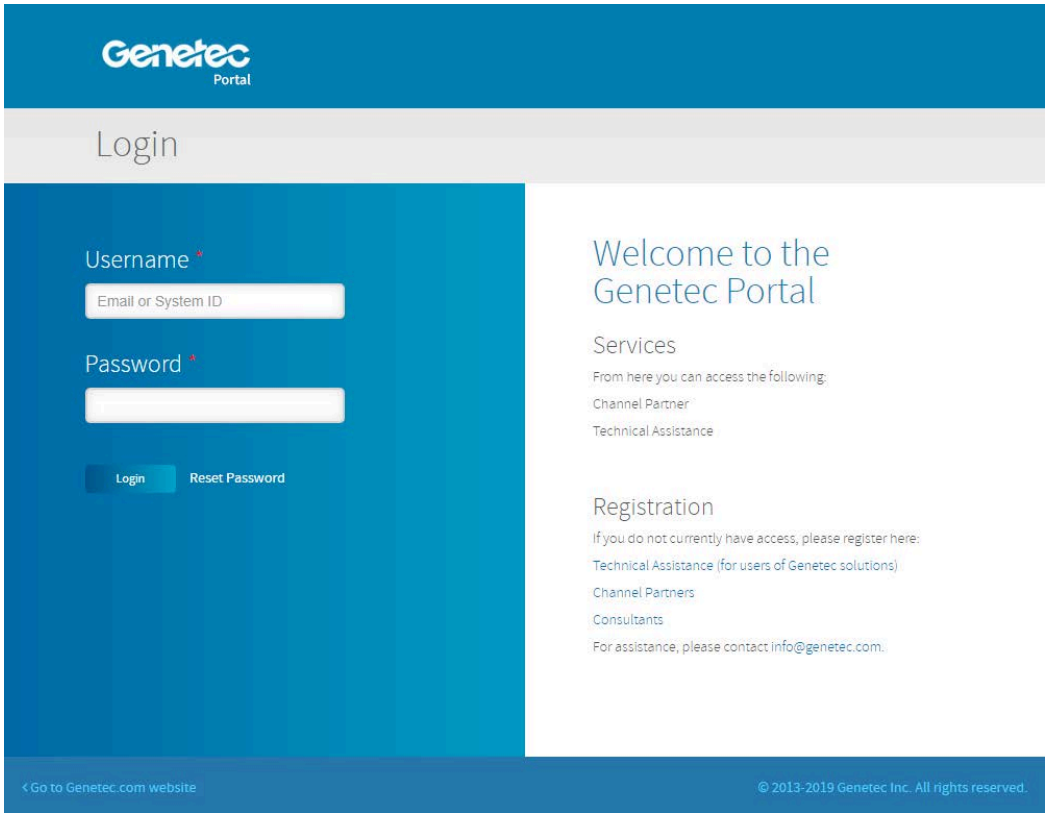
- **Manual activation:** If your workstation has no Internet access, reactivate your Security Center license manually using a license file. Continue with the next step.

5 Click **Save to file** to save the composite validation key to a file.

IMPORTANT: You must use the *composite* validation key that comprises all Directory servers, or the license reactivation fails silently and the Directory failover does not work.

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

6 From a computer with internet access, open the Genetec™ Technical Assistance Portal (GTAP) at: https://portal.genetec.com/support.



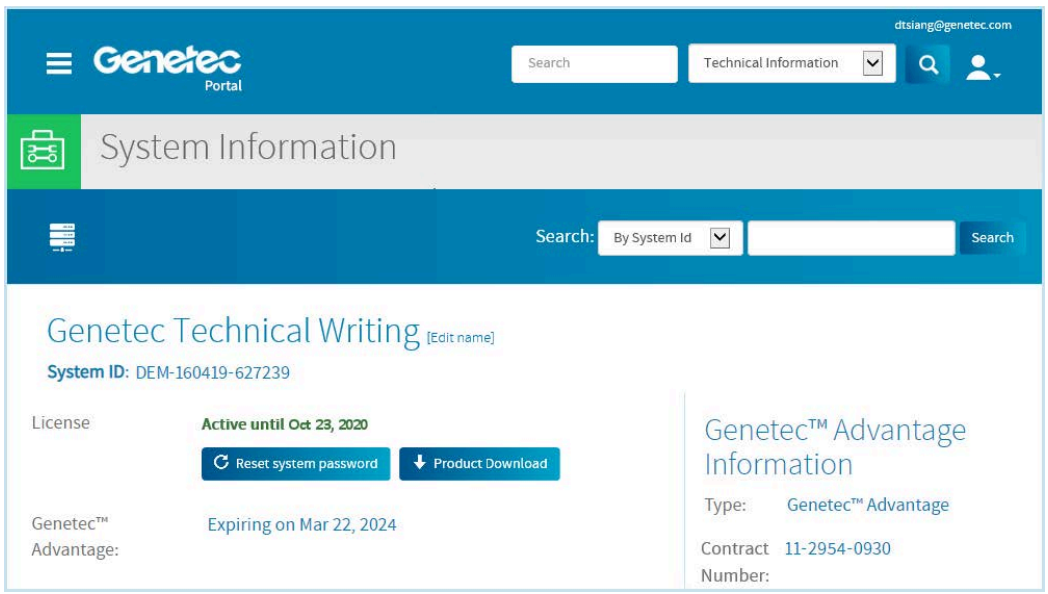
7 On the *Login* page, do one of the following:

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

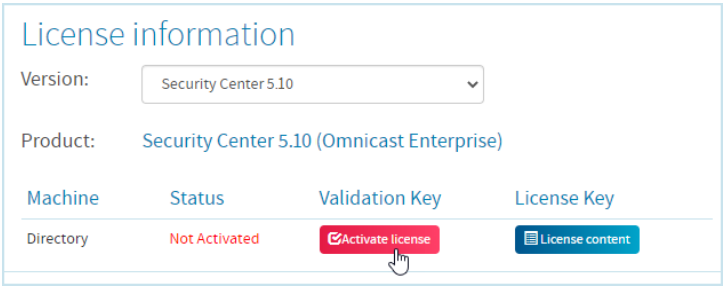
8 On the GTAP home page, open the **Genetec Portal** menu and click **Technical Assistance** > **System Management**.

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

The *System Information* page opens.



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



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

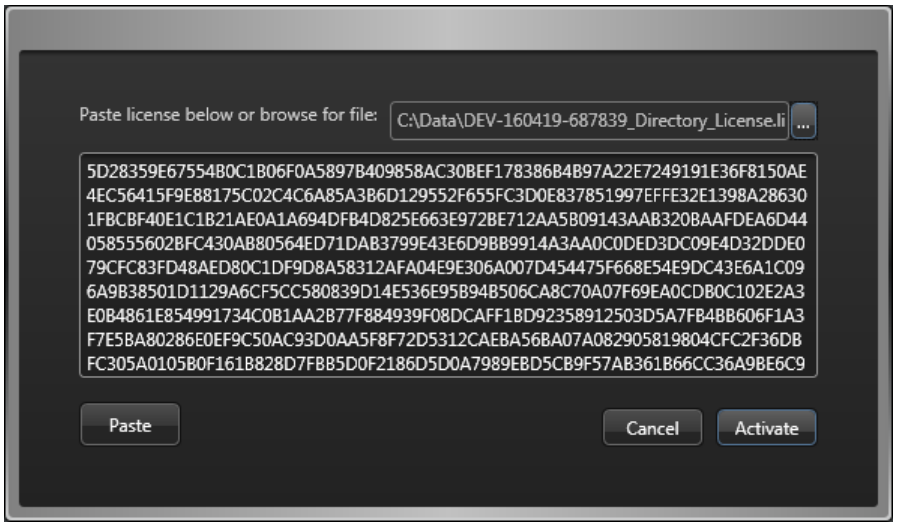
12 When you receive the License activation successful message, click **Download** under *License Key* and save the license key to a file.

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

13 Return to the Config Tool workstation.

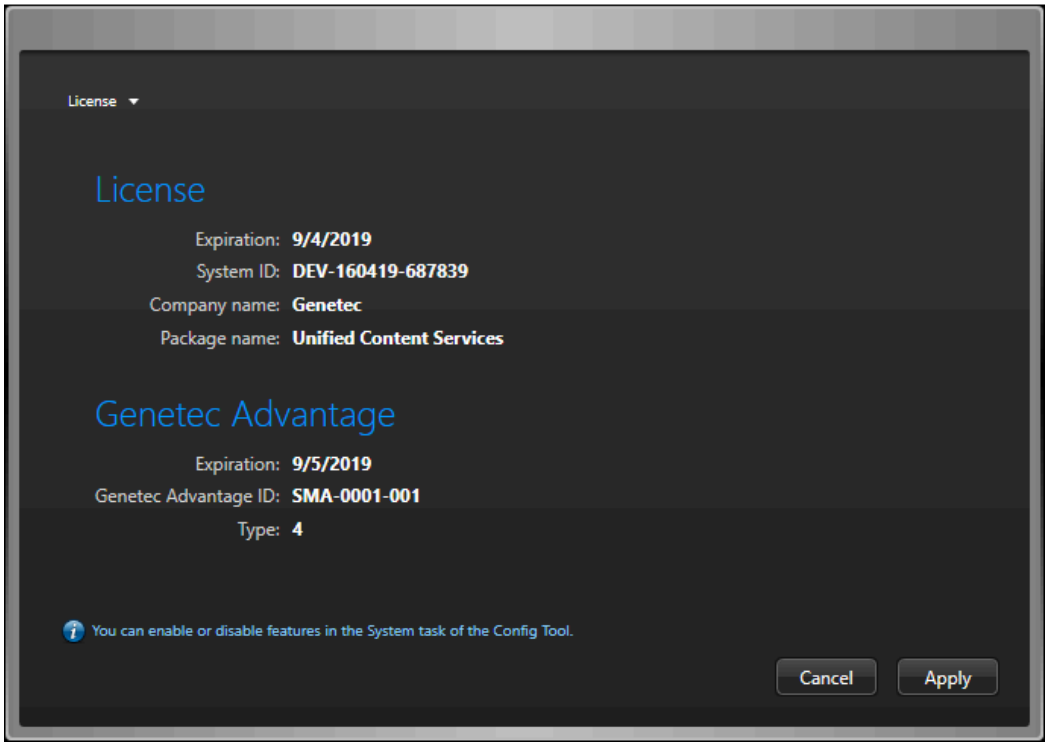
14 In the *License management* dialog box, click **Manual activation**.

15 In the *Manual activation* dialog box, browse for the license key file, and click **Open**.



16 Click **Activate**.

A dialog box showing your license information opens.



17 Click **Apply** to close the dialog box, and click **Apply** at the bottom of the Config Tool window to save your changes.

What Security Center client features are available when the Directory service is offline?

During a Security Center system upgrade, all Directory servers must be shut down for a period of time. During this time, no Directory service is available on the system. Only some features continue to work.

The following Security Center features are available when there is no Directory service:

- Security Desk continues to stream live video from cameras.
- Video continues to be recorded according to schedules as long as Archivers are online.
- All access control functions continue to work as normal, except for commands that must be relayed by the Directory service, such as event-to-actions, and all door open or unlock operations issued from Security Desk.
- Doors can be opened through a switch (input) if all inputs and outputs are controlled by the same access control unit.

The following Security Center features are not available when there is no Directory service:

- Config Tool and Security Desk features are unavailable.
- All manual actions (manual recording, lock/unlock doors, and so on) performed from the Security Desk widgets are disabled, including camera call-ups.
- Alarms and live events cannot be displayed on Security Desk.

Upgrading the Security Center main server

The main server in your current Security Center system must be upgraded before everything else. You must activate the new license and upgrade the Directory database.

Before you begin

- Read the things you need to know and do before you upgrade (see related topics).
- Back up your Directory database and all role databases accessed from your main server.

  BEST PRACTICE: There is an option in the InstallShield Wizard to back up your Directory database after the software upgrade, before restarting your system. Depending on the size of your database, this backup might take several hours. To accelerate your upgrade process, you can back up your Directory database before upgrading the software. Then, when the InstallShield Wizard reaches the *Directory Database Backup* step, you can choose to skip the backup. However, if you choose to let *Genetec™ Update Service (GUS)* perform the upgrade, do not back up the Directory database yourself, because GUS always does it for you.
- Make sure that you have enough disk space for your backup. Delete the backups that you no longer need. The default backup folder is *C:\SecurityCenterBackup* on the server hosting SQL Server.

What you should know

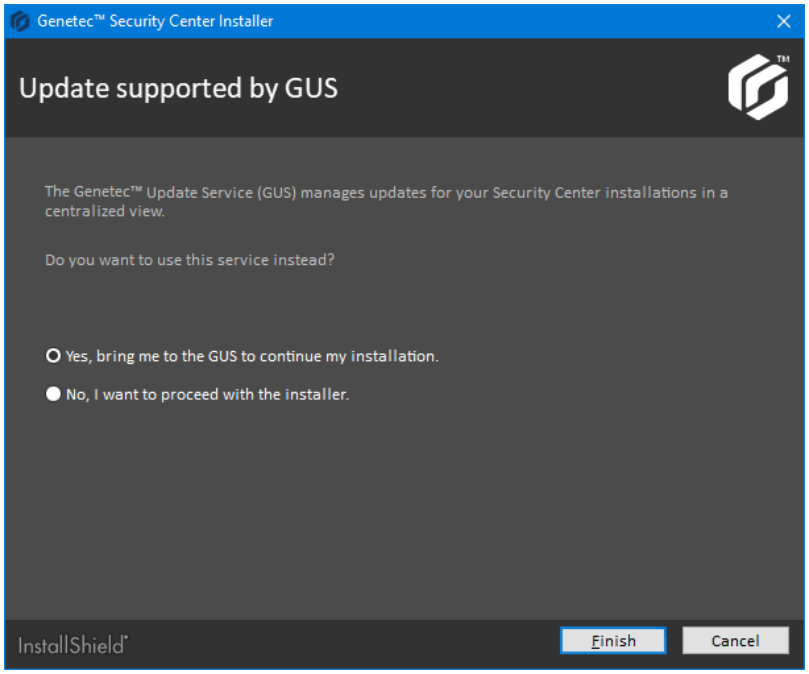
You need the Security Center 5.10 Config Tool to connect it to the 5.10 Directory. If Security Center Client is installed on the main server, upgrade it at the same time.

If a reboot warning message box opens during the upgrade, accept the message and continue with the upgrade procedure. You must reboot after completing the upgrade.

To upgrade the main server:

1 Install Security Center 5.10 on your main server.

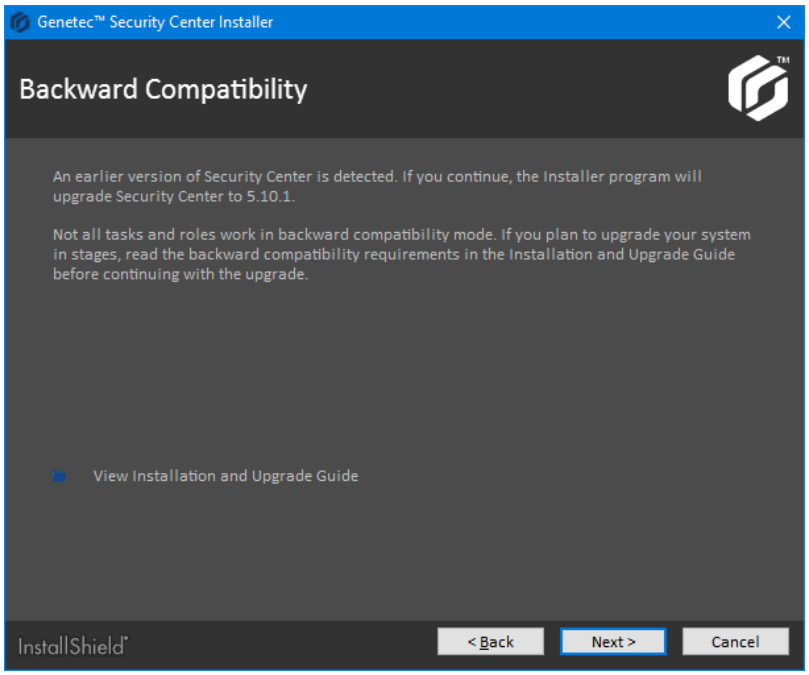
If you have Genetec™ Advantage and are subscribed to our Product Improvement Program, and if the version you want to install corresponds to the most up to date version, you have the option to perform the upgrade through GUS instead of the installer.



If you choose to continue with GUS, the Installer program ends and automatically connects you to the Main GUS. The Main GUS displays a centralized view of all enrolled machines and sends update

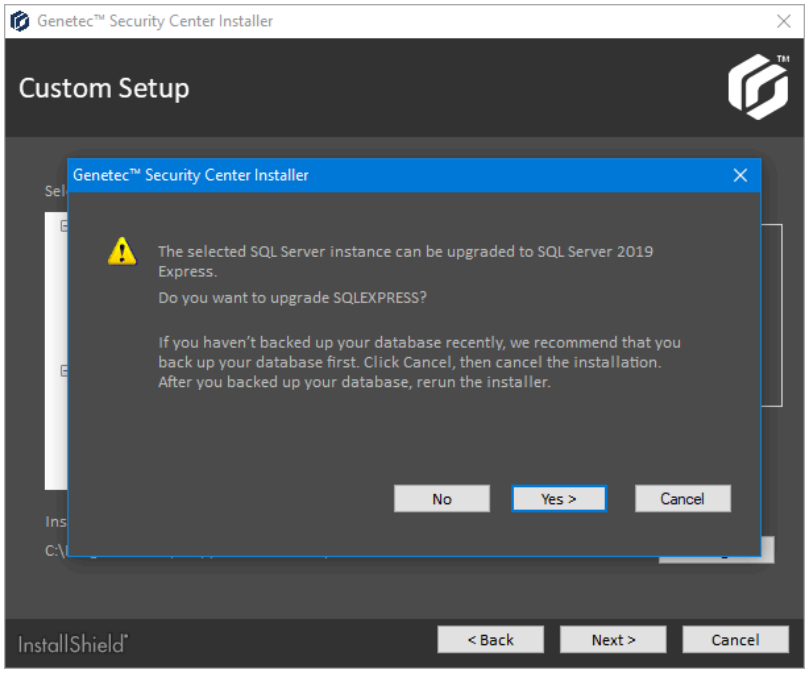
notifications to them. GUS always backs up the Directory database for you, so you don't need to do it before the upgrade. For more information, see the *Genetec™ Update Service User Guide*.

If you choose to continue with the installer, the Installer program automatically detects an earlier version of Security Center and issues warnings and recommendations. Read the messages carefully.



If you continue, the Installer program upgrades Security Center to 5.10.

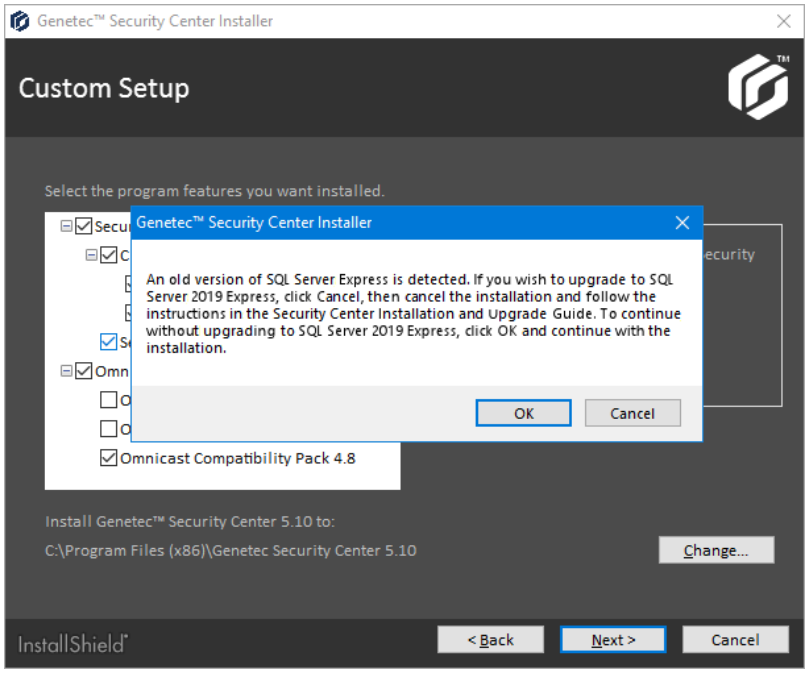
2 If you are running a version of SQL Server Express that is not the latest, but one that is upgradable to SQL Server 2019 Express, the Installer program will offer to upgrade it automatically.



Choose one of the following:

- (Recommended) Let the installer upgrade your SQL Server instance to SQL Server 2019 Express:
  a. Click **Cancel** to close the message box, then click **Cancel** to cancel the installation.
  b. If you haven't backed up your databases recently, do it now.
  c. Rerun the installer.
- Click **Yes** to upgrade your SQL Server instance to SQL Server 2019 Express and continue with the installation.
- Click **No** to continue with the installation without upgrading your SQL Server instance.

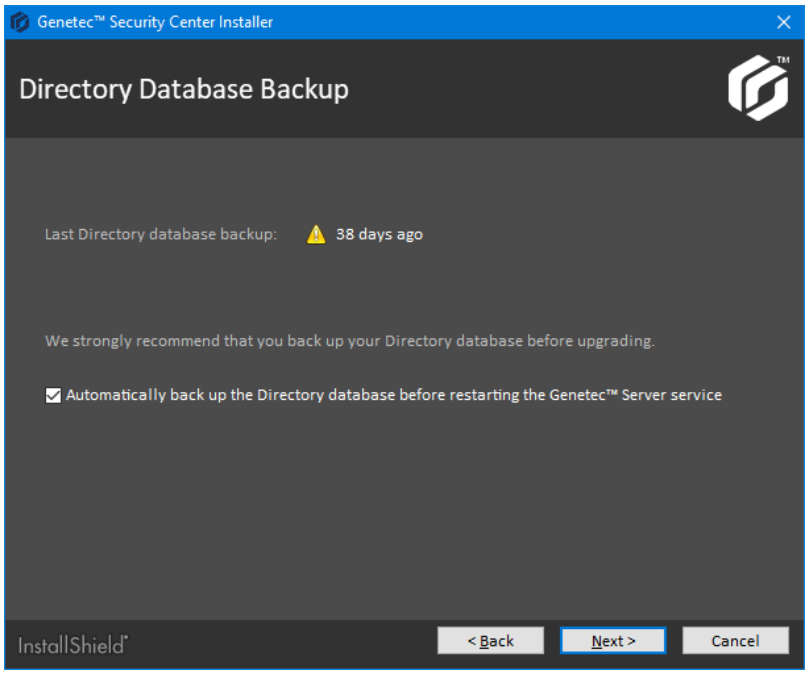
3 If you are running SQL Server 2014 Express SP1 or earlier, the Installer program cannot upgrade it to SQL Server 2019 Express.



Choose one of the following:

- (Recommended) Upgrade your SQL Server instance to SQL Server 2019 Express:
  a. Click **Cancel** to close the message box, then click **Cancel** to cancel the installation.
  b. If you haven't backed up your databases recently, do it now.
  c. Download and run the SQL Server 2014 SP2 Installer.
  d. Restart your server.
  e. Rerun the Security Center Installer.
- Click **OK** to continue with the installation without upgrading your SQL Server instance.

4 On the *Directory Database Backup* page, acknowledge the date of the last Directory database backup, and click **Next** to continue the installation.



If you select the automatic backup option, the Directory database will be backed up after the software upgrade, but before the database upgrade.

NOTE: For the last Directory database backup date, the Installer does not differentiate between full and incremental backups and does not check whether the backup files are still available. The automatic backup option always performs a full backup.

IMPORTANT: It is possible that the date of the last Directory database backup is inaccurate if the last backup was performed outside of Security Center. Regardless, we strongly recommend that you back up your Directory database before upgrading, or let the installer do it for you. The option to automatically back up the Directory database is selected by default if the last backup is more than a day old. Do not clear this option if you are not sure whether the most recent changes are included in the last backup.

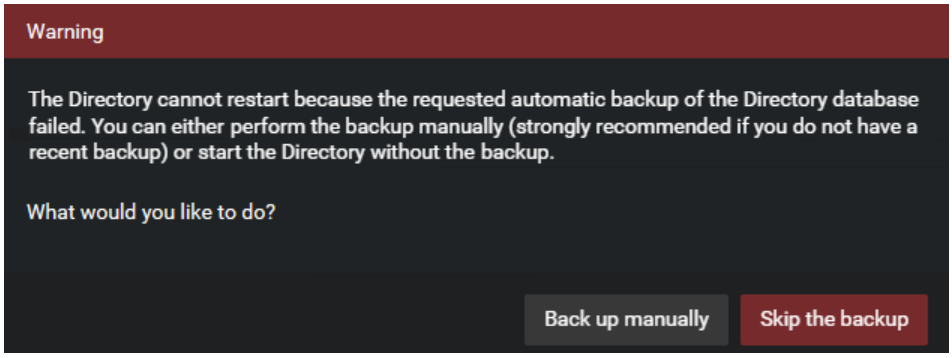
5 Follow the rest of the InstallShield Wizard instructions, and click **Install**.

The installer updates your Security Center software, backs up the Directory database (if you selected the option), updates the schema of your Directory database (if applicable), and launches Server Admin.

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

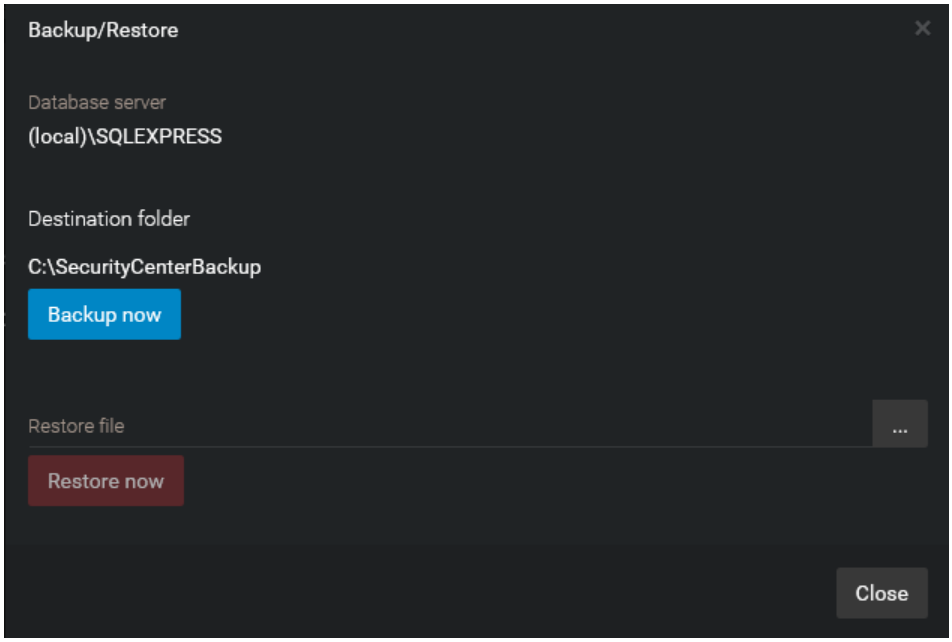
The Server Admin *Overview* page opens.

7 If the automatic backup of the Directory database failed, the Directory does not restart.

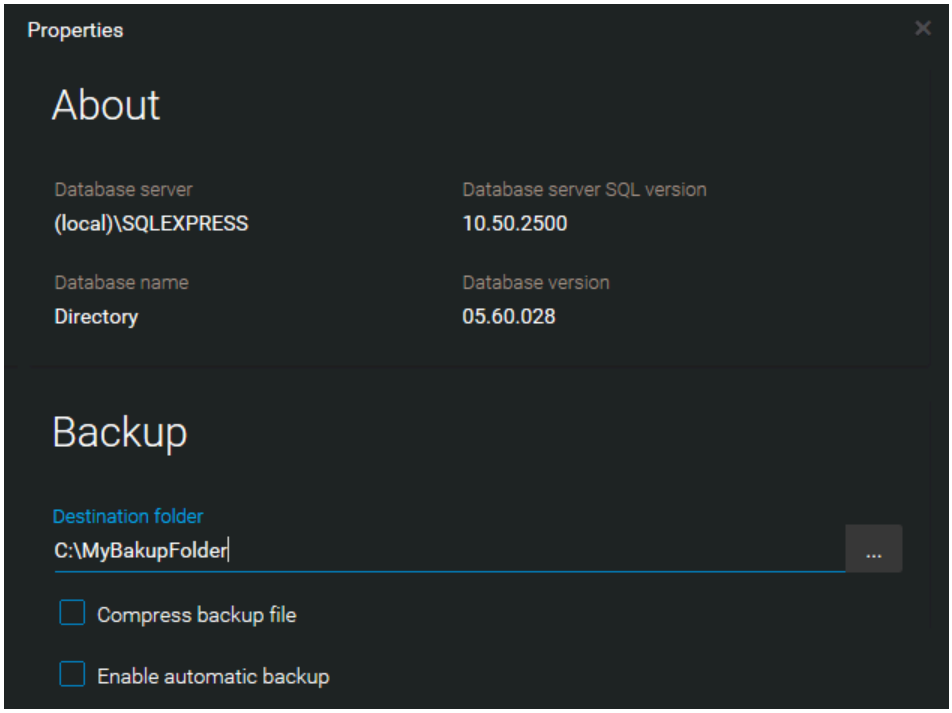


You must choose one of the following:

- **Back up manually**. This is the recommended option. It opens the *Backup/Restore* dialog box.



When a backup fails, it is often because you do not have access to the backup folder. If you need to change the backup folder, close this dialog box, select the main server from the list of servers, and click **Database properties** ( ). In the dialog box that opens, enter the new **Destination folder**.



After the Directory database is successfully backed up, the system restarts. If a database update is required, it will be performed automatically before restarting the Directory.

- **Skip the backup**. Choose this option only if you are sure that the latest backup has all the changes you need. If a database update is required, it will be performed automatically. If you do not have a backup of your database, you will not be able to restore it if necessary.

8 If you are upgrading from an earlier *major version*, activate your new Security Center 5.10 license.

Related Topics

Backing up databases on page 92
Pre-upgrade checklist for upgrading from an earlier major version of Security Center on page 85
Upgrading the Security Center Directory database on page 119
Activating Security Center license using the web on page 46
Activating Security Center license manually on page 49

Upgrading expansion servers in Security Center

To benefit from the latest enhancements to Security Center, you must upgrade the expansion servers. To upgrade, install Security Center Server onto the expansion servers, and follow the instructions in the InstallShield Wizard.

Before you begin

Back up all role databases accessed from your expansion server you are upgrading.

What you should know

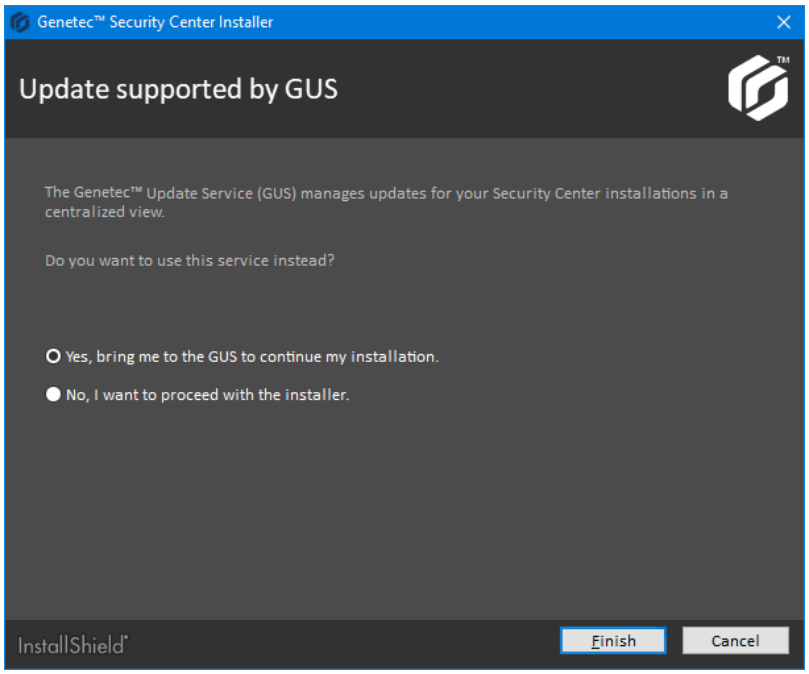
If a reboot warning message box opens during the upgrade, accept the message and continue with the upgrade procedure. You must reboot after completing the upgrade.

To upgrade an expansion server:

1 Install Security Center 5.10 on your expansion server.

Use the **Expansion server** installation type.

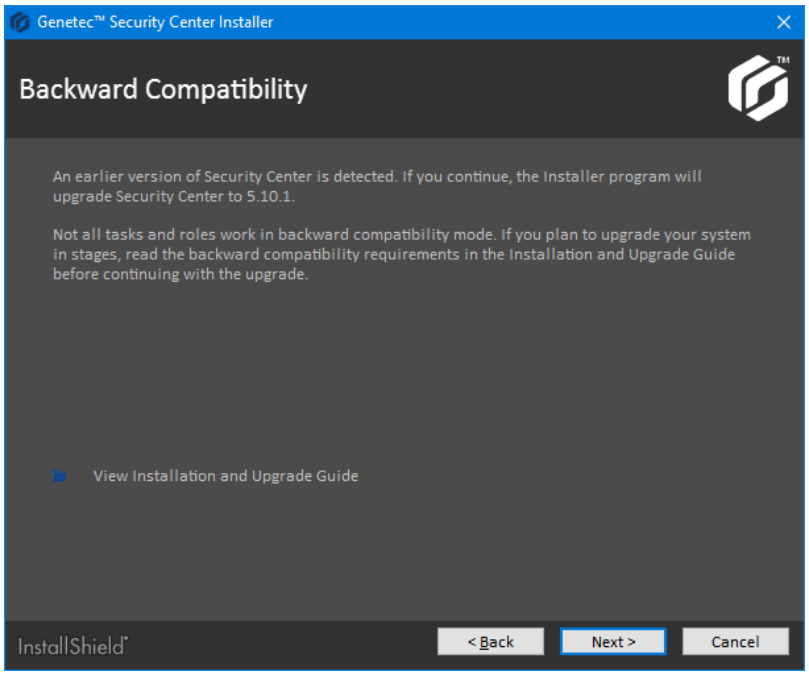
If you have Genetec™ Advantage and are subscribed to our Product Improvement Program, and if the version you want to install corresponds to the most up to date version, you have the option to perform the upgrade through GUS instead of the installer.



If you choose to continue with GUS, the Installer program ends and automatically connects you to the Main GUS. The Main GUS displays a centralized view of all enrolled machines and sends update

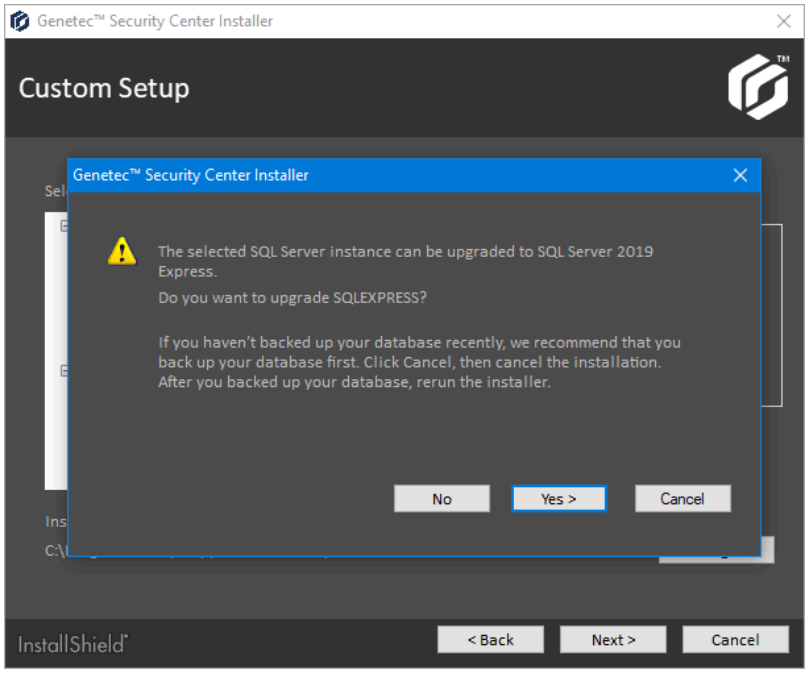
notifications to them. GUS always backs up the Directory database for you, so you don't need to do it before the upgrade. For more information, see the *Genetec™ Update Service User Guide*.

If you choose to continue with the installer, the Installer program automatically detects an earlier version of Security Center and issues warnings and recommendations. Read the messages carefully.



If you continue, the Installer program upgrades Security Center to 5.10.

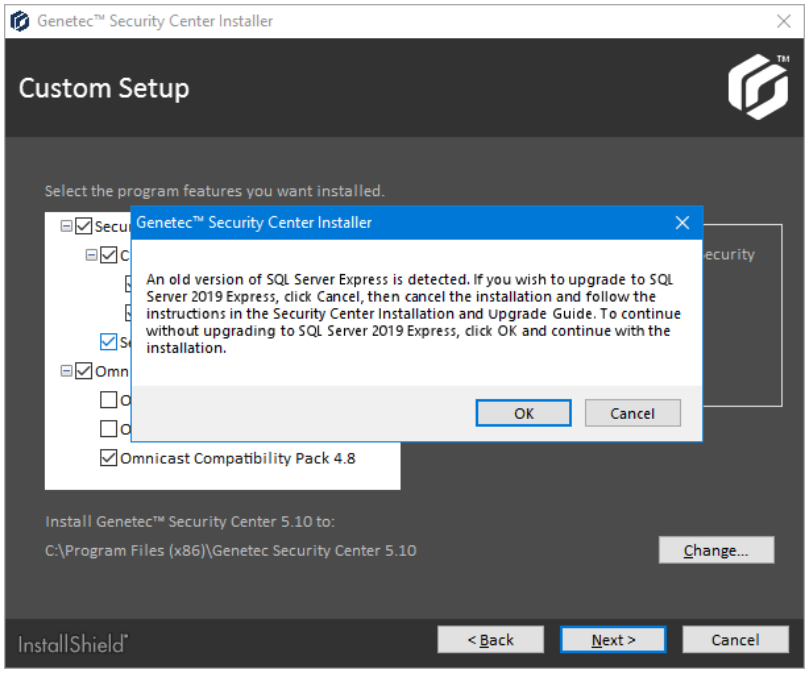
2 If you are running a version of SQL Server Express that is not the latest, but one that is upgradable to SQL Server 2019 Express, the Installer program will offer to upgrade it automatically.



Choose one of the following:

- (Recommended) Let the installer upgrade your SQL Server instance to SQL Server 2019 Express:
  a. Click **Cancel** to close the message box, then click **Cancel** to cancel the installation.
  b. If you haven't backed up your databases recently, do it now.
  c. Rerun the installer.
- Click **Yes** to upgrade your SQL Server instance to SQL Server 2019 Express and continue with the installation.
- Click **No** to continue with the installation without upgrading your SQL Server instance.

3 If you are running SQL Server 2014 Express SP1 or earlier, the Installer program cannot upgrade it to SQL Server 2019 Express.



Choose one of the following:

- (Recommended) Upgrade your SQL Server instance to SQL Server 2019 Express:
  a. Click **Cancel** to close the message box, then click **Cancel** to cancel the installation.
  b. If you haven't backed up your databases recently, do it now.
  c. Download and run the SQL Server 2014 SP2 Installer.
  d. Restart your server.
  e. Rerun the Security Center Installer.
- Click **OK** to continue with the installation without upgrading your SQL Server instance.

4 If you are upgrading a Directory server (Failover Directory configuration), make sure that on the *Directory Database Backup* page, you clear the option **Automatically back up the Directory database before restarting the system** to avoid backing up the Directory database twice.

5 Repeat the steps for all expansion servers in your system.

After you finish

To verify that all servers in your system are active, log on to the main server with Config Tool. In the *Network view* task, all the servers in your system should be shown in black, which means they are active. If some of the roles are still not active, you might need to upgrade the Directory database.

Related Topics

Backing up databases on page 92
Pre-upgrade checklist for upgrading from an earlier major version of Security Center on page 85

Upgrading Security Center Client

After you upgrade the Security Center main server and expansion servers, you can upgrade Security Center Client.

What you should know

The Security Center 5.10 Client is installed side-by-side with previous Security Center Client versions.

From Security Center 5.4, Client settings are automatically carried over to new Client versions. After installing a new version, you can remove the older version.

TIP: If the workstations on your system are enrolled in *Genetec™ Update Service (GUS)*, you can install the lastest Security Center Client on all of them at the same time from the Main GUS. For more information, see the *Genetec™ Update Service User Guide*.

To upgrade from a previous version of Security Center Client (5.4 and later) to 5.10:

- Install Security Center Client.

  The installer automatically detects an earlier version of Security Center software and applies the current settings to 5.10.

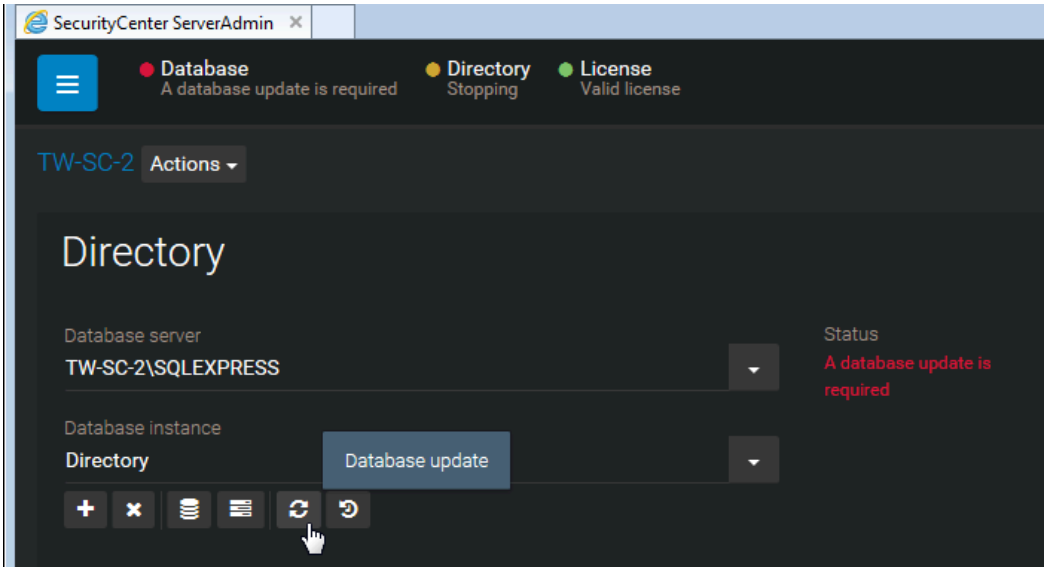
Upgrading the Security Center Directory database

The Security Center 5.10 Installer upgrades the Directory database as part of the main server upgrade. You only need to upgrade the Directory database manually if you restored an older version of the database.

What you should know

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

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



To upgrade the Directory database:

1 Do one of the following:

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

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

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

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

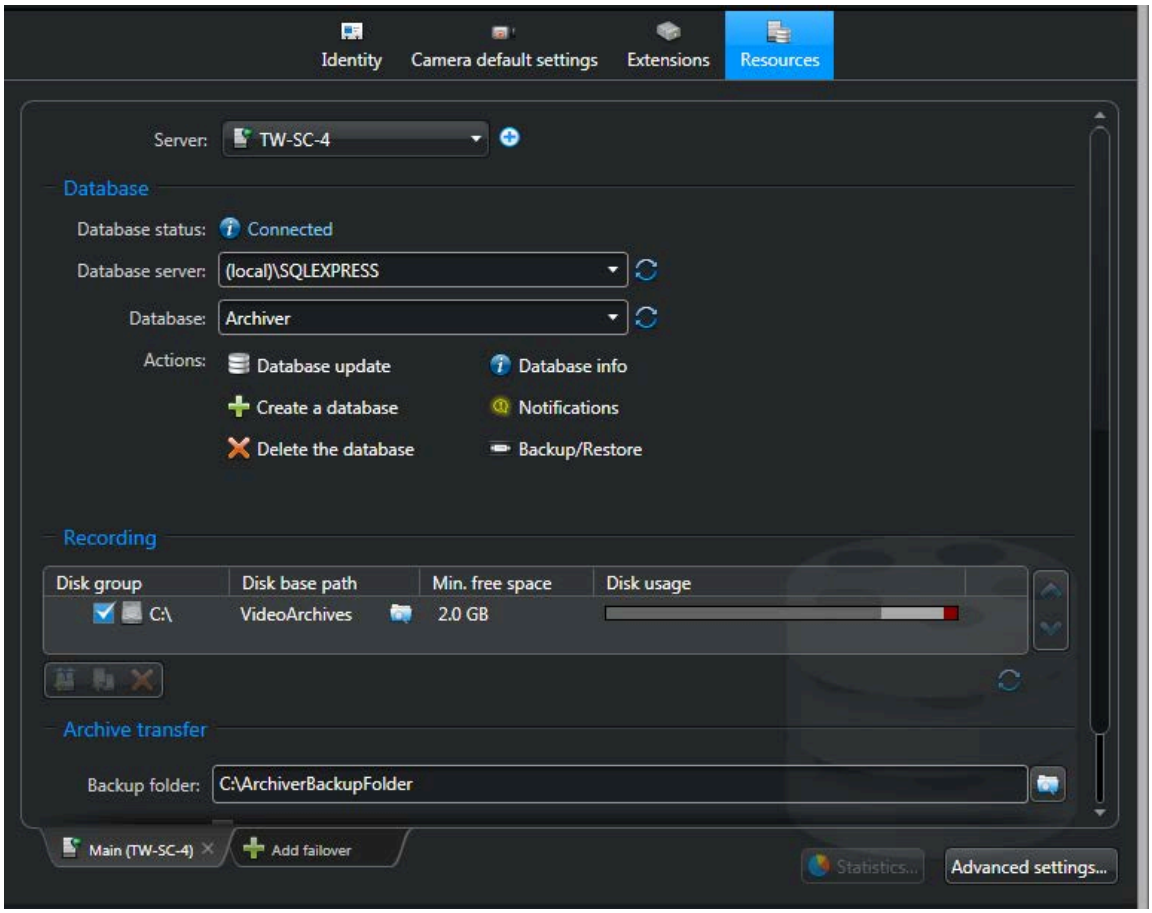
3 Click **Database properties** (🗄) to confirm the version of the database and the number of entities in the database.

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

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

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

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



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

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

After you finish

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

Shrinking Security Center databases after an upgrade

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

Before you begin

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

What you should know

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

- Recovery Models (SQL Server)

- Transaction Log Truncation

To shrink a database:

1. Follow the Shrink a Database procedure from Microsoft.
2. Repeat this procedure for all databases that require shrinking.

Upgrading Security Center with Global Cardholder Synchronizer roles

To upgrade a composite Security Center system involving Global Cardholder Synchronizer (GCS) roles, you must upgrade the sharing host system first, then upgrade the sharing guest systems.

Before you begin

Back up the Directory databases of your *sharing host* and *sharing guest* systems.

What you should know

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). For more information, see "Global cardholder management" in the *Security Center Administrator Guide*.

To upgrade a composite Security Center system involving GCS roles:

1 Disconnect the sharing guests from the sharing host.

Do one of the following:

- Deactivate the GCS roles on the sharing guest systems.
- Temporarily change the passwords of the GCS role user accounts.

2 Upgrade the sharing host system first.

3 Upgrade the sharing guest systems next.

4 Confirm that the upgrades were successful.

5 Reconnect the sharing guests to the sharing host.

Do one of the following:

- If you deactivated the GCS roles on the sharing guest systems, reactivate them.
- If you changed the passwords of the GCS role user accounts, change them back.

6 Give the sharing guests some time to sync with the sharing host.

3

Automating Security Center installation

This section includes the following topics:

- "Silent installation of Security Center" on page 124
- "Preparing to perform a silent installation" on page 125
- "Silent installation options for Security Center" on page 126
- "Security Center options" on page 128
- "Sample Security Center Server installation commands" on page 133
- "Sample Security Center Client installation commands" on page 135
- "Uninstalling Security Center 5.10 in silent mode" on page 136
- "Silent installation options for Security Center SDK" on page 137

Silent installation of Security Center

A silent installation is an automated way of installing software without user intervention. The silent installation is run from the command line using the *Security Center setup.exe* executable, and Windows Installer commands.

You can customize the following options from the command line:

- Installation language
- Application language
- Client or Server installation path
- Client or Server features to install
- Server username and password for running the services
- Server and database name

Limitations

Take note of the following limitations before performing a silent installation:

- You cannot update your license in silent mode. You'll need to run the Server Admin application after installing Security Center to activate the license.
- A command line is limited to a maximum of 850 characters.

  TIP: One way to shorten the command-line length is to reduce the installation path length. This can be achieved by copying the installation files onto a local drive.
- You cannot use mapped drives in your path specifications.
- You cannot install WinPcap (utility for capturing diagnostic data) in silent mode.

Silent installation of the Security Center Drivers

To install the Security Center Drivers in silent mode, you need to ask your representative of Genetec Inc. for the separate driver installation package, and use the following syntax:

```
setup.exe /s /v"/qn /l*v "<msilog>" <restart_option>"
```

where:

- setup.exe is the setup program found in the root folder of the Drivers installation package.
- <msiLog> is the path to the MSI log file. The folder path must exist. The setup program will not create it.

  Example: "C:\Users\Public\install.log"
- <restart_option> indicates whether or not to restart the Genetec™ Server service after installation.
  - RESTART_GENETEC_SERVER=1 (default)
  - RESTART_GENETEC_SERVER=0

  If you choose not to restart Genetec™ Server right away, you must restart it at a later time for the new drivers to take effect.

Silent installation of the Security Center SDK

To install the Security Center SDK in silent mode using the separate SDK installation package, see Silent installation options for Security Center SDK on page 137.

Preparing to perform a silent installation

There are certain tasks you should perform prior to the installation to ensure it goes smoothly.

Before performing a silent installation:

1 Install the Security Center prerequisites.

Security Center installer automatically verifies and installs the software prerequisites on your system. This might cause your system to restart. Therefore, it is best practice to manually install the software prerequisites before launching the silent installer.

2 Apply the latest Windows updates.

3 If you specify a different Windows user than the default (Local System) to run the services, then that user must be created before you begin the installation process.

The user must be a member of the Administrators group and must have the *Log on as service* user privilege.

Related Topics

Installing SQL Server independently of Security Center on page 28

Silent installation options for Security Center

When performing a silent installation, specific program options are required to run the Security Center Installer.

The syntax for running the setup in silent mode is:

```
<setup_exe> <options> <SC_options>
```

where:

- <setup_exe> is the setup program for the Security Center Installer. You can either use the standalone version ("Security Center Setup.exe" found in the *SC Packages* folder) or the web version (SecurityCenterWebSetup.exe).

  Do not use the *setup.exe* in the root folder of the installation package. It is an AutoRun-enabled version of the standalone installer, and does not accept command line arguments.
- <options> are the setup program options. They all start with a forward slash (/) and are case sensitive.
- <SC_options> are the Security Center options. They are all written in capital letters.

The following table describes the setup options.

Setup option	Description
/ISInstallDir	Specifies the root folder where the product subfolder will be created. Default: *C:\Program Files (x86)\Genetec Security Center 5.10*. **EXAMPLES**: • /ISInstallDir=C:\MyFolder • /ISInstallDir="D:\Program Files\MyFolder" **NOTE:** In the second example, the (") are required because the value contains spaces. If not specified, the default is <ProgramFiles>, where <ProgramFiles> is either %PROGRAMFILES% or %PROGRAMFILES(X86)%, depending on the version of your operating system. **CAUTION:** The folder path cannot end with a trailing backslash (\). This causes the silent installation to fail with a fatal error.
/ISFeatureInstall	Specifies the features to be installed. The possible values are: • Server (Genetec™ Server with or without Directory, depends on the SERVER_TYPE installer option) • Client (Security Desk and Config Tool) • SecurityDesk (only Security Desk) • ConfigTool (only Config Tool) • CompPacks,CompPack4x[,CompPack4x] (Omnicast™ compatibility packs, you must specify at least one of CompPack46, CompPack47, or CompPack48) **EXAMPLES**: • /ISFeatureInstall=Server,Client (DEFAULT) • /ISFeatureInstall=Client,CompPacks,CompPack48
/silent	Sets the Security Center setup.exe program to run in silent mode with no user interaction.

Setup option	Description
/debuglog<FilePath>	Enables the creation of the installation log file and specifies the file path. **NOTE:** The folder path specified in <FilePath> must exist. The setup program will not create it. **EXAMPLE:** /debuglog"C:\LogFiles\Install.log"
/log<FolderPath>	Enables the creation of the log files and specifies the folder path. **NOTE:** The <FolderPath> must exist. The setup program will not create it. **EXAMPLE:** /log"C:\LogFiles\"
/language:	Sets the language used by the installation program. Immediately precedes the four-digit language code. No space is allowed. **EXAMPLES** • /language:1033 for English (DEFAULT) • /language:3084 for French
<SecurityCenter_options>	Sets the Security Center options. Each option in this list uses the following syntax: `<option>=<value_list>` where <option> is an option name and <value_list> is a list of comma separated values. No space is allowed on either side of the equal sign (=). If the value list must contain spaces, the entire value list must be included between a pair of double quotes preceded by a backslash (\").

Related Topics

Security Center options on page 128

Security Center options

When performing a silent installation, you can specify additional options for the Security Center.

The following table lists the Installer options for Security Center. All Security Center options are written in capital letters. Unlike the setup options, none of them are preceded with a forward slash (/). All options names are case sensitive.

IMPORTANT: All servers on the system share the same password. Therefore, for the installation of both main and expansion servers, only use the option MAINSERVER_PASSWORD to specify the password.

Security Center option	Description
ACTIVATIONCODE	This is the activation code required to allow *System Availability Monitor Agent (SAMA)* to collect system data. **EXAMPLE**: SAMA_COLLECTPOLICY=On ACTIVATIONCODE=mycode
AGREETOLICENSE	Indicate that you agree with our software license agreement. **IMPORTANT:** The only accepted value is Yes. If omitted, the installation will fail. **EXAMPLE**: AGREETOLICENSE=Yes
ALLOWSQLUPGRADE	Allow the installer to upgrade your database server to SQL Server 2019 Express Edition if your operating system supports it. The accepted values are 0 and 1. • 0 = Do not upgrade (DEFAULT) • 1 = Upgrade if your operating system supports it SQL Server 2019 Express is only supported on the 64-bit version of Windows 10 and Windows Server 2016 and later. **IMPORTANT:** Be sure to back up your databases before the SQL Server upgrade. **EXAMPLE**: ALLOWSSQLUPGRADE=1 When SKIPSQLVALIDATION=1 is specified, the database server upgrade is ignored.
COLLECTPOLICY	Configure the data collection policy for our Product Improvement Program. The accepted values are: • On: We will collect data with system information. • Anonymous: We will collect anonymous data. • Off: We will not collect data. **IMPORTANT:** This option is mandatory if you are installing the main server on a clean machine. If omitted, the installation will fail. You can also use this option to change the existing data collection setting if you are upgrading the main server. It is ignored if you are installing an expansion server or a client workstation. **EXAMPLE**: COLLECTPOLICY=Anonymous

Security Center option	Description
CONFIGURATION_SETTINGS	Specify which configuration settings to use if older configuration files (*ConfigurationFiles*.gconfig*) are found on your machine. The accepted values are: • KeepExistingSettings (FIRST DEFAULT) • DeployNewSettings (SECOND DEFAULT) • UpgradeOldSettings The first option is applicable only if configuration files for the current major version (5.10) are found on your machine. The last option is applicable only if configuration files from an older major version are found on your machine. **EXAMPLE**: CONFIGURATION_SETTINGS=UpgradeOldSettings **NOTE:** This option is only application for fresh installations. If you are upgrading your system, it always upgrades your current settings.
CREATE_FIREWALL_RULES	Add the installed Security Center applications to the Windows Firewall exceptions list. Accepted values are 0 and 1. • 0 = Do not create firewall rules • 1 = Create firewall rules (DEFAULT) **EXAMPLE**: CREATE_FIREWALL_RULES=1
DATABASE_AUTOBACKUP	Back up the Directory database after the software upgrade, but before the database upgrade. Configuration Files are also backed up in the same destination folder as the database. Accepted values are 0 and 1. When this option is omitted, the default value is 1 if the last backup is more than one day old. The default backup folder is *C:\SecurityCenterBackup* on the SQL Server machine. • 0 = Do not back up the Directory database • 1 = Back up the Directory database (DEFAULT) **EXAMPLE**: DATABASE_AUTOBACKUP=0
DATABASE_SERVER	Same as GLOBAL_SERVER option. This parameter maintains backward compatibility with previous silent installation scripts.
DEACTIVBASIC	This is a Boolean value that specifies whether basic camera authentication should be deactivated. • 0 = Basic authentication enabled • 1 = Basic authentication disabled (DEFAULT) **EXAMPLE**: DEACTIVBASIC=0
GLOBAL_SERVER	Specify the database server name for all roles installed by default. When omitted, the default value is (local)\SQLEXPRESS. **EXAMPLE**: GLOBAL_SERVER=BLADE32\SQLServerEnterprise

Security Center option	Description
LANGUAGECHOSEN	Language used by Security Center. The possible code values are: • Arabic - 1025 • Chinese (Simplified) - 2052 • Chinese (Traditional) - 1028 • Czech - 1029 • Dutch - 1043 • English - 1033 • French - 3084 • German - 1031 • Hebrew - 1037 • Hungarian - 1038 • Italian - 1040 • Japanese - 1041 • Korean - 1042 • Norwegian - 1044 • Persian - 1065 • Polish - 1045 • Brazilian Portuguese - 2070 • Russian - 1049 • Spanish - 1034 • Swedish - 1053 • Thai - 1054 • Turkish - 1055 • Vietnamese - 1066 **EXAMPLE**: LANGUAGECHOSEN=3084 If the code is invalid, English will be used. If this option is omitted, the installation language (specified with the /language: setup option) will be used.
MAINSERVER_ENDPOINT	Used for expansion server installation. Specify the name or IP address of the main server. **EXAMPLE**: MAINSERVER_ENDPOINT=MYMAINSERVER
MAINSERVER_PASSWORD	Mandatory option for server installation commands. **IMPORTANT**: The password must meet the following requirements: • At least 8 characters long • 1 or more upper case letters • 1 or more lower case letters • 1 or more numerical characters • 1 or more special characters • No spaces or double quotation marks. **EXAMPLE**: MAINSERVER_PASSWORD=ServerPwd-123

Security Center option	Description
PRODUCT_UPDATES	Turn the automatic check for software updates ON or OFF. Possible values are: • true - Turn the automatic check ON (DEFAULT) • false - Turn the automatic check OFF
SAMA_COLLECTPOLICY	Configure the data collection policy applied by the SAMA. The accepted values are: • On: SAMA will collect data with system information (requires ACTIVATIONCODE). • Anonymous: SAMA will collect anonymous data (DEFAULT) • Off: SAMA will not collect data. **EXAMPLE**: SAMA_COLLECTPOLICY=On ACTIVATIONCODE=mycode
SECURE_COMMUNICATION	This is a Boolean value that specifies whether secure communication (Directory authentication) should be enforced. • 0 = Not enforced, Directory authentication turned off (DEFAULT) • 1 = Enforced, Directory authentication turned on **EXAMPLE**: SECURE_COMMUNICATION=1
SERVER_TYPE	Specify whether to install a main or an expansion server. The accepted values are: • Main: Install Genetec™ Server with Directory (DEFAULT) • Expansion: Install Genetec™ Server without Directory
SERVERADMIN_PORT	Specify the HTTP port for the web-based Server Admin. **EXAMPLE**: SERVERADMIN_PORT=8080 If not specified, the default is 5500.
SERVICEPASSWORD	Specify the password to use in the services. **EXAMPLE**: SERVICEPASSWORD=anypassword **IMPORTANT**: • The username and password must be created first with the right credentials before using those properties. If not specified, the default is blank. • Double quotation marks cannot be part of the password. However, you can use them to wrap your password if you want to include a space. For example: SERVICEPASSWORD="abc efg".
SERVICEUSERNAME	Specify the username to use in the services. **EXAMPLE**: SERVICEUSERNAME=.\admin
SKIPSERVICESTART	Use this option to prevent the Security Center services from starting immediately after the installation (default behavior). You can use this option, if for example, you need to install hotfixes right after the full installation. If you use this option, don't forget to start the Security Center services (NET START GenetecServer and NET START GenetecWatchdog) after the hotfix installation. **EXAMPLE**: SKIPSERVICESTART=Y

Security Center option	Description
SKIPSQLVALIDATION	Use this option if your instance of SQL Server is not available at the time of installation, so the installer will not attempt to connect to it to validate its version. **EXAMPLE**: SKIPSQLVALIDATION=1 When this option is turned on, the ALLOWSQLUPGRADE option is ignored.
SQL_INSTANCE_NAME	This option must be specified when SQLSERVER_GROUP is set to NewServer. It specifies name of the SQL Server instance you want to create on your local machine. **IMPORTANT:** Do not add the server name to the instance name. **EXAMPLES**: • **WRONG:** SQL_INSTANCE_NAME=(local)\SQLEXPRESS2 • **CORRECT:** SQL_INSTANCE_NAME=SQLEXPRESS2
SQLSERVER_GROUP	Specify if a new or an existing SQL Server is silently installed. The accepted values are: • ExistingServer (DEFAULT) • NewServer (must be used with SQL_INSTANCE_NAME) **EXAMPLE**: SQLSERVER_GROUP=NewServer SQL_INSTANCE_NAME=SQLEXPRESS2
UPGRADE_DATABASE	Specify that the Directory database should be automatically upgraded. If no database exists, this option is ignored. Possible values are Y or N. When this option is omitted, the default value is Y. **EXAMPLE**: UPGRADE_DATABASE=N
WEBSERVER_PORT	Specify the HTTP port for the web-based Server Admin. If not specified, the default is 80.

Sample Security Center Server installation commands

Using the different command options, you can customize your Security Center Server silent installation.

Example

Genetec™ Server with the Directory is installed in English with a specific Username and Password for the service to run under. The files are installed in *C:\MyFolder*. The log files are saved to *C:\MyLogs*. The database server is specified. The data collection policy is set to ON. Setup runs in silent mode without any questions.

```
"Security Center Setup.exe" /silent /language:1033 /ISFeatureInstall=Server /
ISInstallDir=C:\MyFolder /debuglog"C:\MyLogs\Intall.log" /log"C:\MyLogs"
 AGREETOLICENSE=Yes COLLECTPOLICY=On SERVICEUSERNAME=.\toto SERVICEPASSWORD=password
 GLOBAL_SERVER=(local)\Genetec MAINSERVER_PASSWORD=ServerPwd-123
```

Example

A standard installation of Genetec™ Server as the main server, without any questions. The data collection policy is set to anonymous. The installation path is C:\GENETEC_PATH.

```
"Security Center Setup.exe" /language:1033 /silent /ISInstallDir=c:
\GENETEC_PATH /ISFeatureInstall=Server AGREETOLICENSE=Yes COLLECTPOLICY=Anonymous
 MAINSERVER_PASSWORD=ServerPwd-123
```

Example

A standard installation of Genetec™ Server as an expansion server, without any questions. Only the installation path is different.

```
"Security Center Setup.exe" /language:1033 /silent /ISInstallDir=c:
\GENETEC_PATH /ISFeatureInstall=Server AGREETOLICENSE=Yes SERVER_TYPE=Expansion
 MAINSERVER_PASSWORD=ServerPwd-123
```

Example

A standard installation in French in silent mode, with the data collection policy set to OFF, without any questions.

```
"Security Center Setup.exe" /language:3084 /silent AGREETOLICENSE=Yes
 COLLECTPOLICY=Off MAINSERVER_PASSWORD=ServerPwd-123
```

Example

A complete installation in English, with Omnicast™ compatibility packs 4.7 and 4.8, in silent mode without any questions. The default database server name, (local)\SQLExpress, is used for the Directory.

```
"Security Center Setup.exe" /
ISFeatureInstall=Client,Server,CompPacks,CompPack47,CompPack48 /language:1033 /silent
 AGREETOLICENSE=Yes COLLECTPOLICY=On MAINSERVER_PASSWORD=ServerPwd-123
```

Example

A complete installation in English, in silent mode, with the data collection policy set to anonymous, without any questions. This setup will create a log file located in C: drive.

```
"Security Center Setup.exe" /language:1033 /silent /ISFeatureInstall=Client,Server /
log"C:\" /debuglog"C:\DebugLog.log" AGREETOLICENSE=Yes COLLECTPOLICY=Anonymous
 MAINSERVER_PASSWORD=ServerPwd-123
```

Example

A complete installation in English, in silent mode without any questions. Security Center applications will use Arabic.

```
"Security Center Setup.exe" /language:1033 /silent /ISFeatureInstall=Client,Server
 AGREETOLICENSE=Yes COLLECTPOLICY=On LANGUAGECHOSEN=1025
 MAINSERVER_PASSWORD=ServerPwd-123
```

Sample Security Center Client installation commands

Using the different command options, you can customize your Security Center Client silent install.

Example

Security Desk is installed in English, in silent mode without any questions. The log files are saved to *C:\MyLogs*.

```
"Security Center Setup.exe" /language:1033 /silent /ISInstallDir=c:\GENETEC_PATH /
ISFeatureInstall=SecurityDesk /debuglog"C:\MyLogs\Intall.log" /log"C:\MyLogs"
 AGREETOLICENSE=Yes
```

Example

Config Tool and Security Desk are installed in French, in silent mode without any questions.

```
"Security Center Setup.exe" /language:3084 /silent /ISInstallDir=c:\GENETEC_PATH /
ISFeatureInstall=ConfigTool,SecurityDesk AGREETOLICENSE=Yes
```

Example

Config Tool and Security Desk are installed in English, in silent mode without any questions.

```
"Security Center Setup.exe" /language:1033 /silent /ISInstallDir=c:\GENETEC_PATH /
ISFeatureInstall=ConfigTool,SecurityDesk AGREETOLICENSE=Yes
```

Example

A typical Installation in French, in silent mode without any questions.

```
"Security Center Setup.exe" /language:3084 /silent AGREETOLICENSE=Yes
 MAINSERVER_PASSWORD=serverpassword
```

Example

A complete installation in English, with Omnicast™ compatibility pack 4.8, in silent mode without any questions.

```
"Security Center Setup.exe" /ISFeatureInstall=Client,Server,CompPacks,CompPack48 /
language:1033 /silent AGREETOLICENSE=Yes MAINSERVER_PASSWORD=serverpassword
```

Example

A complete installation in English, in silent mode without any questions. Security Center applications will use Arabic.

```
"Security Center Setup.exe" /language:1033 /silent /ISFeatureInstall=Client,Server
 AGREETOLICENSE=Yes LANGUAGECHOSEN=1025 MAINSERVER_PASSWORD=serverpassword
```

Uninstalling Security Center 5.10 in silent mode

Security Center can be uninstalled in silent mode.

To uninstall Security Center (Client and Server components) in silent mode:

- Run the following command from the *SC Packages* folder of the Security Center installation package:

```
"Security Center Setup.exe" /silent /remove
```

Silent installation options for Security Center SDK

You can install the Security Center SDK from a separate package instead of using the full Security Center installation package. If you are using this separate package, be aware that the silent SDK installation options are slightly different from those of Security Center.

Command syntax

The syntax for running the setup in silent mode is:

```
setup.exe /debuglog<setupLog> /s /v"/qn /l*v <msiLog> <SDK_options>"
```

where:

- setup.exe is the setup program found in the root folder of the SDK installation package.
- <setupLog> is the path to the setup log file. The folder path must exist. The setup program will not create it.
- <msiLog> is the path to the MIS log file. The folder path must exist. The setup program will not create it.
- <SDK_options> are the Security Center SDK options.

  An option follows the <option>=<value> syntax, where <option> is written in all caps. No space is allowed on either side of the equal sign (=). If the value contains spaces, the value must be included between double quotes.

SDK options

The following table describes the SDK options.

SDK option	Description
AGREETOLICENSE	Indicate that you agree with our software license agreement. **IMPORTANT:** The only accepted value is Yes. If omitted, the installation will fail. **EXAMPLE:** AGREETOLICENSE=Yes
CREATE_FIREWALL_RULES	Add the installed Security Center applications to the Windows Firewall exceptions list. Accepted values are 0 and 1. • 0 = Do not create firewall rules • 1 = Create firewall rules (DEFAULT) **EXAMPLE:** CREATE_FIREWALL_RULES=1
INSTALLDIR	Specify the folder where the SDK package is installed. The default is [ProgramFilesFolder]Genetec Security Center <version> SDK

Sample command line

```
setup.exe /debuglog"C:\Users\Public\prereqinstall.log"
  /s /v"/qn /l*v "C:\Users\Public\sdkmsi.log"
  AGREETOLICENSE=Yes CREATE_FIREWALL_RULES=0 INSTALLDIR="C:\NewFolder""
```

4

Troubleshooting

This section includes the following topics:

- "Disabling the SQL Server telemetry service manually" on page 139
- "Cameras stop working after installing Security Center with the default security options" on page 140
- "Error when installing Microsoft .NET Framework, Return Code: 0x800f081f" on page 141
- "Video stability and performance issues" on page 142
- "Files remain blocked after unblocking them manually" on page 143
- "One or more services failed to install" on page 144

Disabling the SQL Server telemetry service manually

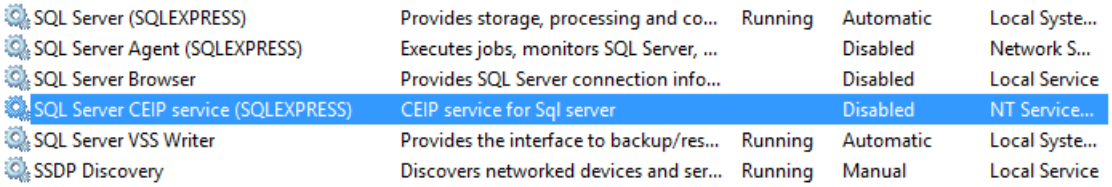
If the Security Center Installer fails to disable the SQL Server telemetry service, you can disable it manually after Security Center is installed.

What you should know

Microsoft installs the SQL Server Telemetry or CEIP (Customer Experience Improvement Program) Services as part of the SQL Server 2019 Express Edition installation. The telemetry service sends feature usage info back to Microsoft. The Security Center Installer always tries to disable this service. When it fails, you get a warning message at the end of the Security Center installation so you can disable it manually.

To disable the SQL Server telemetry service manually:

1 Run *services.msc* in Windows, and disable the **SQL Server CEIP service**.



2 In the Windows **Start** menu, type `regedit`, and then press **ENTER**.

3 In the *Registry Editor*, set the following registry entries to zero (0):

- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\150
  - CustomerFeedback REG_DWORD
  - EnableErrorReporting REG_DWORD
- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Microsoft SQL Server\150
  - CustomerFeedback REG_DWORD
  - EnableErrorReporting REG_DWORD
- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server \MSSQL15.<InstanceName>\CPE
  - CustomerFeedback REG_DWORD
  - EnableErrorReporting REG_DWORD

Cameras stop working after installing Security Center with the default security options

After installing Security Center using default security settings, cameras that do not support digest access authentication might not work. To fix this issue, you can reactivate basic access authentication by video unit or by manufacturer.

What you should know

Digest access authentication is the authentication scheme that the majority of recent video unit models support. This authentication scheme is more secure than basic access authentication because the passwords are hashed before sending them over the network. For this reason, basic access authentication is disabled by default. After installation, if you realize that some of your cameras do not support digest access authentication, you can revert them to basic access authentication in Config Tool.

For added security, Security Center remembers whether or not a specific video unit supports the digest authentication scheme. After the system has successfully authenticated to a video unit using the digest scheme, you cannot revert to the less secure basic scheme. You can see the authentication scheme used for each camera in the *Hardware inventory* report.

To revert to the basic authentication scheme on a specific video unit:

1. From Config Tool, open the *Hardware inventory* task.
2. Run the report on the video units that are inactive (in red) in your system.
   You might need to scroll horizontally to the right to see the **Authentication scheme** column.
3. In the report pane, select the video units that are inactive and click **Reset authentication scheme**.
   The **Authentication scheme** changes to **Anonymous**. After the Archiver successfully connects to the video unit, the exact authentication scheme is displayed.

To revert to the basic authentication scheme for a specific manufacturer:

1. From Config Tool, open the *Video* task.
2. Select the Archiver role that controls your cameras and click **Extensions**.
3. Select the manufacturer you want and set **Refuse basic authentication** to **OFF**.
4. Click **Apply**.

Error when installing Microsoft .NET Framework, Return Code: 0x800f081f

If your Security Center installation on a Windows 10 machine is interrupted with the return code 0x800f081f, you must use your Windows 10 installation disk (or a virtual copy of it) to turn on *.NET Framework 3.5*, and rerun the Security Center installation.

What you should know

Security Center requires the feature .NET Framework 3.5 to be turned on in order to work. Security Center installer turns .NET Framework 3.5 on by default. However, this feature cannot be turned on if you are missing the .NET 3.5.1 files, which causes the error 0x800f081f.

To fix the Microsoft .NET Framework installation error 0x800f081f:

1. Get a copy of the Windows 10 installation disk (or a virtual copy of it) from your IT department, and make sure it is accessible from the computer where Security Center needs to be installed.
2. Open a command prompt with full administrator rights.

   For more information, see Windows 10: Elevated Command Prompt.
3. Enter the following command:

   ```
   DISM /online /enable-feature /featurename:NetFx3 /All /Source:F:\sources\sxs
   ```

   where F: is the drive letter where the installation disk or virtual disk with the Windows 10 setup files are located.

   The command prompt will run through a repair and activation of the .NET framework feature.
4. Close the command prompt.
5. From the Windows Control Panel, open the *Programs and Features* applet and click **Turn Windows features on or off**.
6. In the *Windows Features* dialog box, click **.NET Framework 3.5**, and then click **OK**.
7. Rerun the Security Center installation.

Video stability and performance issues

After installing Security Center, you might have to install some Microsoft hotfixes for Security Center to run smoothly.

What you should know

The following scenarios require that you install a Microsoft hotfix:

- You log on to Config Tool or Security Desk after installing Security Center and you receive the message: "A necessary dependency for this application has not been found on the system. Video stability and performance are not guaranteed without the hotfix KB2494124/KB2468871".

To install the Microsoft hotfixes:

1. Close Config Tool and Security Desk.
2. Download the required hotfixes from the Internet:
   - For a 64-bit system, download the following files:
     - *NDP40-KB2468871-v2-IA64.exe*
     - *NDP40-KB2468871-v2-x64.exe*
     - *NDP40-KB294124-x64.exe*
     - *Windows6.1-KB2588507-v2-x64.msu*
   - For a 32-bit system, download the following files:
     - *NDP40-KB2468871-v2-x86.exe*
     - *NDP40-KB294124-x86.exe*
3. Run the hotfixes you've downloaded one after another, in the same sequence you downloaded them.
4. Restart your computer.

Files remain blocked after unblocking them manually

Use *streams.exe* to unblock Security Center installation package files that remain blocked after manual intervention.

What you should know

Only run *streams.exe* on files that remain blocked after attempting to manually unblock them. If the installation package contains blocked files, the following error message can show during installation: “Setup detected blocked file(s) in the download package. Setup will stop. To restart the installation, unblock the downloaded package.”

To unblock files using *streams.exe*:

1. Download *streams.exe* from https://technet.microsoft.com/en-ca/sysinternals/bb897440.aspx.
2. Open a command prompt window.
3. Enter `streams.exe -d <filename>`, where <*filename*> is the name of the file that needs to be unblocked.

After you finish

If you unblocked the entire ZIP installation package (not specific files contained in it), you must extract the package again prior to installing Security Center.

One or more services failed to install

If one or more Security Center services failed to install, you can uninstall Security Center and then reinstall it, or you can create the missing services manually.

Before you begin

Ensure that the username and password for *Service Logon* are entered correctly.

The valid username formats are:

- DOMAIN\username; Example: GENETEC\jsmith
- username@domain.local; Eample: jsmith@genetec.com

What you should know

The following services are created during a Security Center installation:

- Genetec™ Server
- Genetec™ Watchdog

If the Microsoft Management Console (MMC) is open while upgrading Security Center, these services might be locked, preventing one or both of them from being upgraded.

To manually create Security Center services:

1 On the computer that is missing Security Center services, open an elevated *Command Prompt* as Administrator.

2 If the Genetec™ Watchdog service is missing, create it manually:

a) In the *Administrator: Command Prompt* window, run the following command:

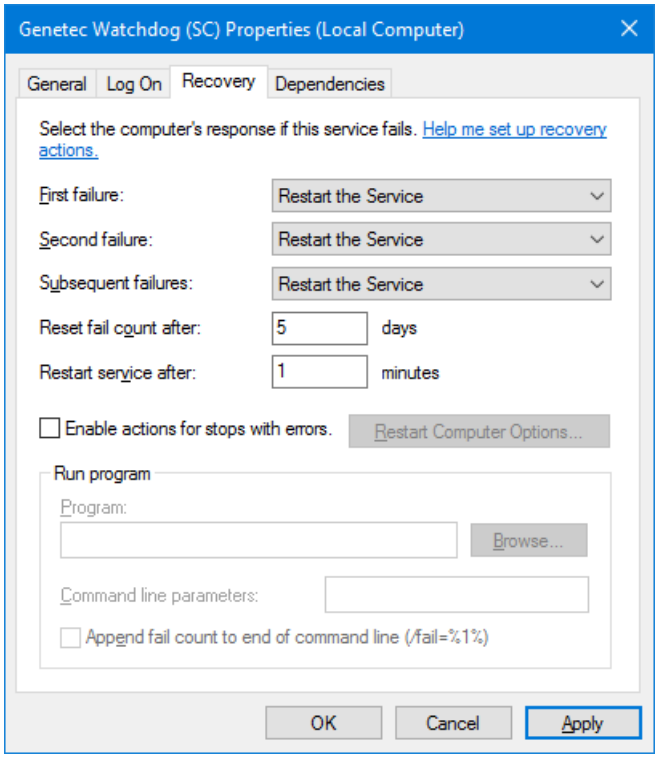
IMPORTANT: On 64-bit computers, the default installation folder is *C:\Program Files (x86)\Genetec Security Center 5.10*. This path must be changed if Security Center was installed to another location.

```
sc create GenetecWatchdog binPath= "C:\Program Files (x86)\Genetec Security
 Center 5.10\GenetecWatchdog.exe" start= auto DisplayName= “Genetec Watchdog
 (SC)”
```

b) In Windows, open the *Services* console.

c) In the *Services* console, open the properties of the **Genetec™ Watchdog (SC)** service, and click the **Recovery** tab.

d) Set the recovery options to match the following screen capture, and click **Apply**.



e) Start the **Genetec™ Watchdog (SC)** service.

3 If the Genetec™ Server service was created but is missing dependencies, run the following commands in the *Administrator: Command Prompt* window:

```
sc config GenetecServer binPath= "C:\Program Files (x86)\Genetec Security
 Center 5.10\GenetecServer.exe" start= auto depend= GenetecWatchdog/Winmgmt
sc start GenetecServer
```

4 If the Genetec™ Server service is missing, run the following commands in the *Administrator: Command Prompt* window:

IMPORTANT: On 64-bit computers, the default installation folder is *C:\Program Files (x86)\Genetec Security Center 5.10*. This path must be changed if Security Center was installed to another location.

```
sc create GenetecServer binPath= "C:\Program Files (x86)\Genetec Security
 Center 5.10\GenetecServer.exe" start= auto depend= GenetecWatchdog/Winmgmt
 DisplayName= “Genetec Server”
sc start GenetecServer
```

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.