Genetec™
Security Center.

Security Center Installation and Upgrade Guide 5.8 GA

Click here for the most recent version of this document.

Document last updated: September 25, 2019

Genetec™

Legal notices

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.

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™, Citywise™, Community Connect™, Genetec Citigraf™, Federation™, Flexreader™, Genetec Clearance™, Genetec Retail Sense™, Genetec Traffic Sense™, Genetec Airport Sense™, Genetec Motoscan™, Genetec Mission Control™, Genetec ClearID™, Genetec Patroller™, Omnicast™, Stratocast™, Streamvault™, Synergis™, 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.

KiwiSecurity™, KiwiVision™, Privacy Protector™ and their respective logos are trademarks of KiwiSecurity Software GmbH, 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™, 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

Document number: EN.500.002-V5.8.B(2)

Document update date: September 25, 2019

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

Chapter 1: Installing Security Center

Chapter 2: Upgrading to Security Center 5.8

Chapter 3: LPR database migration

1

Installing Security Center

This section includes the following topics:

Preparing to install Security Center

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

What you should know

IMPORTANT: No server name can be longer than 15 characters. Security Center truncates all server names longer than the maximum limit to 15 characters, causing errors when the system tries to access those servers.

CAUTION: Do not use the image of a configured machine to install Security Center 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, then it will cause conflicts with the entities in the system sharing the identifiers. This may make the system unusable.

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.

Before installing Security Center:

1. Read the *Security Center Release Notes* for any known issues, limitations, and other information about the release.
2. If you plan to use restricted cameras, do the following:
   a) Contact your sales representative to obtain a special connection license for your restricted camera connections.
   b) Sign the “Exclusion of Liability and Hold Harmless” waiver.
3. 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.
   - Security Center Server (main or expansion server?)
   - Security Center Client (Config Tool, Security Desk, or both?)
   - SQL Server (Express, Standard, or Enterprise edition?)
4. Review the system requirements to ensure that the minimum hardware requirements (servers and workstations) and software requirements (Windows, web browser, and so on) are met. For Security Center 5.8 GA system requirements, refer to the *Security Center System Requirements Guide*.
5. Read the Best practices for configuring Windows to work with Security Center.

   You will have to follow these recommendations after you have installed Security Center to ensure the optimal performance of your system.
6. If you are running Windows 7 SP1 or Windows Server 2008 R2 SP1, you must install Microsoft hotfix 2588507 followed by update 2999226.
7. If you are running Windows 8.1 or Windows Server 2012 R2, you must install Microsoft update 2919355 followed by 2999226.
8. 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.
9. Verify the unicast and multicast network connections and settings.

   Security Center does not modify your network infrastructure or how it works. Multicast will work with Security Center out of the box automatically, as long as the network supports it with 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.

10 Read the Security Center 5.8 GA installation prerequisites.

Security Center Installer automatically verifies and installs the software prerequisites on your system but it is good practice to know what they are beforehand.

11 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.

12 Make sure you have administrative privileges. If not, then the installation *setup.exe* must be run as administrator.

You may need to be a Microsoft Windows Domain administrator to access databases and storage on the machines. Check with your IT administrator.

13 (For Directory failover or VSS operation) Install SQL Server on a separate drive.

14 Grant the service users all necessary SQL server permissions.

15 (Windows Server 2012 and Windows Server 2016) Activate the Media Foundation feature.

16 Download the Security Center installation package.

17 Unblock any blocked files.

After downloading the Security Center installation package, the ZIP files may need to be unblocked before their contents are extracted.

After you finish

Install Security Center.

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.

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 2014 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.

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://gtap.genetec.com/SystemManagement/DownloadSection/. Note, you'll need a username and password to log on to GTAP.

- **SecurityCenterWebSetup.exe:** This is the web installer. During the installation, the web installer downloads the necessary components for your system from the Internet.
- **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*.

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. The web installer connects to Genetec™ and only downloads the modules you choose to install.
  - **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 in Security Center on page 99

Security Center 5.8 GA 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
DirectX End-User Runtimes	✓	✓	✓	✓
Fsharp Redistributable Package 2.0	✓	✓	✓	✓
Microsoft .NET Framework 3.5 SP1 (Windows Feature)	✓	✓	✓	✓
Microsoft .NET Framework 4.7.1 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 2008 R2 SP3 Shared Management Objects	✓	✓		
Microsoft SQL Server 2008 R2 SP3 Shared Management Objects (x64)			✓	✓
Microsoft SQL Server 2008 System CLR Types v10.50.1600.1	✓	✓		
Microsoft SQL Server 2008 System CLR Types v10.50.1600.1 (x64)			✓	✓
Microsoft SQL Server 2012 Native Client v11.0.6538.0	✓	✓		
Microsoft SQL Server 2012 Native Client v11.0.6538.0 (x64)			✓	✓
Microsoft SQL Server 2012 System CLR Types v11.1.3000.0	✓	✓		
Microsoft SQL Server 2012 System CLR Types v11.1.3000 (x64)			✓	✓

	32-bit Client	32-bit Server	64-bit Client	64-bit Server
Microsoft SQL Server 2014 Shared Management Objects	✓	✓		
Microsoft SQL Server 2014 Shared Management Objects (x64)			✓	✓
Microsoft SQL Server Compact 4.0 SP1 (x86)	✓	✓		
Microsoft SQL Server Compact 4.0 SP1 (x64)			✓	✓
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 Visual C++ 2010 SP1 Redistributable Package (x64)			✓	✓
Microsoft Visual C++ 2012 Update 4 Redistributable Package (x86)	✓	✓	✓	✓
Microsoft Visual C++ 2013 Redistributable (x86)	✓	✓	✓	✓
Microsoft Visual C++ 2017 14.16.27027.0 Redistributable (x86)	✓	✓	✓	✓
Microsoft Visual C++ 2017 14.16.27027.0 Redistributable (x64)			✓	✓
MSMQ 3.0 and up[b]	✓	✓	✓	✓
Visual C++ 2008 SP1 Redistributable	✓	✓	✓	✓
Visual C++ 2010 Redistributable	✓	✓	✓	✓
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.

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 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 on a separate drive from the OS drive.

   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

For Security Center to work properly, you need to create firewall rules to allow proper communication between the various services.

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.

The following table lists the default network ports used by core applications in Security Center. To view the network diagram, click here.

Application	Inbound	Outbound	Port usage
Directory	TCP 5500		Client connections
Client applications (Security Desk, Config Tool, SDK)		TCP 5500	Genetec™ Server/Directory communication
		TCP 8012	Map download requests to Map Manager (HTTPS)
Client applications (Config Tool)		TCP 443	Communication with GTAP for Genetec™ Advantage validation and feedback (HTTPS)
Client applications (Security Desk, Config Tool)		TCP 443	Secured communication with the portal of the mobile credential provider (HTTPS)
All roles (new installation)	TCP 5500	TCP 5500	Genetec™ Server/Directory communication
	TCP 4502	TCP 4502	Genetec™ Server communication (backward compatibility with Security Center 5.3 and earlier)
	TCP 80	TCP 80	REST/Server Admin communication (HTTP)
	TCP 443	TCP 443	Secured REST/Server Admin communication (HTTPS)
All roles (upgraded from 5.3 and earlier)	TCP 4502	TCP 4502	If 4502 was the server port before the upgrade, then 4502 remains the server port after the upgrade, and 4503 is used for backward compatibility. If another port was used as server port before the upgrade, then that same port is kept as server port after the upgrade. 4502 is then used for backward compatibility, and 4503 is not necessary.
	TCP 4503	TCP 4503	
Intrusion Manager	TCP 3001	TCP 3001	Communication with Bosch intrusion panels
Map Manager	TCP 8012		Map download requests from client application (HTTPS)
Mobile Server	TCP 443		Communication from mobile clients.
Genetec™ Update Service (GUS)	TCP 4595	TCP 4595	Communication with other GUS servers
	TCP 443	TCP 443	Communication with Azure and Genetec Inc. (HTTPS)
System Availability Monitor Agent (SAMA)	TCP 4592		Connection from Security Center servers
		TCP 443	Connection to the Health Service in the Cloud (HTTPS)

Ports used by AutoVu™ applications in Security Center

When AutoVu™ is enabled in your system, you need to create additional firewall rules to allow proper communication between Security Center and external AutoVu™ components.

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.

The following table lists the default network ports used by AutoVu™ applications in Security Center. To view the network diagram, click here.

Application	Inbound	Outbound	Port usage
LPR Manager		UDP 5000	Fixed Sharp unit discovery
	TCP 8731		Fixed Sharp units and Genetec Patroller™ installations
	TCP 8787		Pay-by-Plate (plugin installed separately)
	TCP 8832		Updater service
	TCP 9001		LPM protocol listening port
		TCP 8001	Sharp control port (used for **Live** connections, not **LPM protocol** connections).
		TCP 2323	Sharp unit configuration (HTTP)
Flexreader™ (Sharp unit)	TCP 80		Video port (Security Center extension HTTP)
	TCP 443		Video port (Security Center extension HTTPS)
	TCP 2323		Extension configuration service (HTTP)
	TCP 4502-4534		Silverlight ports and image feed service (for Sharp models prior to SharpV)
	TCP 4545		Control port (Mobile installation)
	UDP 5000		Discovery port
	TCP 8001		Control port (Fixed installation)
		TCP 21	FTP file upload
		TCP 8666	Communication with Updater Service
Portal Server (Sharp unit)	TCP 80		Communication port (HTTP)
	TCP 443		Secure communication port (HTTPS)

Application	Inbound	Outbound	Port usage
Updater service (Sharp unit and in-vehicle computer)	TCP 8666		Communication with Flexreader™ (greetings only)
	TCP 8889	TCP 8899	Communication with Genetec Patroller™ Updater
		TCP 8832	Communication with LPR Manager
Genetec Patroller™ (in-vehicle computer)	TCP 4546		Communication with Time server
	TCP 8001		Communication with Simple Host
		UDP 5000	Sharp camera discovery
		TCP 8666	Communication with Updater Service (greetings only)
		TCP 8731	LPR Manager connection

Ports used by Omnicast™ applications in Security Center

When Omnicast™ is enabled in your system, you need to create additional firewall rules to allow proper communication between Security Center and external IP video devices.

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.

The following table lists the default network ports used by Omnicast™ applications in Security Center. To view the network diagram, click here.

Application	Inbound	Outbound	Port usage
Archiver	TCP 555[1]		Live and playback stream requests
	TCP 605[1]		Edge playback stream requests
	TCP 5602[1]		Telnet console connection requests
	UDP 6000-6500		Audio from client applications
	UDP 15000–19999[2]		Live unicast streaming from IP cameras
	UDP 47806, 47807	UDP 47806, 47807	Live video and audio multicast streaming
	TCP & UDP		Vendor specific ports for events and IP camera discovery
		TCP 80	HTTP port
		TCP 443	HTTPS port
		TCP 554	RTSP port

Application	Inbound	Outbound	Port usage
Redirector	TCP 560, 960[3]		Live and playback stream requests
		TCP 554	Communication with Media Router (Security Center Federation™)
		TCP 555	Communication with Archiver
		TCP 558	Communication with Auxiliary Archiver
		TCP 560, 960[3]	Stream requests to other redirectors
		UDP 6000-6500	Media transmission to client applications
	UDP 8000–12000	UDP 8000–12000	Media transmission to other redirectors
	UDP 47806, 47807	UDP 47806, 47807	Live video and audio multicast streaming
Auxiliary Archiver	TCP 558		Live and playback stream requests
	UDP 15000–19999[2]		Live unicast streaming (IP cameras)
	UDP 47806, 47807	UDP 47806, 47807	Live video and audio multicast streaming
		TCP 554, 560, 960[3]	Live and playback stream requests
Media Router	TCP 554		Live and playback stream requests
		TCP 554	Federated Media Router stream requests
Media Gateway	TCP 654		Live and playback stream requests
	UDP 6000-6500		Live video unicast streams
	UDP 47806	UDP 51914	Live video multicast streaming
		TCP 554, 560, 960[3]	Live and playback video requests
Media processing applications (Privacy Protector™ and Camera integrity monitor)	TCP 754		Live video requests
	UDP 7000-7500		Live video unicast streams
	UDP 47806		Live video multicast streaming
		TCP 554, 560, 960[3]	Live and playback video requests
Omnicast™ Federation™		TCP 5001-5002	Connection to remote Omnicast™ 4.x systems.

Application	Inbound	Outbound	Port usage
Client applications (Security Desk and Config Tool)	UDP 6000–6200		Unicast media streams
	UDP 47806, 47807		Live video and audio multicast streams
		TCP 554, 560, 960[3]	Live and playback video and audio requests
Client application (Config Tool)		Vendor-specific TCP and UDP ports	Unit discovery with the Unit enrollment tool

[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 upgrades from Security Center 5.5 to 5.8. Systems upgraded from Security Center 5.6 and Security Center 5.7 will continue to use TCP port 5004.

Ports used by Synergis™ applications in Security Center

When Synergis™ is enabled in your system, you need to create additional firewall rules to allow proper communication between Security Center and external IP access control devices.

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.

The following table lists the default network ports used by Synergis™ applications in Security Center. To view the network diagram, click here.

Application	Inbound	Outbound	Port usage
Access Manager		UDP 2000	Synergis™ extension - discovery
		TCP 443	Secure communication with Synergis™ units and HID units (HTTPS)
	TCP 20	TCP 21	HID extension - FTP data and command[1]
		TCP 22	HID extension - SSH[1]
		TCP 23	HID extension - Telnet[1]
		TCP 80	HID extension - HTTP communication
		TCP 4050/4433[2]	HID extension - VertX OPIN protocol

Application	Inbound	Outbound	Port usage
	TCP/UDP 4070	TCP/UDP 4070	HID extension - VertX discovery[3]
	TCP/UDP		Vendor specific ports for events and discovery from IP access control device
Synergis™ Softwire (Synergis™ unit)	TCP 80	TCP 80	Communication port (HTTP)
	TCP 443	TCP 443	Secure communication port (HTTPS)
			AutoVu™ SharpV integration (HTTPS)
	UDP 2000	UDP 2000	Discovery and P2P communication
	TCP 3389		RDP connection (disabled by default)
		TCP 9999	Assa Abloy Aperio IP
	TCP 2571	TCP 2571	Assa Abloy IP lock (R3 protocol)
		UDP 5353	Axis controller discovery (mDNS)
	TCP 3001	TCP 3001	Mercury or Honeywell communication
	TCP 1234	TCP 1234	Salto Sallis lock communication
HID VertX/Edge Legacy and EVO controllers	TCP 21		FTP command[1]
	TCP 22		SSH port (EVO only)[1]
	TCP 23		Telnet[1]
	TCP 4050/4433[2]		VertX OPIN protocol
	UDP 4070	UDP 4070	VertX discovery

[1] Not required if HID units are configured with **Secure mode**.

[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. Once it is discovered, the unit is assigned to an Access Manager that uses the ports shown in the table above to control it.

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

Installing SQL Server on a separate drive

Depending on your deployment requirements, you might be required to install SQL Server on a drive that is separate from the system drive (typically the C: drive). You must perform this procedure before installing Security Center components.

Before you begin

If you are installing SQL Server Standard or Enterprise edition, you must purchase it from Microsoft, and download the installation package.

What you should know

You must install SQL Server on a separate drive in the following situations:

- You plan to set up Directory failover and load balancing. In this case, install SQL Server on a server that is different from all your Directory servers. 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.

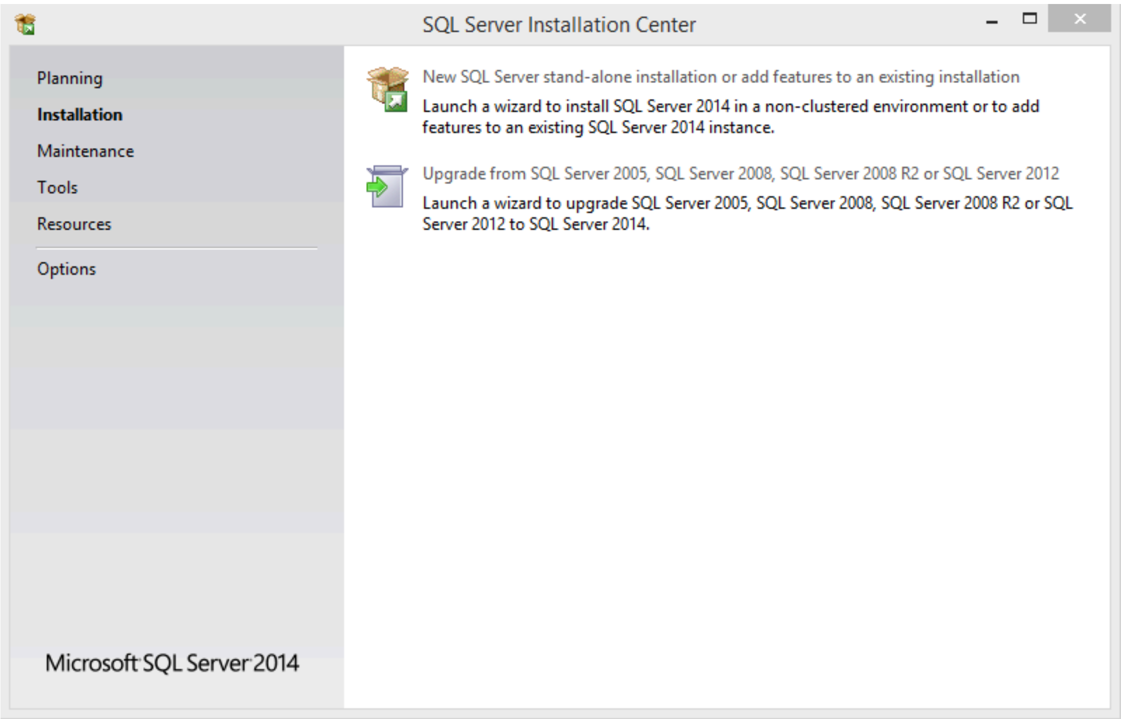
  CAUTION: Do not disable VSS. Disabling VSS interferes with the operation of Windows System Restore.

To install SQL Server on a separate drive:

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. Click **SC Packages** > **SQLExpress**.
     c. Double-click one of the following:
        - If you are on a 64-bit computer: *SQLEXRWT_x64_ENU.exe*.
        - If you are on a 32-bit computer: *SQLEXRWT_x86_ENU.exe*.

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

3 On the *Installation Type* page, select **New installation or add shared features**, and then click **Next**.



New SQL Server stand-alone installation or add features to an existing installation

Launch a wizard to install SQL Server 2014 in a non-clustered environment or to add features to an existing SQL Server 2014 instance.

Upgrade from SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012

Launch a wizard to upgrade SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012 to SQL Server 2014.

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

5 On the *Feature Selection* page, select the features you want to install.

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

7 Click **Next**.

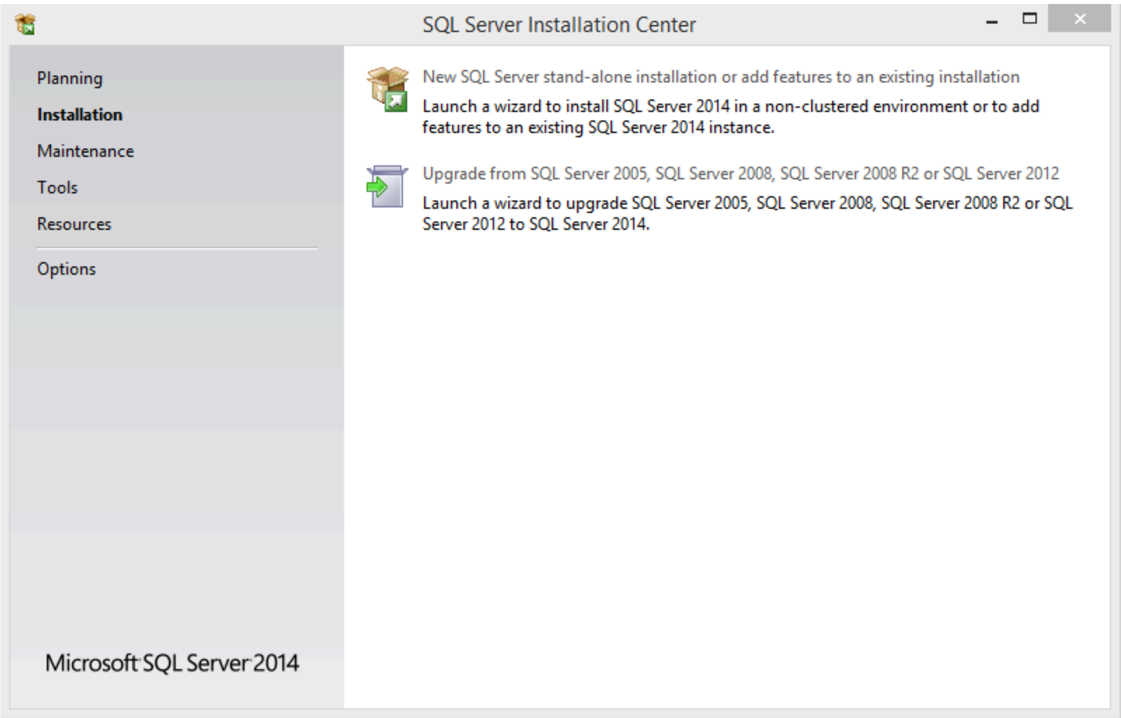
8 On the *Instance Configuration* page, select a name for the SQL Server.

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

- It cannot 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 In the **Instance root directory** field, select where to install the SQL Server and all directory database files, and click **Next**.

You can type a path, or browse for a folder.



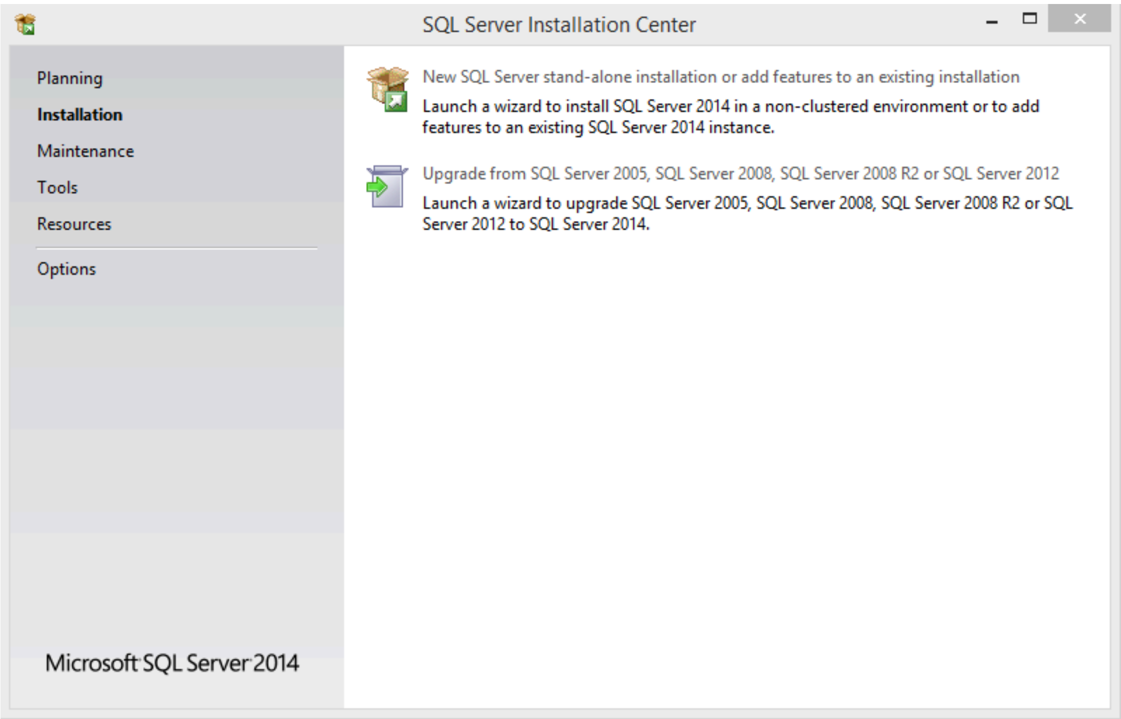
New SQL Server stand-alone installation or add features to an existing installation

Launch a wizard to install SQL Server 2014 in a non-clustered environment or to add features to an existing SQL Server 2014 instance.

Upgrade from SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012

Launch a wizard to upgrade SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012 to SQL Server 2014.

10 On the *Server Configuration* page, select the account name for each SQL Server service, and click **Next**.



New SQL Server stand-alone installation or add features to an existing installation

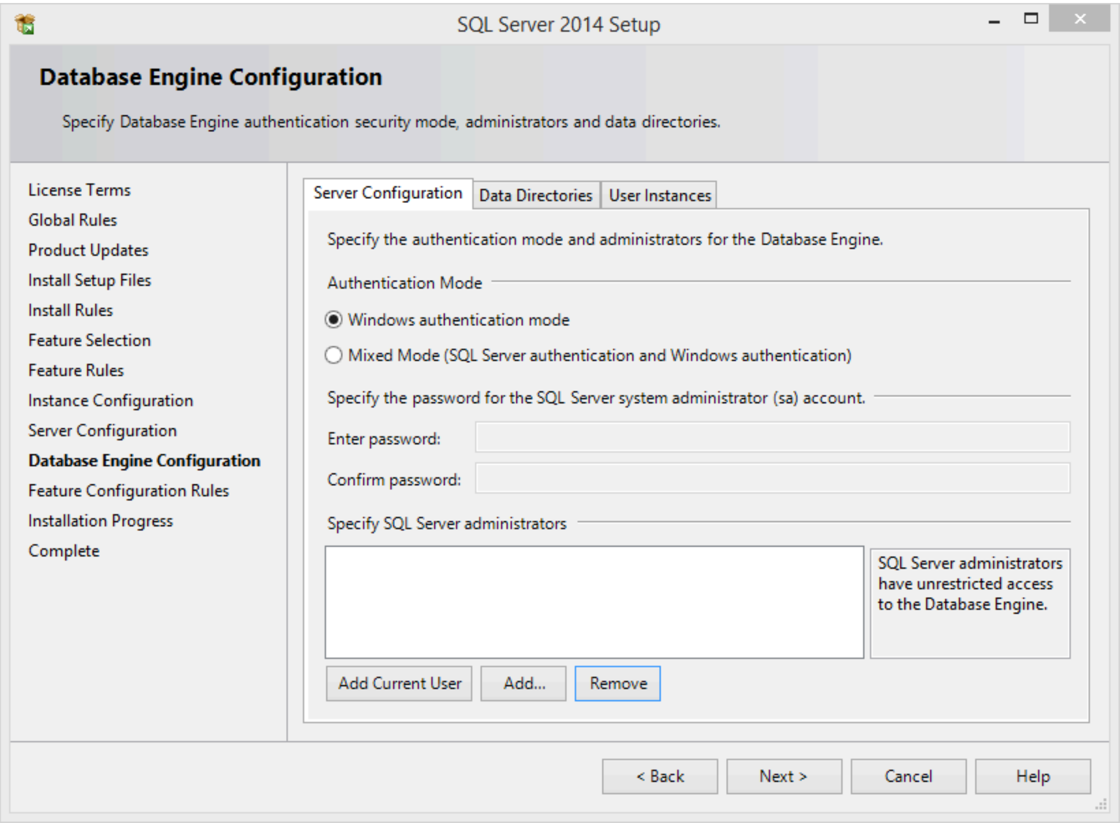
Launch a wizard to install SQL Server 2014 in a non-clustered environment or to add features to an existing SQL Server 2014 instance.

Upgrade from SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012

Launch a wizard to upgrade SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012 to SQL Server 2014.

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

- **Windows authentication mode:** Windows username and password.
- **Mixed mode:** Windows administrators can access the database engine using either their Windows credentials, or the password you specify here.



SQL Server 2014 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

● Windows authentication mode

○ Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password:

Confirm password:

Specify SQL Server administrators

SQL Server administrators have unrestricted access to the Database Engine.

12 On the *Error Reporting* page, specify if you want to send errors to Microsoft, and click **Next**.

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

14 Click **Close**.

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

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 100

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:

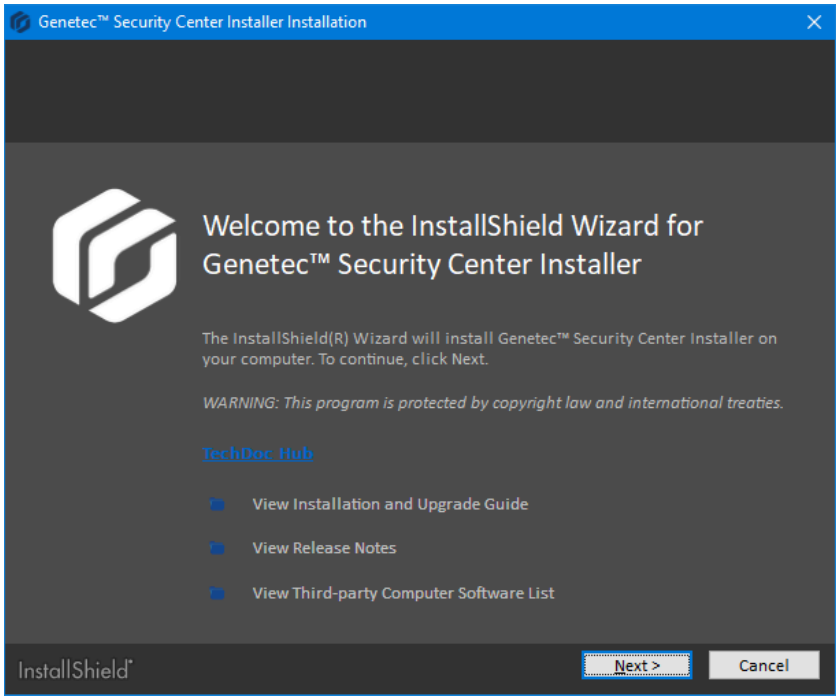
1 Right-click either *setup.exe* (standalone version) or *SecurityCenterWebSetup.exe* (web version), and click **Run as administrator**.

The InstallShield Wizard opens.

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

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

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



Genetec™ Security Center Installer Installation

Welcome to the InstallShield Wizard for Genetec™ Security Center Installer

The InstallShield(R) Wizard will install Genetec™ Security Center Installer on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

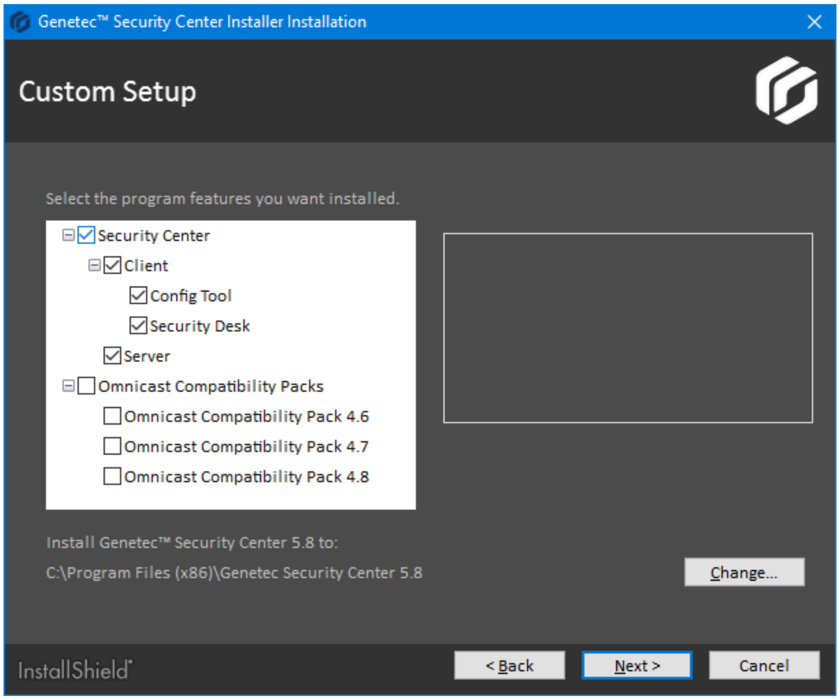
TechDoc Hub
View Installation and Upgrade Guide
View Release Notes
View Third-party Computer Software List
InstallShield
Next >
Cancel

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**.



Select the program features you want installed.

- ☑ Security Center
  - ☑ Client
    - ☑ Config Tool
    - ☑ Security Desk
  - ☑ Server
- □ Omnicast Compatibility Packs
  - □ Omnicast Compatibility Pack 4.6
  - □ Omnicast Compatibility Pack 4.7
  - □ Omnicast Compatibility Pack 4.8

Install Genetec™ Security Center 5.8 to:
C:\Program Files (x86)\Genetec Security Center 5.8

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 5.8* folder is created. On a 64-bit machine, the default root folder is *C:\Program Files (x86)*.

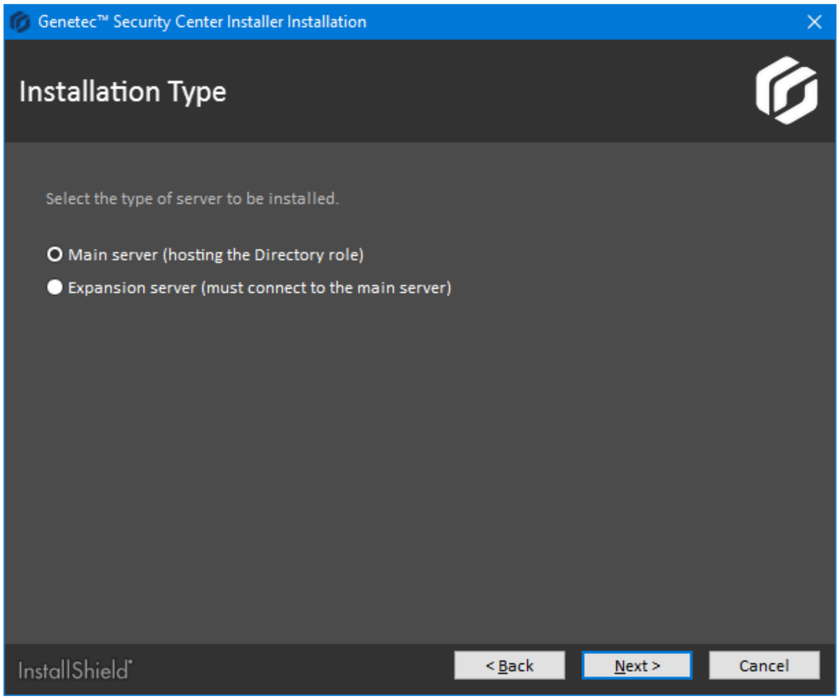
6 On the *Genetec™ Security Center Language Selection* page, select the user interface language for Security Center applications, and click **Next**.

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*.



Genetec™ Security Center Installer Installation

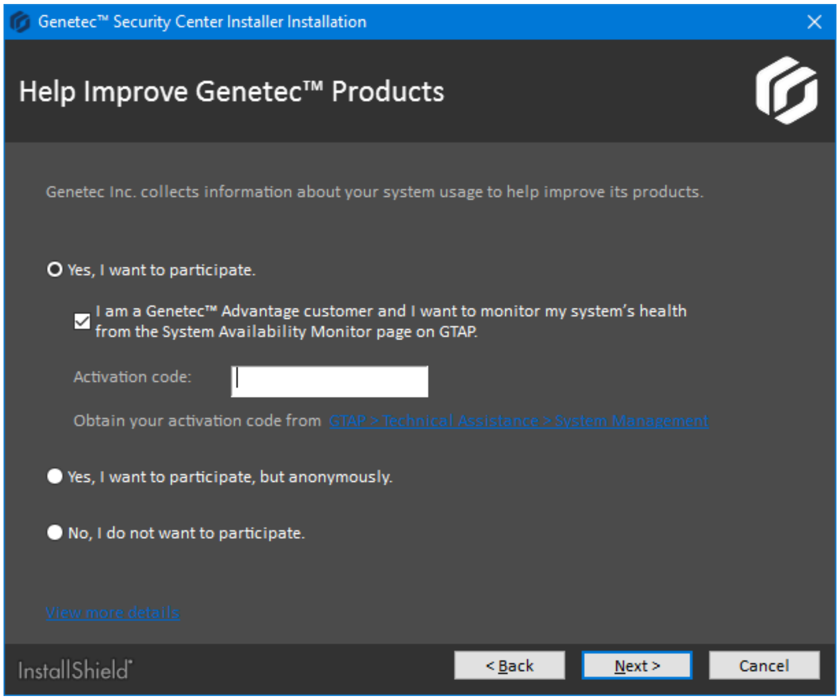
Installation Type

Select the type of server to be installed.

○ Main server (hosting the Directory role)

● Expansion server (must connect to the main server)

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



Genetec™ Security Center Installer Installation

Help Improve Genetec™ Products

Genetec Inc. collects information about your system usage to help improve its products.

○ Yes, I want to participate.

☑ I am a Genetec™ Advantage customer and I want to monitor my system's health from the System Availability Monitor page on GTAP.

Activation code:

Obtain your activation code from GTAP > Technical Assistance > System Management

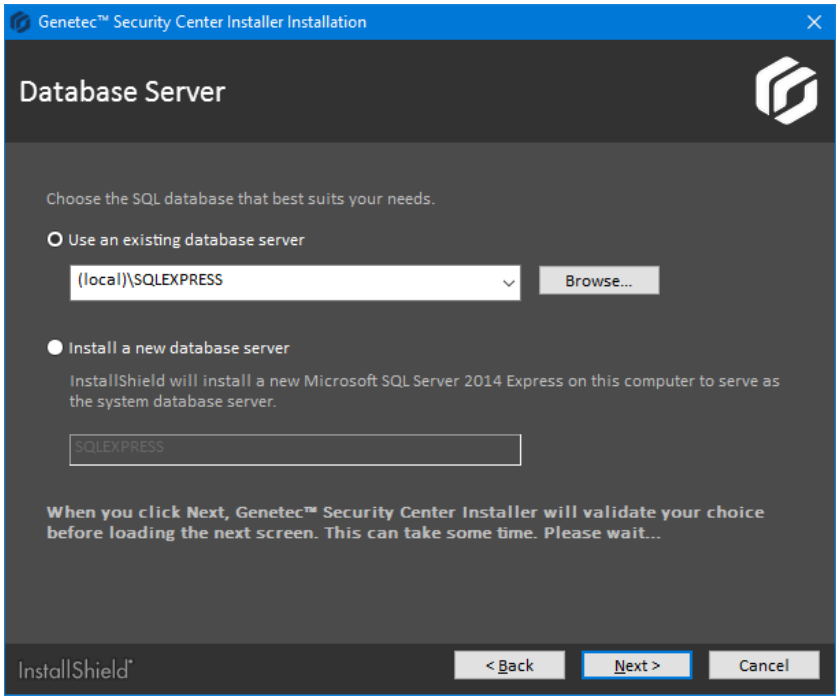
● Yes, I want to participate, but anonymously.

● No, I do not want to participate.

View more details

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**.



Genetec™ Security Center Installer Installation

Database Server

Choose the SQL database that best suits your needs.

○ Use an existing database server

(local)\SQLEXPRESS

● Install a new database server

InstallShield will install a new Microsoft SQL Server 2014 Express on this computer to serve as the system database server.

SQLEXPRESS

When you click Next, Genetec™ Security Center Installer will validate your choice before loading the next screen. This can take some time. Please wait...

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

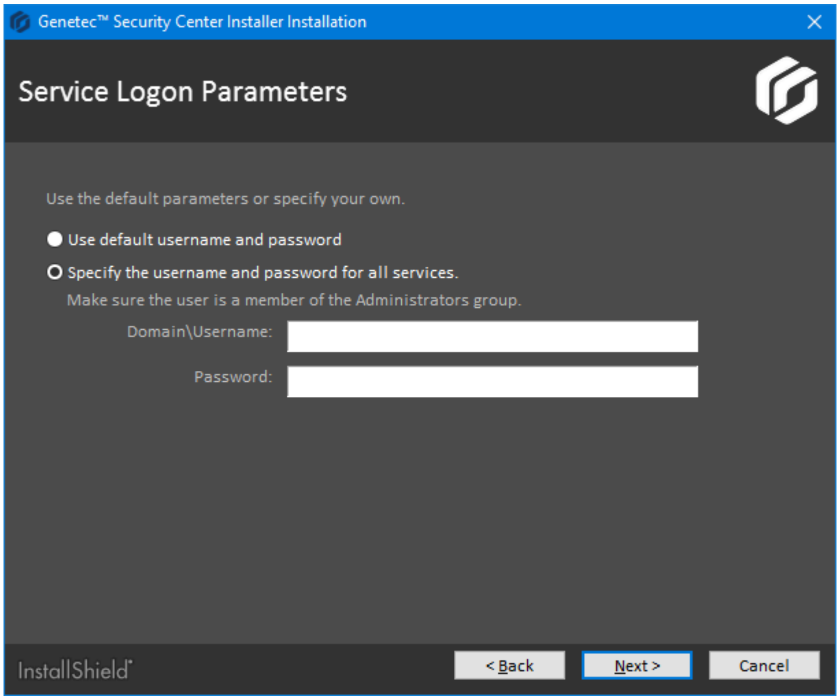
  If you are upgrading from a supported version of Security Center, the installer automatically upgrades all databases that your system requires.

- **Install a new database server:** Installs Microsoft SQL Server 2014 Express Edition on this machine. 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 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: \ , : ; ' & # @

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



Genetec™ Security Center Installer Installation

Service Logon Parameters

Use the default parameters or specify your own.

● Use default username and password

○ Specify the username and password for all services.

Make sure the user is a member of the Administrators group.

Domain\Username:

Password:

a) Select one of the following options:

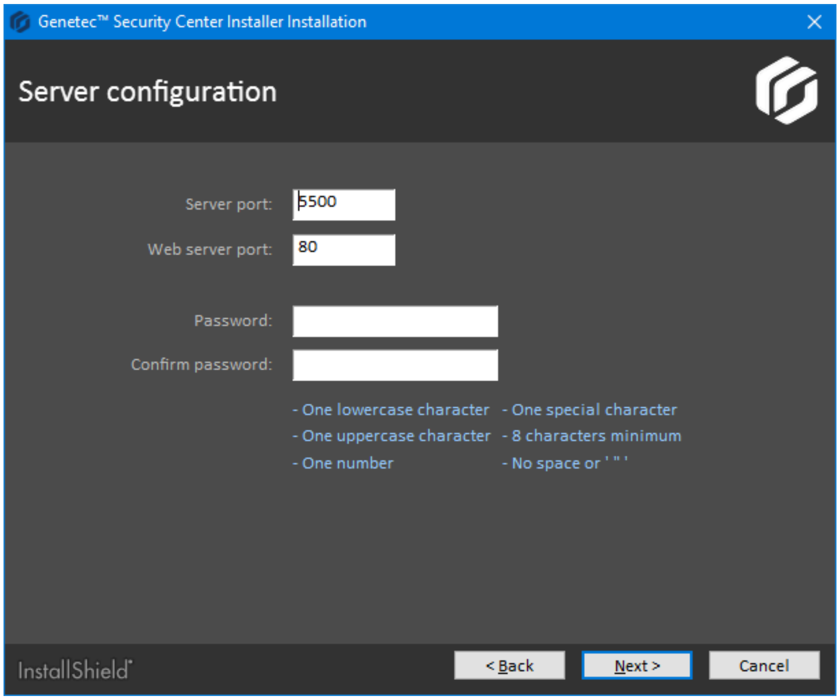
- **Use default name and password:** Use the default username (LocalSystem).
- **Specify the username and password for all services:** Enter a valid domain username and a strong password, and record them in a safe place. You must provide these credentials every time you upgrade your Security Center software. 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: You can change the service logon user later from Microsoft Management Console.

b) Click **Next**.

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



Genetec™ Security Center Installer Installation

Server configuration

Server port: 5500

Web server port: 80

Password:

Confirm password:

- One lowercase character - One special character
- One uppercase character - 8 characters minimum
- One number - No space or ' " '

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.

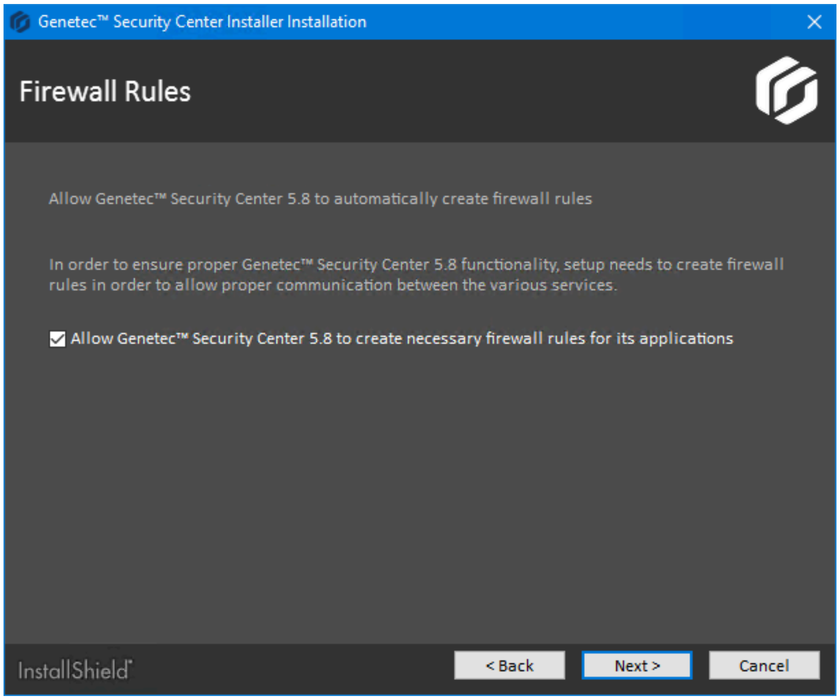
  CAUTION: Watch out for conflicts with other software, such as a Skype, running on the server that might use port 80.
- **Password/Confirm password:** Enter and confirm the password to open the web-based Server Admin.

  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**.



Allow Genetec™ Security Center 5.8 to automatically create firewall rules

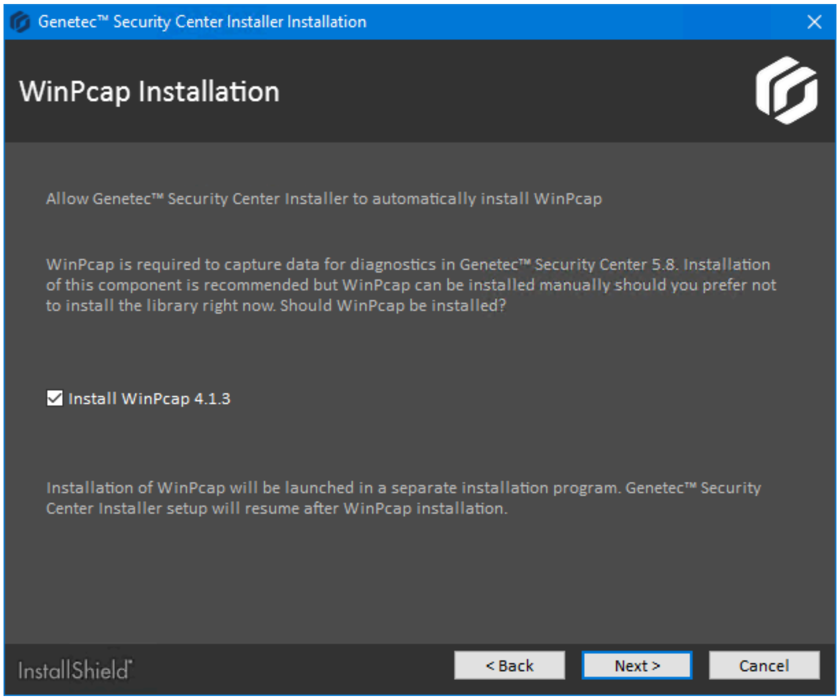
In order to ensure proper Genetec™ Security Center 5.8 functionality, setup needs to create firewall rules in order to allow proper communication between the various services.

☑ Allow Genetec™ Security Center 5.8 to create necessary firewall rules for its applications

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.

- 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**.



Allow Genetec™ Security Center Installer to automatically install WinPcap

WinPcap is required to capture data for diagnostics in Genetec™ Security Center 5.8. Installation of this component is recommended but WinPcap can be installed manually should you prefer not to install the library right now. Should WinPcap be installed?

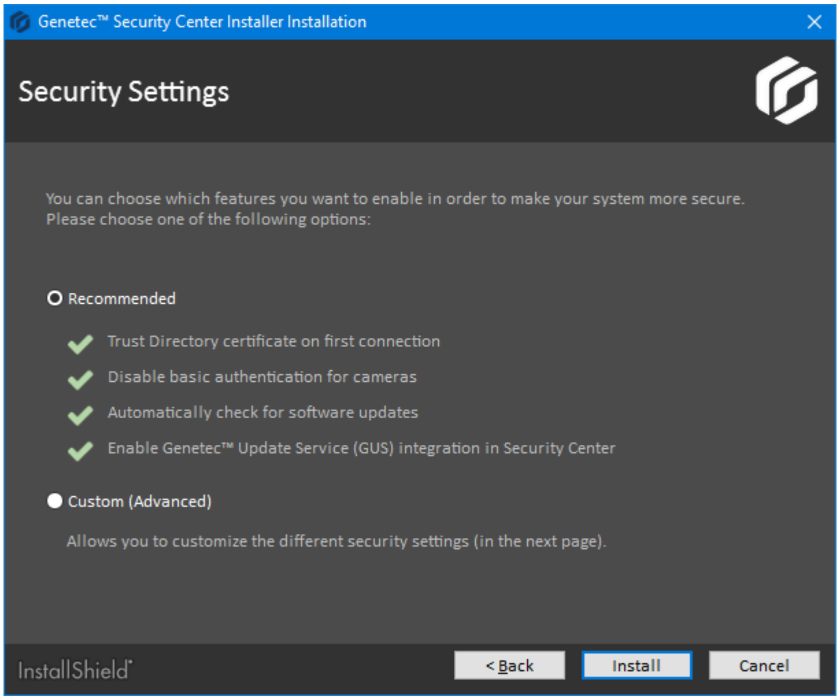
☑ Install WinPcap 4.1.3

Installation of WinPcap will be launched in a separate installation program. Genetec™ Security Center Installer setup will resume after WinPcap installation.

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.



Security Settings

You can choose which features you want to enable in order to make your system more secure.
Please choose one of the following options:

○ Recommended

✓ Trust Directory certificate on first connection

✓ Disable basic authentication for cameras

✓ Automatically check for software updates

✓ Enable Genetec™ Update Service (GUS) integration in Security Center

● Custom (Advanced)

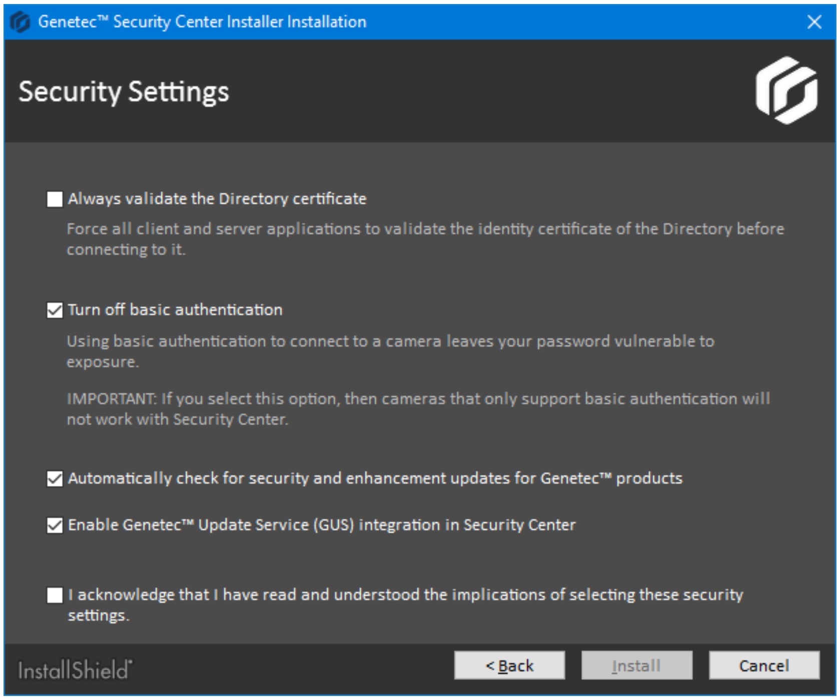
Allows you to customize the different security settings (in the next page).

- 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.



Genetec™ Security Center Installer Installation

Security Settings

□ Always validate the Directory certificate

Force all client and server applications to validate the identity certificate of the Directory before connecting to it.

☑ Turn off basic authentication

Using basic authentication to connect to a camera leaves your password vulnerable to exposure.

IMPORTANT: If you select this option, then cameras that only support basic authentication will not work with Security Center.

☑ Automatically check for security and enhancement updates for Genetec™ products

☑ Enable Genetec™ Update Service (GUS) integration in Security Center

□ I acknowledge that I have read and understood the implications of selecting these 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.

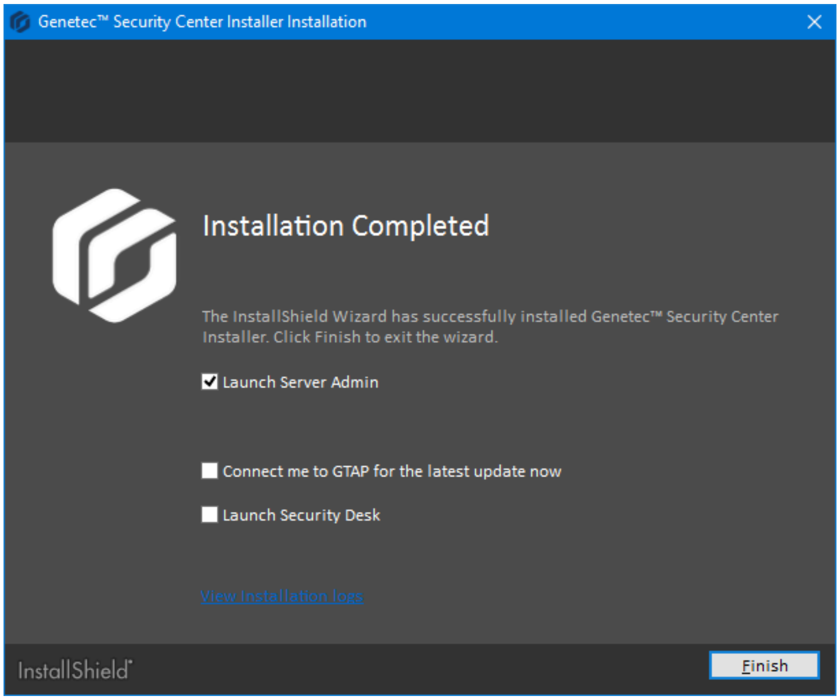
b) Select **I acknowledge that I have read and understood the implications of selecting these security settings**, and click **Install** to start the installation.

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**.



Genetec™ Security Center Installer Installation

Installation Completed

The InstallShield Wizard has successfully installed Genetec™ Security Center Installer. Click Finish to exit the wizard.

☑ Launch Server Admin

□ Connect me to GTAP for the latest update now

□ Launch Security Desk

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**.

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 29

Activating Security Center license without Internet access on page 33

Installing Security Center expansion servers on page 39

Activating Security Center license using the web

The Security Center license is activated on the main server. You must activate your Security Center license after you install Security Center on the main server, and when you promote an expansion server to a main server. If you have Internet access, you can activate your Security Center license using a web connection through Server Admin.

Before you begin

To activate your license using the web, you need the following:

- **Internet connection:** If your server does not have Internet access, then see Activating Security Center license without Internet access on page 33.
- **System ID and password:** The System ID and password are found in the *Security Center License Information* document. Genetec™ Customer Service sends you this document when you purchase the product.
- **Server password:** The server password is used to log on to Server Admin. The server password is set during the installation.

To activate your Security Center license using the web:

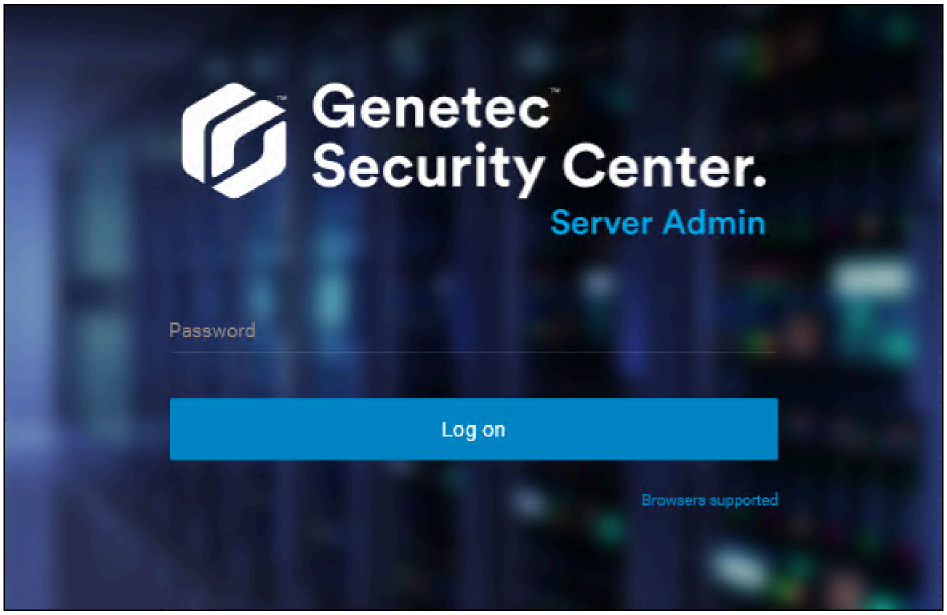
1 Open the Server Admin web page by doing one of the following:

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

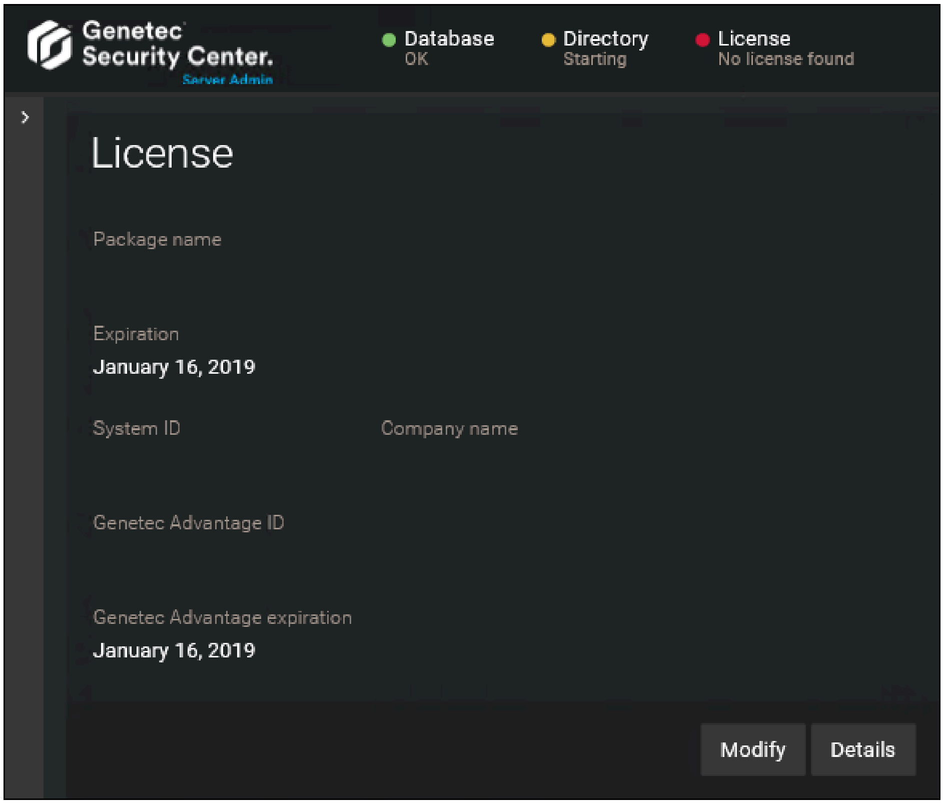
     You can omit the web server port if you are using the default value (80).

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



The Server Admin *Overview* page appears.



Database OK

Directory Starting

License No license found

License

Package name

Expiration
January 16, 2019

System ID

Company name

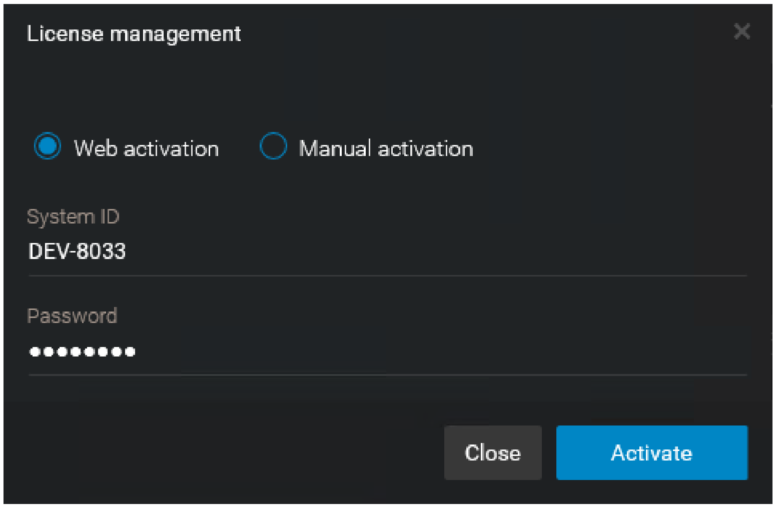
Genetec Advantage ID

Genetec Advantage expiration
January 16, 2019

3 Do one of the following:

- Click **License** at the top of the Server Admin browser window.
- Click **Modify** under the *License* section of the Server Admin *Overview* page.

4 In the *License management* dialog box, click **Web activation**, and enter your **System ID** and **Password** as specified in the *Security Center License Information* document you received when you purchased your license.



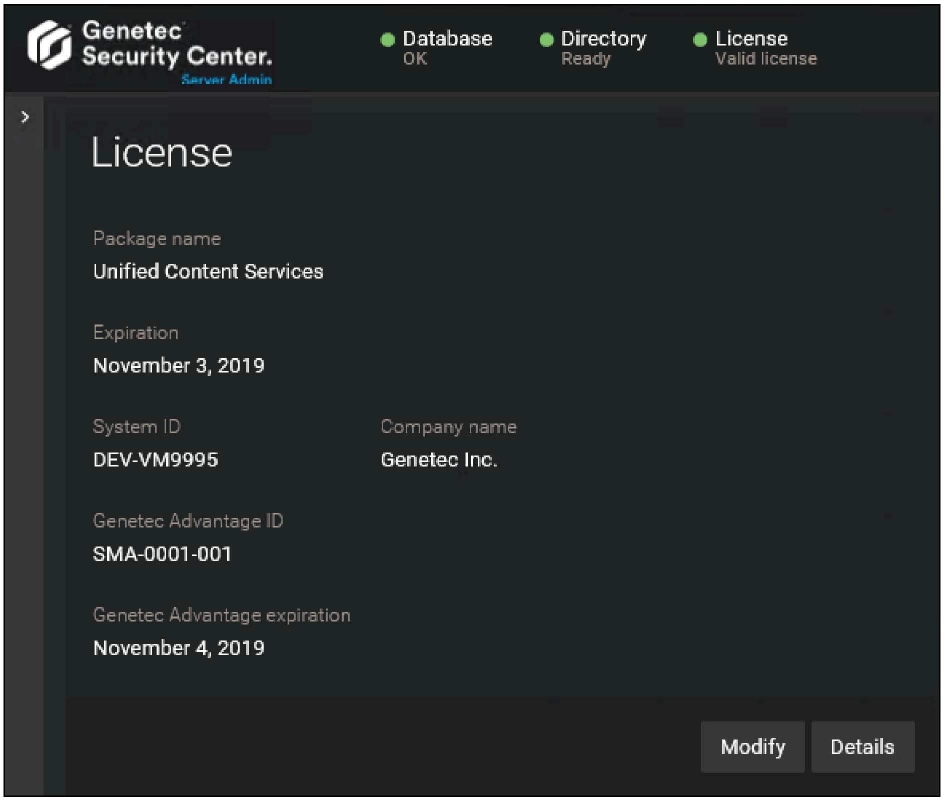
License management

● Web activation ○ Manual activation

System ID
DEV-8033

Password
••••••••

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



License

Package name
Unified Content Services

Expiration
November 3, 2019

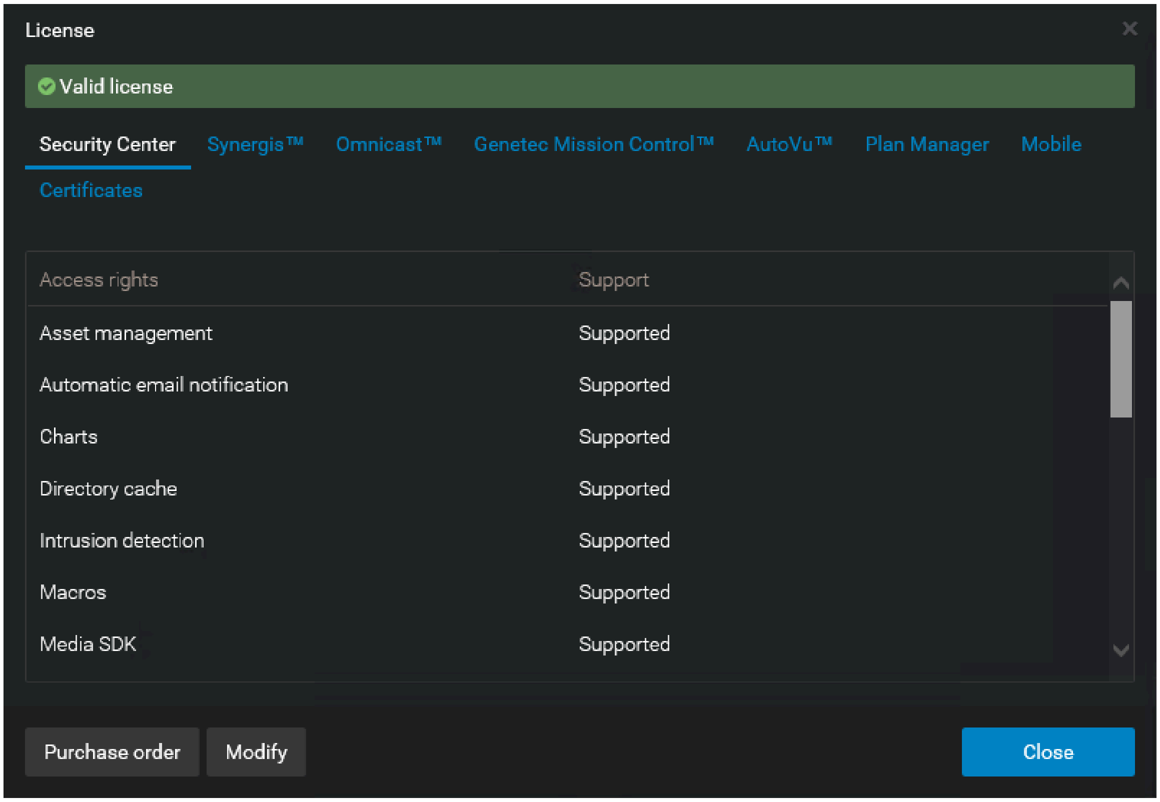
System ID
DEV-VM9995

Company name
Genetec Inc.

Genetec Advantage ID
SMA-0001-001

Genetec Advantage expiration
November 4, 2019

6 Click **Details** to view your license options in a dialog box.



Access rights	Support
Asset management	Supported
Automatic email notification	Supported
Charts	Supported
Directory cache	Supported
Intrusion detection	Supported
Macros	Supported
Media SDK	Supported

Your license options are divided into many tabs. For more information, see the *Security Center Administrator Guide*.

7 Click **Close**, and then close your browser window.

Activating Security Center license without Internet access

The Security Center license is activated on the main server. You must activate your Security Center license after you install Security Center on the main server, and when you promote an expansion server to a main server. If you do not have Internet access, you can activate your Security Center license manually using a combination of Server Admin and GTAP.

Before you begin

To activate your license, you need the following:

- **System ID and password:** The System ID and password are found in the *Security Center License Information* document. Genetec™ Customer Service sends you this document when you purchase the product.
- **Server password:** The server password is used to log on to Server Admin. The server password is set during the installation.

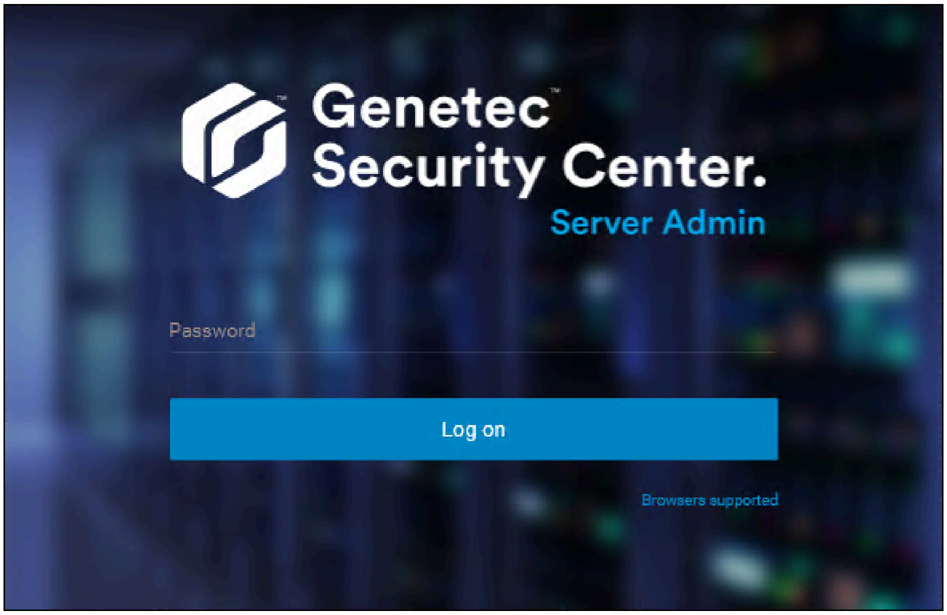
To activate your Security Center license without Internet access:

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

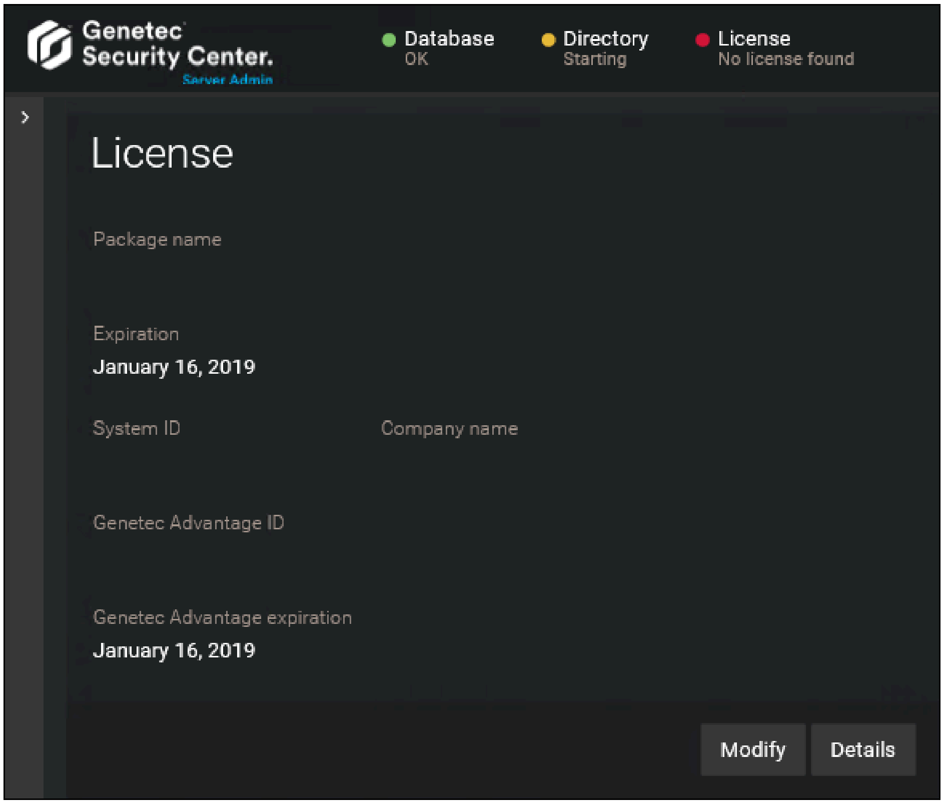
   - In the address bar of your web browser, type `http://computer:port/Genetec`, where `computer` is the hostname or the IP address of your server, and `port` is the web server port specified during the Security Center expansion server installation.

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



The Server Admin *Overview* page appears.



Database
OK

Directory
Starting

License
No license found

License

Package name

Expiration
January 16, 2019

System ID

Company name

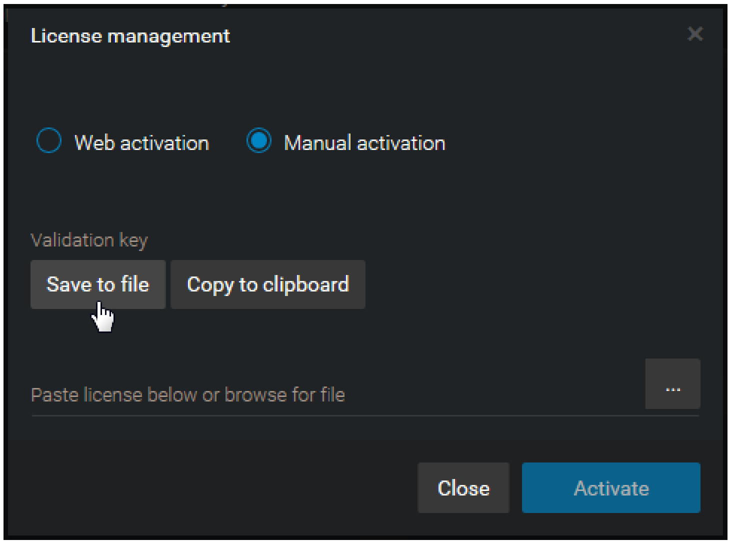
Genetec Advantage ID

Genetec Advantage expiration
January 16, 2019

3 Do one of the following:

- Click **License** at the top of the Server Admin browser window.
- Click **Modify** under the *License* section of the Server Admin *Overview* page.

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



License management

○ Web activation ● Manual activation

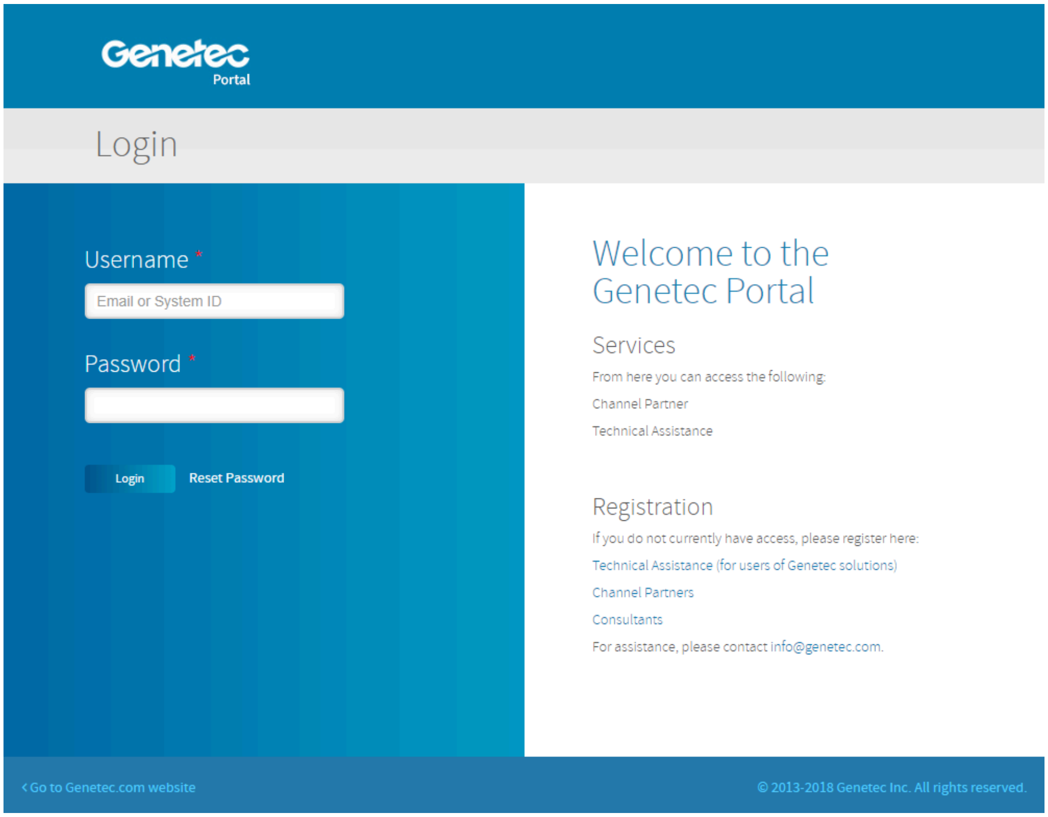
Validation key

Paste license below or browse for file

The validation key is a sequence of numbers (in hexadecimal text format) generated by Security Center that uniquely identifies your server. The validation key is used to generate the license key that unlocks your Security Center software. The license key that is generated 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. Make sure you copy this file to a location (this can be a USB key) that you can access from another computer that has Internet access.

5 From another computer with Internet access, open the Genetec™ Technical Assistance Portal (GTAP) at: https://gtap.genetec.com.



Welcome to the Genetec Portal

Services

From here you can access the following:

Channel Partner

Technical Assistance

Registration

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

Technical Assistance (for users of Genetec solutions)

Channel Partners

Consultants

For assistance, please contact info@genetec.com.

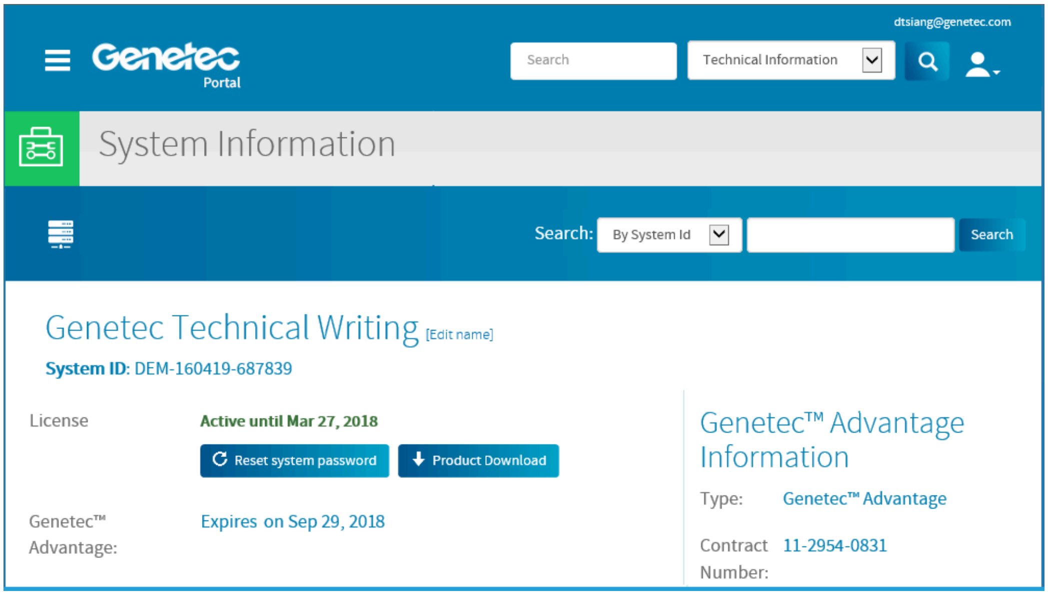
‹ Go to Genetec.com website
© 2013-2018 Genetec Inc. All rights reserved.

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

- Enter the System ID and the Password specified in the *Security Center License Information* document, and click **Login**.
- Enter your GTAP user account (your email address) and Password, and click **Login**

7 On GTAP, click **Activate new system**, select your system from the **System ID** drop-down list, and click **Submit**.

The the *System Information* page opens.



System Information

Genetec Technical Writing [Edit name]

System ID: DEM-160419-687839

License: **Active until Mar 27, 2018**

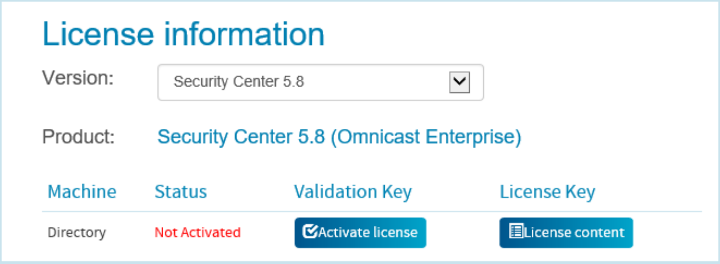
Genetec™ Advantage: Expires on Sep 29, 2018

Genetec™ Advantage Information

Type: Genetec™ Advantage

Contract Number: 11-2954-0831

8 Scroll down to the *License information* section and click **Activate license**.



License information

Version: Security Center 5.8

Product: Security Center 5.8 (Omnicast Enterprise)

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

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

The message *License activation successful* appears.

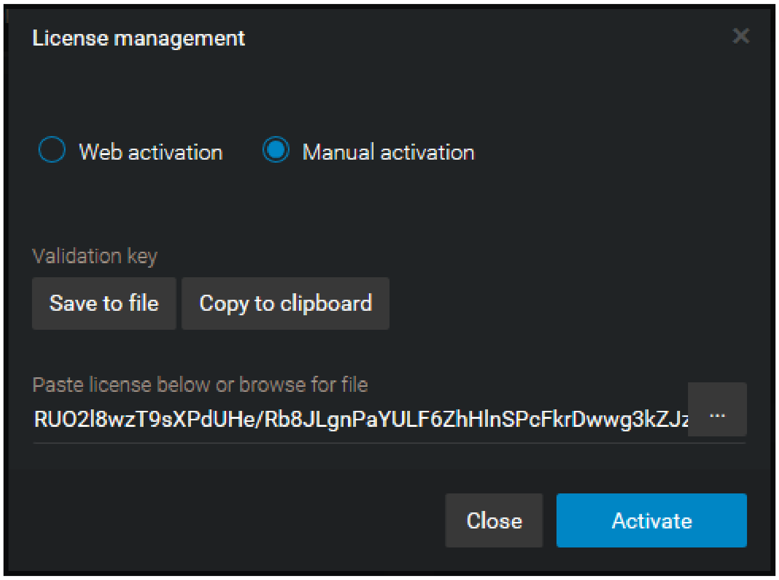
10 Click **Download License**, and save the license key to a file.

The default name is your System ID followed by *_Directory_License.lic*.

11 Return to Server Admin which is connected to your Security Center main server.

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

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



License management

○ Web activation ● Manual activation

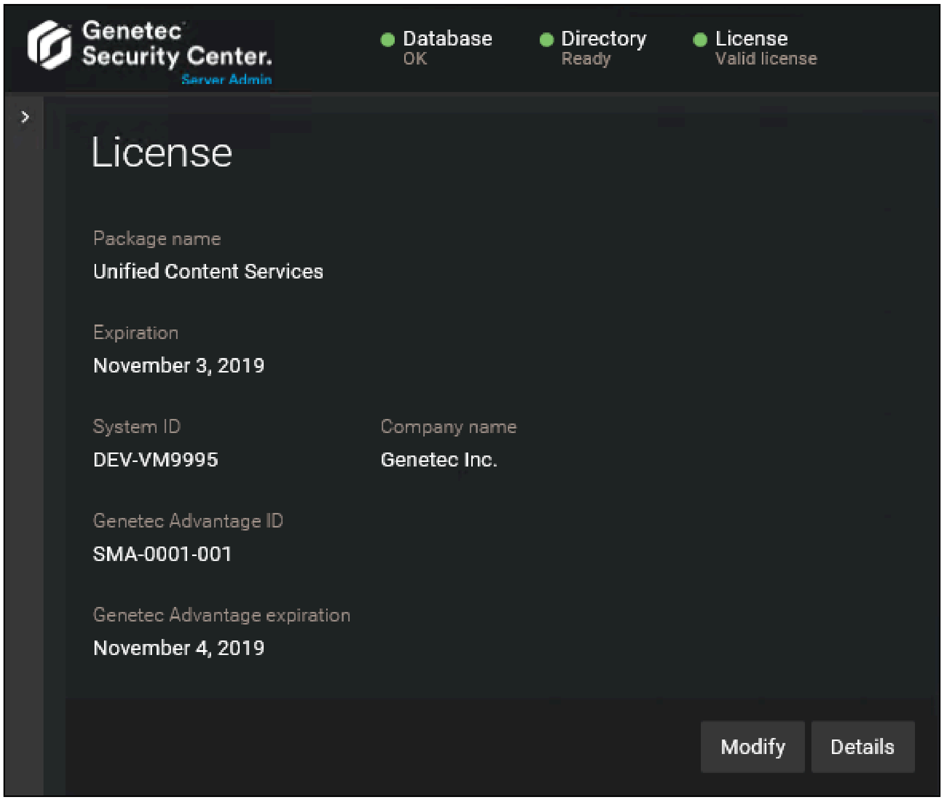
Validation key

Paste license below or browse for file

RUO2l8wzT9sXPdUHe/Rb8JLgnPaYULF6ZhHlnSPcFkrDwwg3kZJz

13 Click **Activate**.

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



● Database OK ● Directory Ready ● License Valid license

License

Package name
Unified Content Services

Expiration
November 3, 2019

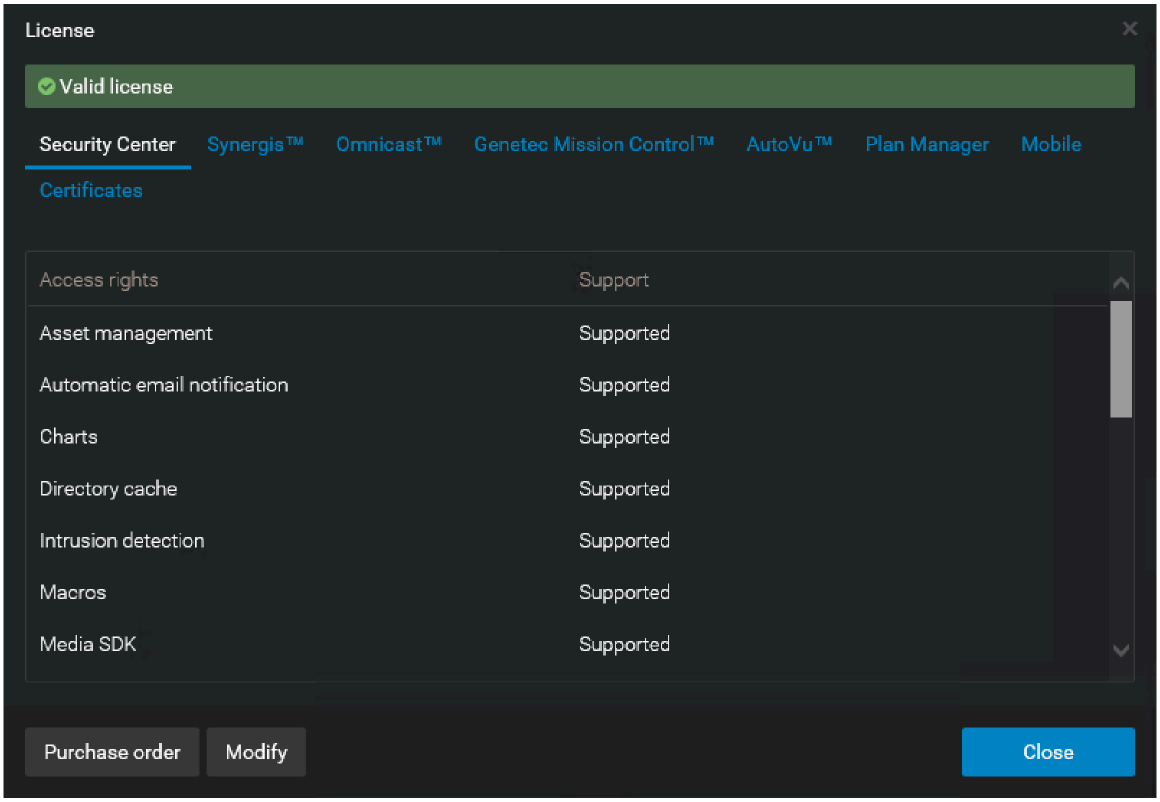
System ID
DEV-VM9995

Company name
Genetec Inc.

Genetec Advantage ID
SMA-0001-001

Genetec Advantage expiration
November 4, 2019

14 Click **Details** to view your license options in a dialog box.



Access rights	Support
Asset management	Supported
Automatic email notification	Supported
Charts	Supported
Directory cache	Supported
Intrusion detection	Supported
Macros	Supported
Media SDK	Supported

Your license options are divided into many tabs. For more information, see the *Security Center Administrator Guide*.

15 Click **Close**, and then close your browser window.

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.

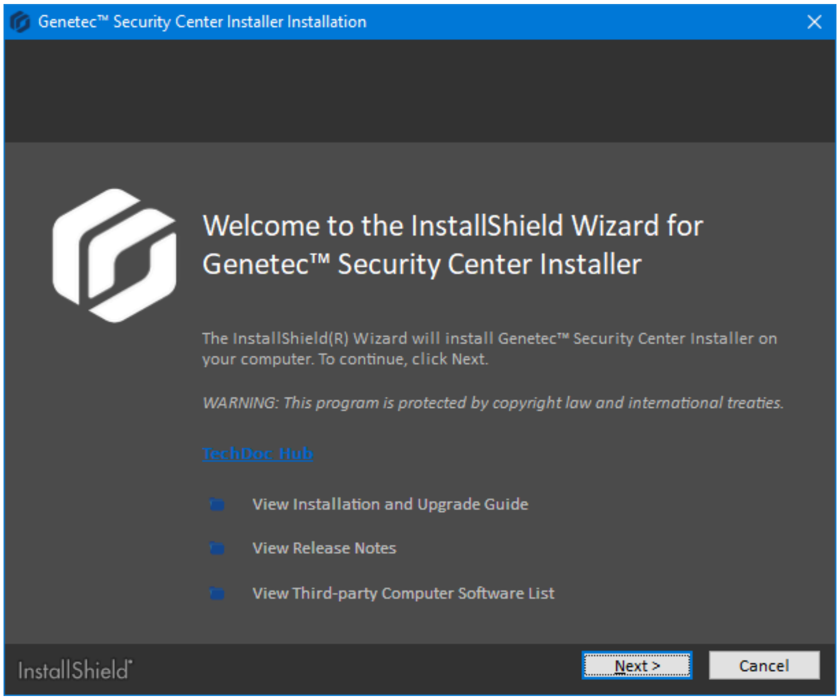
What you should know

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



Genetec™ Security Center Installer Installation

Welcome to the InstallShield Wizard for Genetec™ Security Center Installer

The InstallShield(R) Wizard will install Genetec™ Security Center Installer on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

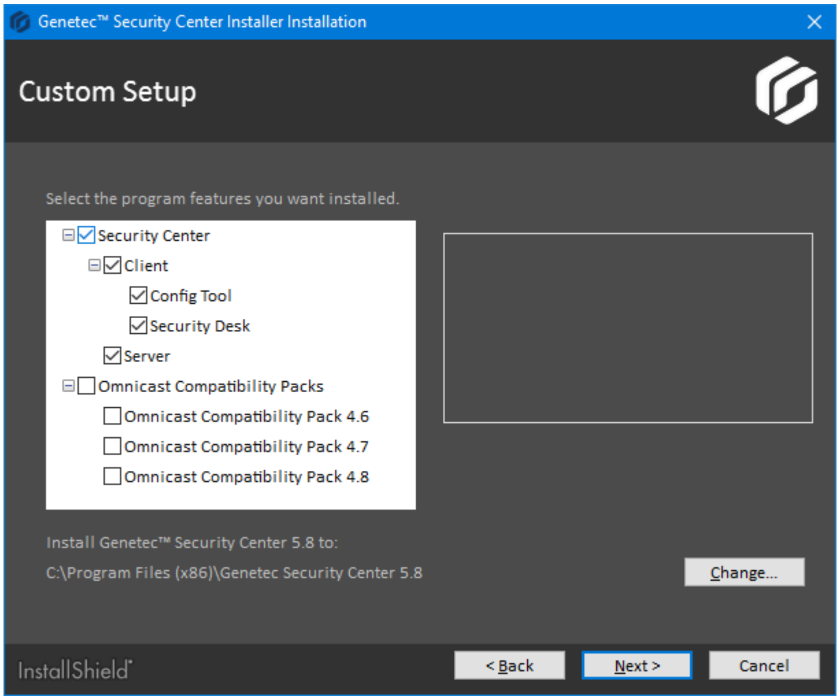
TechDoc Hub
View Installation and Upgrade Guide
View Release Notes
View Third-party Computer Software List
InstallShield
Next >
Cancel

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**.



Genetec™ Security Center Installer Installation

Custom Setup

Select the program features you want installed.

- ☑ Security Center
  - ☑ Client
    - ☑ Config Tool
    - ☑ Security Desk
  - ☑ Server
- □ Omnicast Compatibility Packs
  - □ Omnicast Compatibility Pack 4.6
  - □ Omnicast Compatibility Pack 4.7
  - □ Omnicast Compatibility Pack 4.8

Install Genetec™ Security Center 5.8 to:
C:\Program Files (x86)\Genetec Security Center 5.8

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

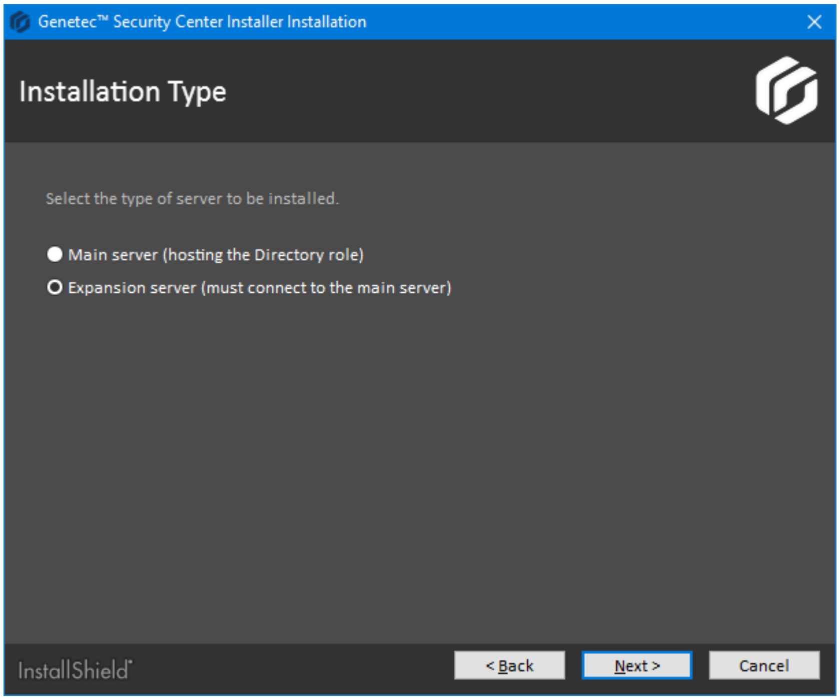
For the destination folder, you can only change the *root folder* where the *Genetec Security Center 5.8* folder is created. On a 64-bit machine, the default root folder is *C:\Program Files (x86)*.

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**.



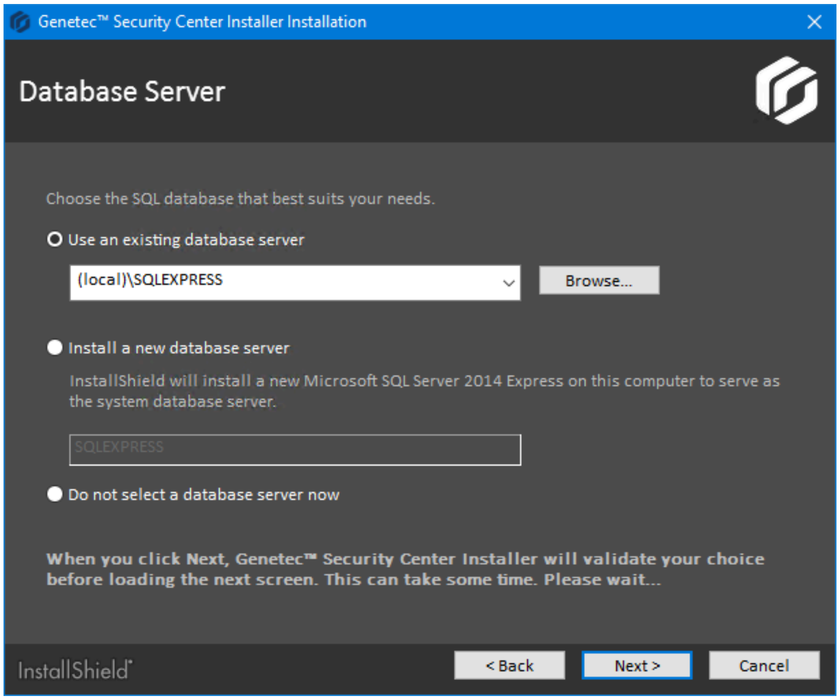
Installation Type

Select the type of server to be installed.

● Main server (hosting the Directory role)

○ Expansion server (must connect to the main server)

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



Database Server

Choose the SQL database that best suits your needs.

○ Use an existing database server

(local)\SQLEXPRESS

● Install a new database server

InstallShield will install a new Microsoft SQL Server 2014 Express on this computer to serve as the system database server.

SQLEXPRESS

● Do not select a database server now

When you click Next, Genetec™ Security Center Installer will validate your choice before loading the next screen. This can take some time. Please wait...

The following options are available:

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

  BEST PRACTICE: Replace `(local)` with the computer name. You must use a computer name if you are configuring the Directory for load balancing. For more information on load balancing, see the *Security Center Administrator Guide*.

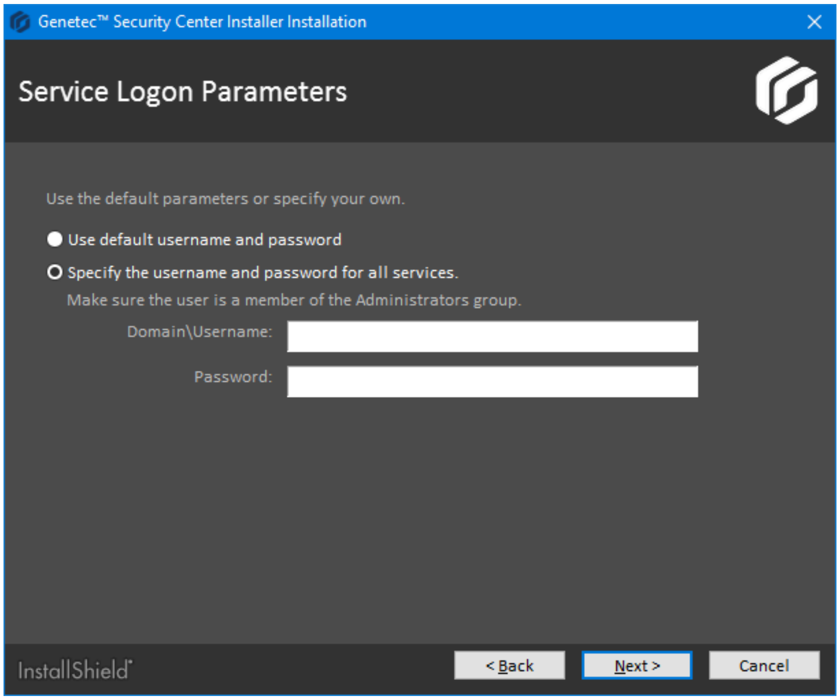
If you are upgrading from a supported version of Security Center, the installer automatically upgrades all databases that your system requires.

- **Install a new database server:** Install Microsoft SQL Server 2014 Express Edition on this machine. 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 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: \ , : ; ' & # @
- **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. An SQL database can be added later.

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



Genetec™ Security Center Installer Installation

Service Logon Parameters

Use the default parameters or specify your own.

● Use default username and password

○ Specify the username and password for all services.

Make sure the user is a member of the Administrators group.

Domain\Username:

Password:

a) Select one of the following options:

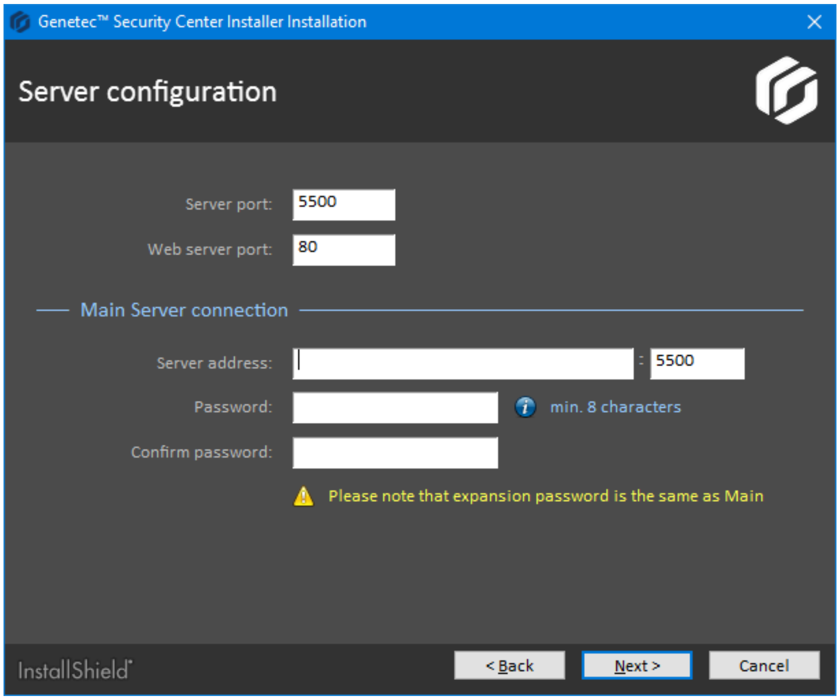
  - **Use default name and password:** Use the default username (LocalSystem).
  - **Specify the username and password for all services:** Enter a valid domain username and a strong password, and record them in a safe place. You must provide these credentials every time you upgrade your Security Center 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: You can change the service logon user later from Microsoft Management Console.

b) Click **Next**.

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



Genetec™ Security Center Installer Installation

Server configuration

Server port: 5500

Web server port: 80

Main Server connection

Server address: : 5500

Password: min. 8 characters

Confirm password:

Please note that expansion password is the same as Main

a) Complete the following fields:

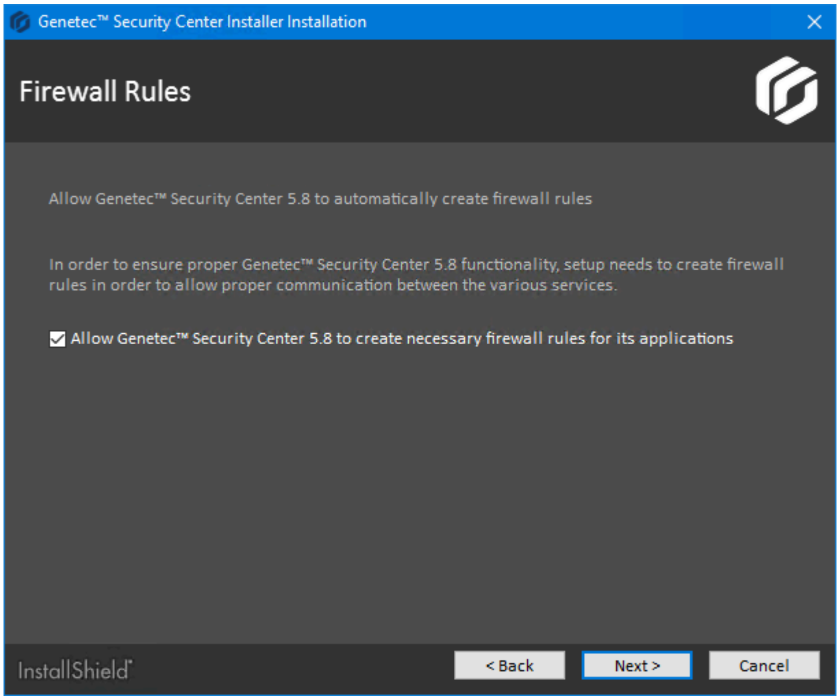
- **Server port:** The TCP port through which the servers in your system communicate.
- **Web server port:** The HTTP port that is used for the web-based Server Admin. If you change the default port, the Server Admin address must include the port number in the URL. For example, *http://computer:port/Genetec*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



Genetec™ Security Center Installer Installation

Firewall Rules

Allow Genetec™ Security Center 5.8 to automatically create firewall rules

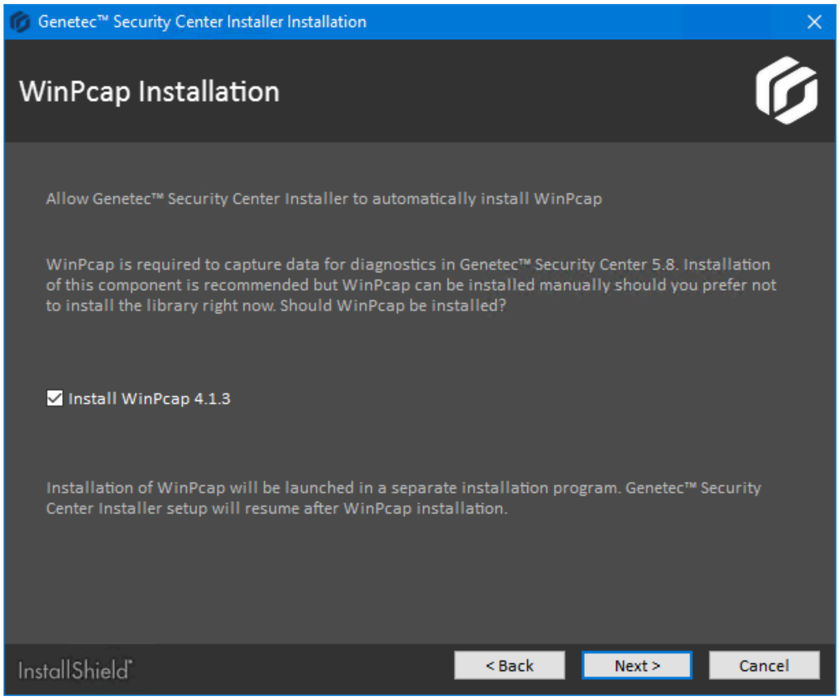
In order to ensure proper Genetec™ Security Center 5.8 functionality, setup needs to create firewall rules in order to allow proper communication between the various services.

☑ Allow Genetec™ Security Center 5.8 to create necessary firewall rules for its applications

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.

- 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.

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



Genetec™ Security Center Installer Installation

WinPcap Installation

Allow Genetec™ Security Center Installer to automatically install WinPcap

WinPcap is required to capture data for diagnostics in Genetec™ Security Center 5.8. Installation of this component is recommended but WinPcap can be installed manually should you prefer not to install the library right now. Should WinPcap be installed?

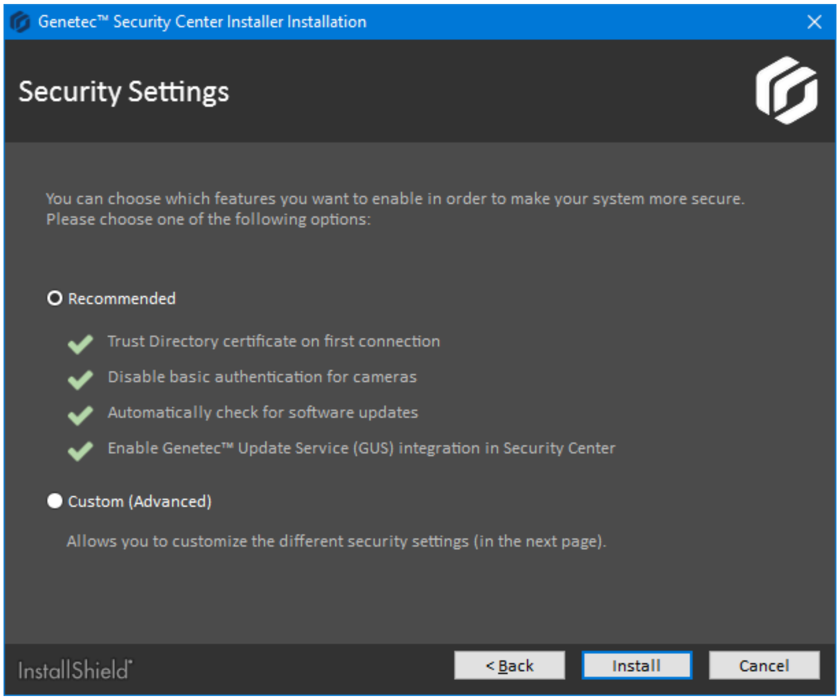
☑ Install WinPcap 4.1.3

Installation of WinPcap will be launched in a separate installation program. Genetec™ Security Center Installer setup will resume after WinPcap installation.

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.

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



Genetec™ Security Center Installer Installation

Security Settings

You can choose which features you want to enable in order to make your system more secure.
Please choose one of the following options:

○ Recommended

✓ Trust Directory certificate on first connection

✓ Disable basic authentication for cameras

✓ Automatically check for software updates

✓ Enable Genetec™ Update Service (GUS) integration in Security Center

● Custom (Advanced)

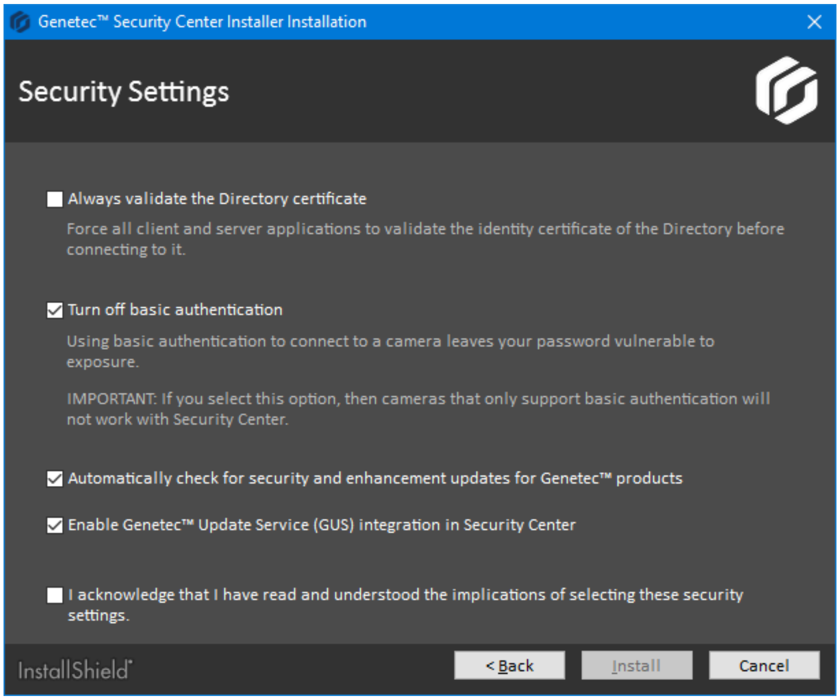
Allows you to customize the different security settings (in the next page).

- 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**.

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



Security Settings

□ Always validate the Directory certificate

Force all client and server applications to validate the identity certificate of the Directory before connecting to it.

☑ Turn off basic authentication

Using basic authentication to connect to a camera leaves your password vulnerable to exposure.

IMPORTANT: If you select this option, then cameras that only support basic authentication will not work with Security Center.

☑ Automatically check for security and enhancement updates for Genetec™ products

☑ Enable Genetec™ Update Service (GUS) integration in Security Center

□ I acknowledge that I have read and understood the implications of selecting these 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.

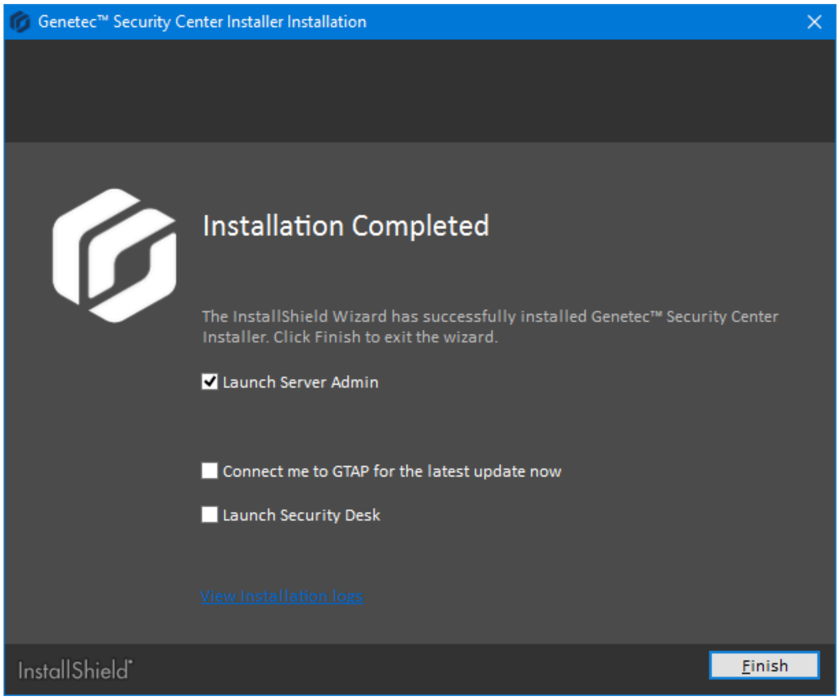
b) Select **I acknowledge that I have read and understood the implications of selecting these security settings**, and click **Install** to start the installation.

15 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**.

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



Genetec™ Security Center Installer Installation

Installation Completed

The InstallShield Wizard has successfully installed Genetec™ Security Center Installer. Click Finish to exit the wizard.

☑ Launch Server Admin

□ Connect me to GTAP for the latest update now

□ Launch Security Desk

View Installation logs

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**.

The Security Center expansion server is now installed.

After you finish

Connect the expansion server to the main server.

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

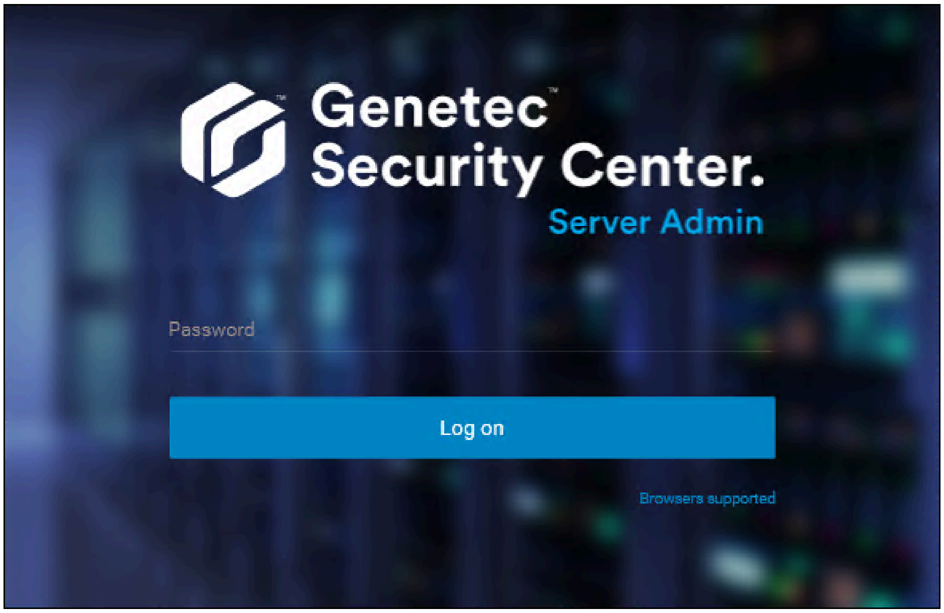
After successfully installing an expansion server, it automatically connects to the main server. These steps are only necessary if:

- 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.

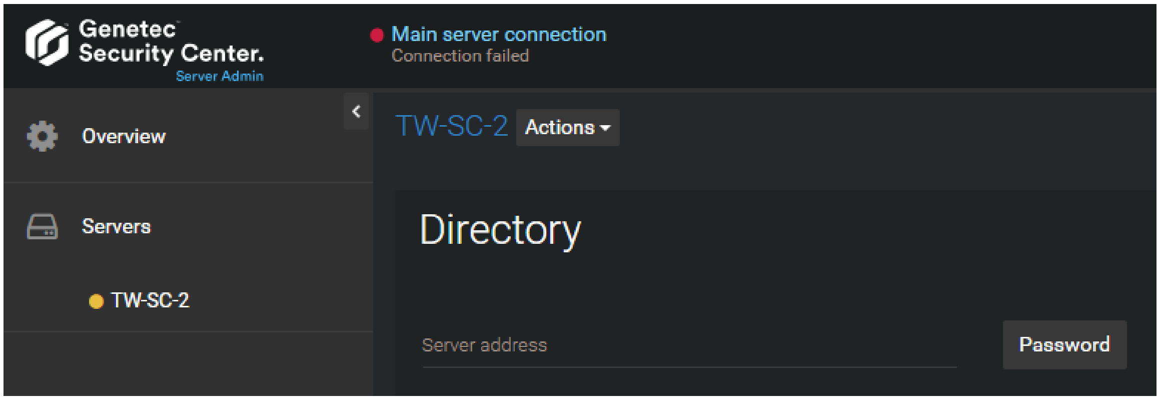
To connect an expansion server to the main server:

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.

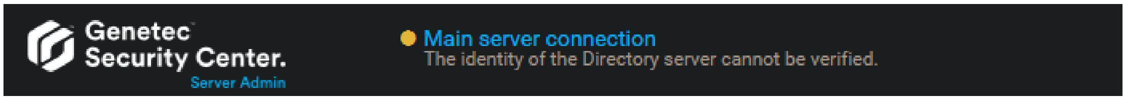
4. Enter the **Server address** (main server hostname or IP address) and **Password**, and then click **Save**.
5. When prompted to restart the service, click **Yes**.

   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.



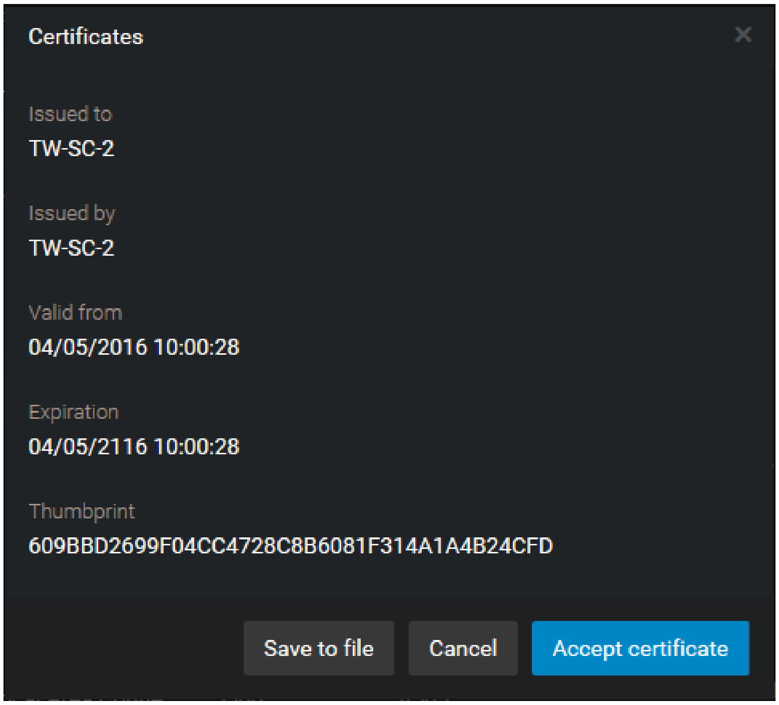
Main server connection

The identity of the Directory server cannot be verified.

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

a) Click **Main server connection**.

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


Certificates

Issued to
TW-SC-2

Issued by
TW-SC-2

Valid from
04/05/2016 10:00:28

Expiration
04/05/2116 10:00:28

Thumbprint
609BBD2699F04CC4728C8B6081F314A1A4B24CFD

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:

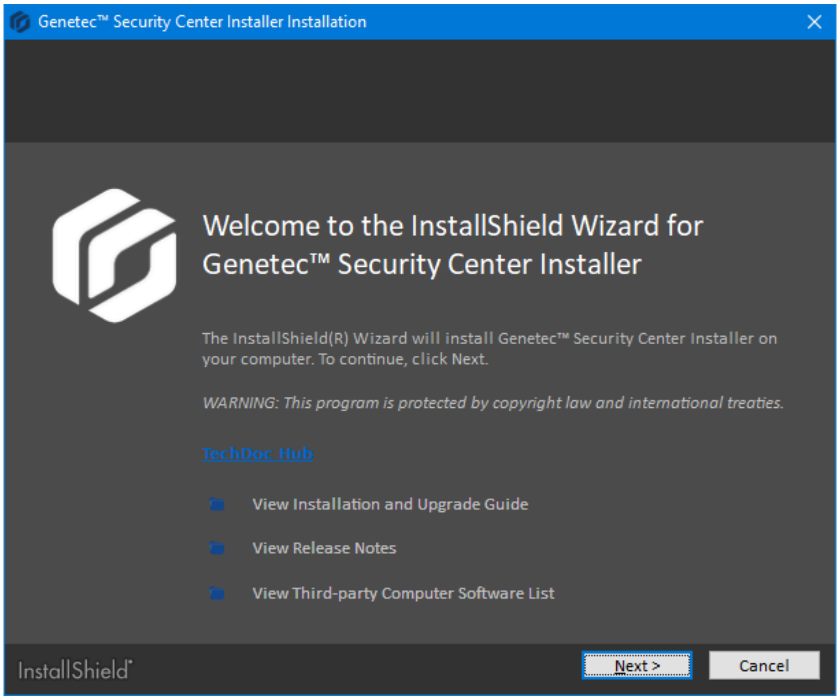
1 Right-click either *setup.exe* (standalone version) or *SecurityCenterWebSetup.exe* (web version), and click **Run as administrator**.

The InstallShield Wizard opens.

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

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

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



Genetec™ Security Center Installer Installation

Welcome to the InstallShield Wizard for Genetec™ Security Center Installer

The InstallShield(R) Wizard will install Genetec™ Security Center Installer on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

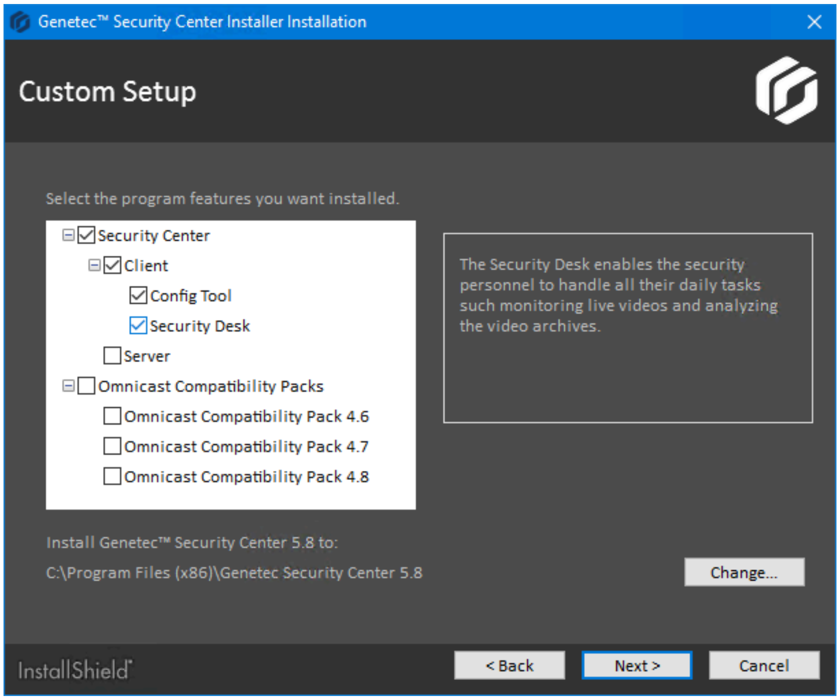
TechDoc Hub
View Installation and Upgrade Guide
View Release Notes
View Third-party Computer Software List
InstallShield
Next >
Cancel

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**.



Genetec™ Security Center Installer Installation

Custom Setup

Select the program features you want installed.

- ☑ Security Center
  - ☑ Client
    - ☑ Config Tool
    - ☑ Security Desk
  - □ Server
- □ Omnicast Compatibility Packs
  - □ Omnicast Compatibility Pack 4.6
  - □ Omnicast Compatibility Pack 4.7
  - □ Omnicast Compatibility Pack 4.8

The Security Desk enables the security personnel to handle all their daily tasks such monitoring live videos and analyzing the video archives.

Install Genetec™ Security Center 5.8 to:
C:\Program Files (x86)\Genetec Security Center 5.8

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

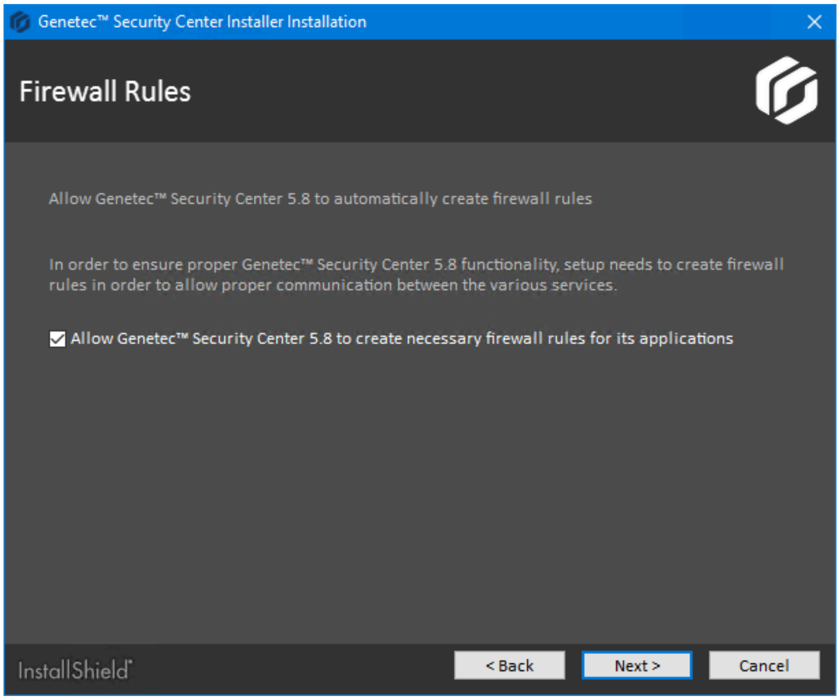
For the destination folder, you can only change the *root folder* where the *Genetec Security Center 5.8* folder is created. On a 64-bit machine, the default root folder is *C:\Program Files (x86)*.

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**.



Allow Genetec™ Security Center 5.8 to automatically create firewall rules

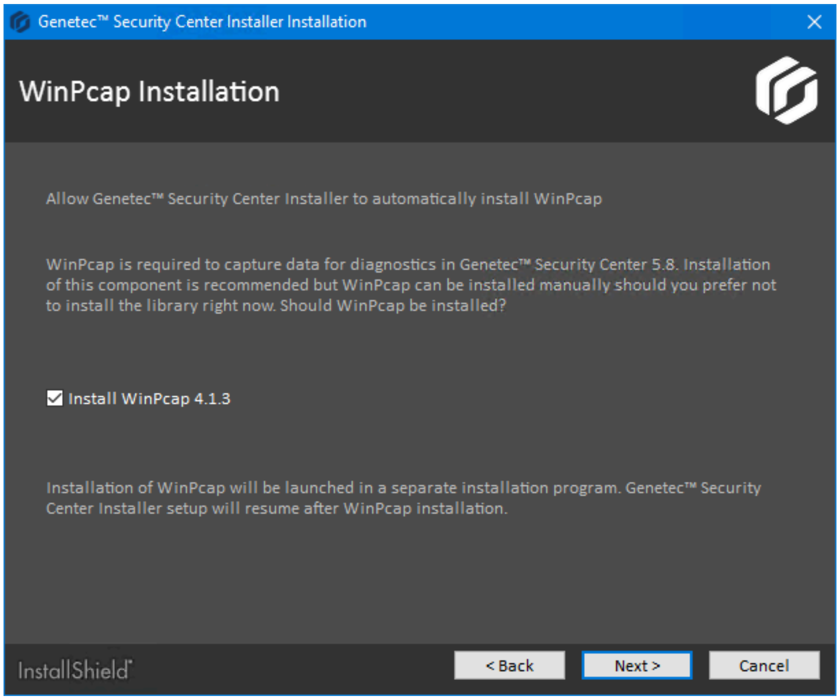
In order to ensure proper Genetec™ Security Center 5.8 functionality, setup needs to create firewall rules in order to allow proper communication between the various services.

☑ Allow Genetec™ Security Center 5.8 to create necessary firewall rules for its applications

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.

- 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.

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



Genetec™ Security Center Installer Installation

WinPcap Installation

Allow Genetec™ Security Center Installer to automatically install WinPcap

WinPcap is required to capture data for diagnostics in Genetec™ Security Center 5.8. Installation of this component is recommended but WinPcap can be installed manually should you prefer not to install the library right now. Should WinPcap be installed?

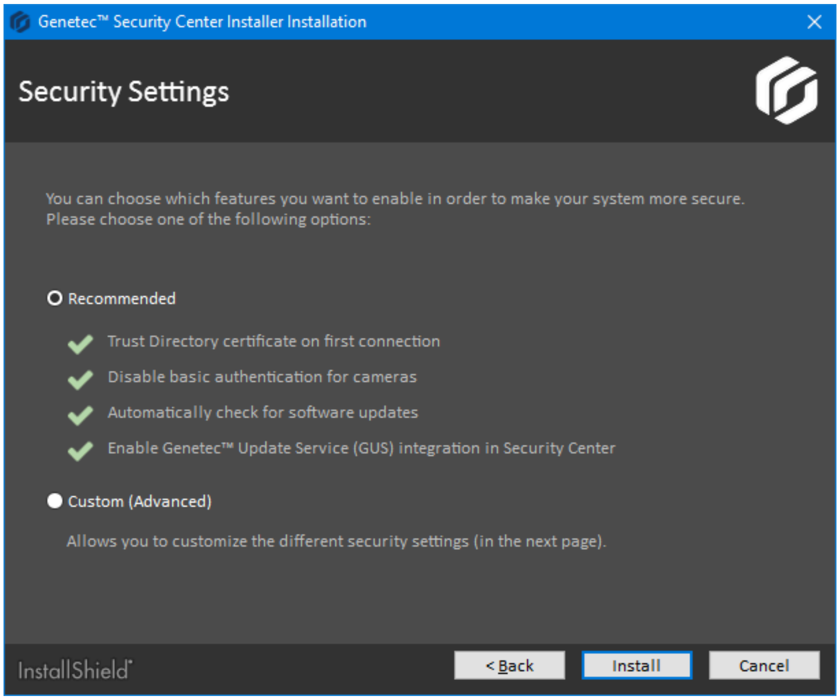
☑ Install WinPcap 4.1.3

Installation of WinPcap will be launched in a separate installation program. Genetec™ Security Center Installer setup will resume after WinPcap installation.

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.

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



Genetec™ Security Center Installer Installation

Security Settings

You can choose which features you want to enable in order to make your system more secure.
Please choose one of the following options:

○ Recommended

- ✓ Trust Directory certificate on first connection
- ✓ Disable basic authentication for cameras
- ✓ Automatically check for software updates
- ✓ Enable Genetec™ Update Service (GUS) integration in Security Center

● Custom (Advanced)

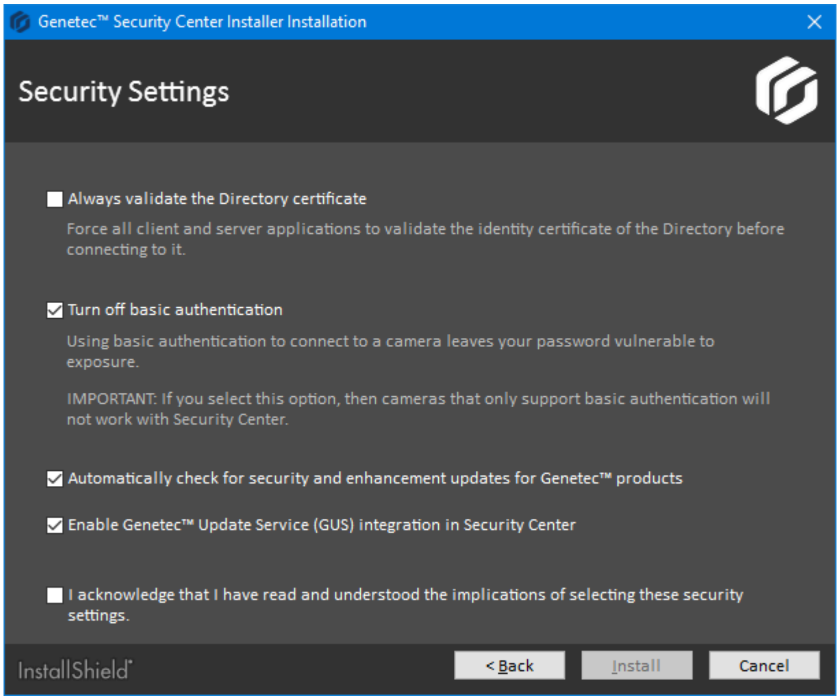
Allows you to customize the different security settings (in the next page).

- 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**.

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



Genetec™ Security Center Installer Installation

Security Settings

☐ Always validate the Directory certificate

Force all client and server applications to validate the identity certificate of the Directory before connecting to it.

☑ Turn off basic authentication

Using basic authentication to connect to a camera leaves your password vulnerable to exposure.

IMPORTANT: If you select this option, then cameras that only support basic authentication will not work with Security Center.

☑ Automatically check for security and enhancement updates for Genetec™ products

☑ Enable Genetec™ Update Service (GUS) integration in Security Center

☐ I acknowledge that I have read and understood the implications of selecting these 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.

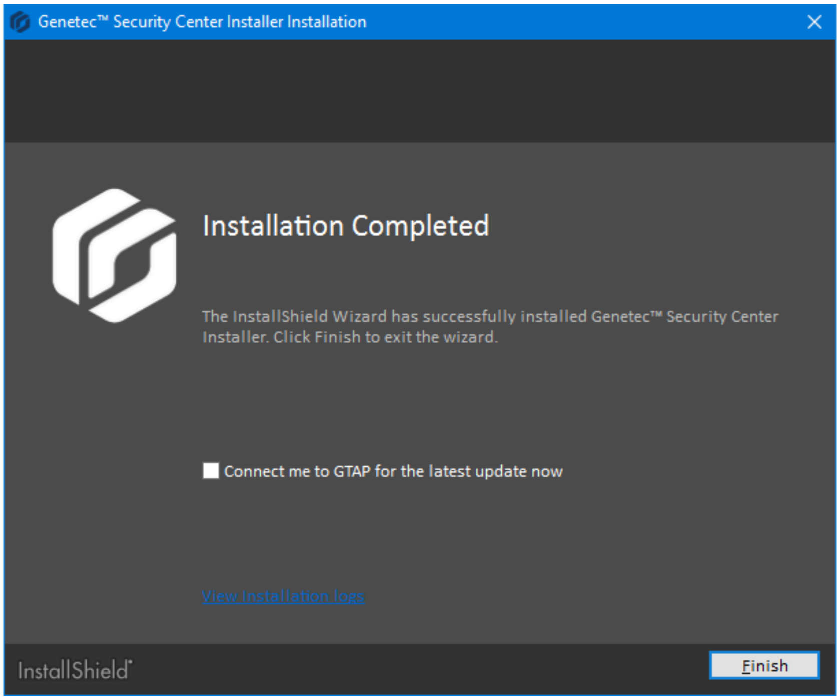
b) Select **I acknowledge that I have read and understood the implications of selecting these security settings**, and click **Install** to start the installation.

11 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**.

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



Genetec™ Security Center Installer Installation

Installation Completed

The InstallShield Wizard has successfully installed Genetec™ Security Center Installer. Click Finish to exit the wizard.

□ Connect me to GTAP for the latest update now

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 5.8 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. From the Windows Control Panel, open the *Programs and Features* applet.
6. In the *Programs and Features* window, right-click **Genetec Security Center Installer**, and then click **Uninstall**.
7. In the *Remove the Program* dialog box, click **Remove**.
8. When the message **Uninstallation Completed** appears, click **Finish**.

   Genetec™Security Center 5.8, the installer program, and all Omnicast™ Compatibility Packs, are removed.
9. (Optional) If you do not want to keep database information, including video archives, uninstall the SQL Server.
10. In the Windows **Start** menu, type `regedit`, and then press **ENTER**.
11. 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*
12. 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 5.8
    - On 64-bit systems: C:\Program Files (x86)\Genetec Security Center 5.8
    - On all systems:
      - C:\ProgramData\Genetec Security Center
      - C:\ProgramData\Genetec Security Center 5.8
      - C:\ProgramData\Genetec Update Service
      - C:\ProgramData\AppData\Local\Genetec Security Center 5.8
      - C:\Users\<username>\AppData\Local\Genetec Inc
      - C:\Users\<username>\AppData\Local\Genetec Security Center 5.8
      - C:\Users\<username>\AppData\Local\IsolatedStorage

        NOTE: You may not be able to delete this folder if other applications are using it.
13. (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 perform to check the status of your system.

Before you begin

Install Security Center.

To complete the installation process:

1. Log on to Server Admin, click **Overview**, and check the following:
   - Directory database is connected (●).
   - Directory is ready (●).
   - License is valid (●) with all features confirmed.
   - All servers are connected (●)
   - SMA number is confirmed with expiration date.
   - Genetec™ Watchdog, connection, and SMTP settings.
2. Under *Servers* (🖴), click the main server (🌐), and check the following:
   - Automatic Directory database backup is enabled and configured.

     Check under **Database properties** (🛢).
   - Data collection policy is properly configured.
   - Network interface card (NIC) is properly selected.
   - Server authentication certificate is configured.
3. Under *Servers* (🖴), click each expansion server, and check the following:
   - NIC is properly selected.
   - Server authentication certificate is configured.
4. Log on to Config Tool, open the **Network view**, 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.
5. Open the **System** task, and then click **Roles**.
6. For every Security Center role, check the following:
   - Role is online with no health issues (not displayed in a yellow warning state).
   - Role database is connected.
   - Automatic backup of the role database is configured (if required).
   - Proper NIC is selected for the role, and in the case of the Media Router, for each redirector.
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 with Security Desk.

9 On the server, check for the following:
   - The storage drive has sufficient free space left.
   - Windows storage indexing is disabled on all drives to be used for video archiving.
   - Order of the NICs displayed in the *Adapters and Bindings* settings is configured properly.
   - Unused NICs are disabled.
   - Server is not a domain controller.
   - Windows Update is not configured to automatically reboot the server after installation of updates.
   - Windows clock is synchronized to a time source.
   - No unwanted application is running.
   - No crash or restart is shown in the Windows Event Viewer.
   - System antivirus is configured properly (if required) and all exclusions are made.

10 Follow the best practices for configuring Windows to work with Security Center.

After you finish

Depending on your deployment requirements, configure your system for:

- Video surveillance and management
- Access control
- License Plate Recognition
- Configure user groups and partitions.

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 5.8

This section includes the following topics:

Supported upgrade paths to Security Center 5.8 GA

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 5.8 GA is supported from the following software versions:

- Security Center 5.7 GA and all SRs
- Security Center 5.6 GA and all SRs
- Security Center 5.5 GA and all SRs

Two-step upgrades

A two-step upgrade to Security Center 5.8 GA is supported from the following software versions:

- Security Center 5.4 GA and all SRs
- Security Center 5.3 GA and all SRs
- Security Center 5.2 GA and all SRs

To maintain backward compatibility during a two-step upgrade, supported systems are first upgraded to Security Center 5.5 SR5 and then directly upgraded to Security Center 5.8 GA.

Older version upgrades

To upgrade Security Center 5.1 and earlier, contact your representative of Genetec Inc..

Preparing to upgrade to Security Center 5.8

If you need to upgrade your Security Center system from an earlier version to 5.8, you must go through a series of preparatory steps.

Before you begin

- Read the *Security Center Release Notes* for important information when upgrading to Security Center 5.8.
- Read Backward compatibility requirements for Security Center on page 64.
- Back up your Directory and role-specific databases.
- 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.

What you should know

- Starting with Security Center 5.6 GA, there is a new license option called *Number of restricted cameras*. 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. If you have restricted cameras on your system after upgrading to Security Center 5.8, these video units will stop working and the Archiver will be in a warning state until you license the restricted camera connections.

  To view a list of manufacturers that require a restricted license, use the **Restricted** *License Type* filter on the Supported Device List.
- 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 not on the same domain as 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.

To prepare to upgrade to 5.8:

1. Close all applications related to Microsoft Management Console (MMC), such as Services, Event Viewer, and so on, because they might lock the Security Center services and prevent them from being updated.
2. If you plan to start using restricted cameras, or increase the number of restricted cameras in use, do the following:
   a) Contact your sales representative to obtain a special connection license for your restricted camera connections.
   b) Sign the “Exclusion of Liability and Hold Harmless” waiver.
3. If you are running Windows 7 SR1 or Windows Server 2008 R2 SP1, you must install Microsoft hotfix 2588507.

   NOTE: This hotfix is not required for SV appliances.
4. If you are running Windows 8.1 or Windows Server 2012 R2, you must install Microsoft update 2919355 followed by 2999226.
5. If you are running Microsoft SQL Server 2005, install a more recent version of the database server.

   Security Center 5.8 is not compatible with Microsoft SQL Server 2005. (see the system requirements for a list of compatible versions). For more information on how to upgrade your SQL Server, refer to your Microsoft documentation.

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.

Starting from Security Center 5.2 SR6, a new standard Windows Active Directory attribute (*accountExpires*) is used by the Active Directory role to import users and cardholders to Security Center. The new attribute sets an expiration date for imported cardholders in Security Center, and changes the status of imported users to inactive after the specified date.

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.

Backward compatibility requirements for Security Center

Security Center 5.8 GA is backward compatible with many Security Center components from the three previous versions.

IMPORTANT: Security Center 5.8 is backward compatible with the three previous versions. A server or workstation that is three versions behind can connect to the 5.8 Directory, but one that is four versions behind cannot. To retain backward compatibility when upgrading your system in stages, no part of Security Center can be more than three versions apart. For systems that are three to six versions behind, use a two-step upgrade process that maintains backward compatibility.

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 5.8 GA, 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 software version and service release. For example, if you upgrade to Security Center 5.8 GA, you must upgrade all Directory servers to 5.8 GA.
- **SQL Server:** Because Security Center 5.8 is not compatible with Microsoft SQL Server 2005, you must install a more recent version of the database server (see the system requirements for a list of compatible versions). For more information on how to upgrade your SQL Server, refer to your Microsoft documentation.

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

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 role that is not backward compatible must be upgraded to the same version as the main server hosting the Directory.

Not all roles and tasks can run in backward compatibility mode. The following tables show which 5.8 roles and tasks are backward compatible.

5.8 role	Backward compatible with 5.5, 5.6 and 5.7
Access Manager	Yes

5.8 role	Backward compatible with 5.5, 5.6 and 5.7
Active Directory	Yes (starting from 5.6)
Active Directory Federation Services	No
Archiver	Yes
Auxilliary Archiver	Yes
Camera Integrity Monitor (hidden)	No (introduced in 5.8)
Directory Manager	No
Global Cardholder Synchronizer (GCS)	No
Health Monitor	No
Intrusion Manager	Yes
LPR Manager	Yes
Map Manager	Yes
Media Gateway	No (renamed from *RTSP Media Router* in 5.5 SR1)
Media Router	No
Mobile Server	No (introduced in 5.8)
Omnicast™ Federation™	Yes
Plugin (all instances)	No
Point of Sale	No
Privacy Protector™ (hidden)	Yes (introduced in 5.7 SR1)
Report Manager	No
Reverse Tunnel	No (introduced in 5.7 SR2)
Reverse Tunnel Server	No (introduced in 5.7 SR2)
Security Center Federation™	Yes
Wearable Camera Manager	No (introduced in 5.7 SR2)
Web Server	Yes (introduced in 5.6)
Web-based SDK	Yes
Zone Manager	Yes

Backward compatibility with Security Center tasks

The Security Center 5.8 tasks that are backward compatible with Security Desk 5.5, 5.6 and 5.7 are summarized in the following table.

Task category	Task type	Backward compatible with Security Desk 5.5, 5.6 and 5.7
Operation	Monitoring (live and playback video)	Yes
	Maps	Yes
	Dashboards	No (introduced in 5.8)
	Remote	No
	Cardholder management	Yes
	Credential management	Yes
	Visitor management	Yes
	People counting	Yes
	Hotlist and permit editor	Yes
	Inventory management	Yes
Alarm management	Alarm monitoring	Yes
	Alarm report	Yes
Investigation	Incidents	Yes
	Transactions	No
	Zone activities	Yes
Investigation > Access control	Area activities	Yes
	Door activities	Yes
	Cardholder activities	Yes
	Visitor activities	Yes
	Area presence	Yes
	Time and attendance	Yes
	Credential activities	Yes
	Credential request history	Yes
	Elevator activities	Yes
	Visit details	Yes

Task category	Task type	Backward compatible with Security Desk 5.5, 5.6 and 5.7
Investigation > Asset management	Asset activities	No
	Asset inventory	No
Investigation > Intrusion detection	Intrusion detection area activities	Yes
	Security video analytics	Yes (introduced in 5.7 SR2, renamed from *KiwiVision intrusion detector* in 5.7 SR5)
Investigation > LPR	Hits	Yes
	Hits (Mutli-region)	Yes
	Reads	Yes
	Reads (Mutli-region)	Yes
	Patroller tracking	Yes
	Inventory report	Yes
	Daily usage per Patroller	Yes
	Logons per Patroller	Yes
	Reads/hits per day	Yes
	Reads/hits per zone	Yes
	Zone occupancy	Yes
	Parking sessions	Yes (introduced in 5.6)
	Parking zone activities	Yes (introduced in 5.6)
Investigation > Video	Archives	Yes
	Bookmarks	Yes
	Motion search	Yes
	Camera events	Yes
	Video file explorer	Yes
	Forensic search	Yes
Maintenance	System status	Yes
	Audit trails	Yes
	Activity trails	Yes
	Health history	Yes

Task category	Task type	Backward compatible with Security Desk 5.5, 5.6 and 5.7
	Health statistics	Yes
	Hardware inventory	Yes
Maintenance > Access control	Access control health history	Yes
	Access control unit events	Yes
	Cardholder access rights	Yes
	Door troubleshooter	Yes
	Access rule configuration	Yes
	Cardholder configuration	Yes
	Credential configuration	Yes
	I/O configuration	Yes
Maintenance > Intrusion detection	Intrusion detection unit events	Yes
Maintenance > Video	Camera configuration	Yes
	Archiver events	Yes
	Archiver statistics	No (introduced in 5.8)
	Archive storage details	Yes
	Wearable camera evidence	No (introduced in 5.8)

Backing up databases

You can protect the data in a role's database by regularly backing up the database. 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.

All role databases are backed up from Config Tool, except for the Directory database, which must be backed up from the Server Admin main server page. The procedures are similar in both cases. Therefore, only backing up from Config Tool is described here.

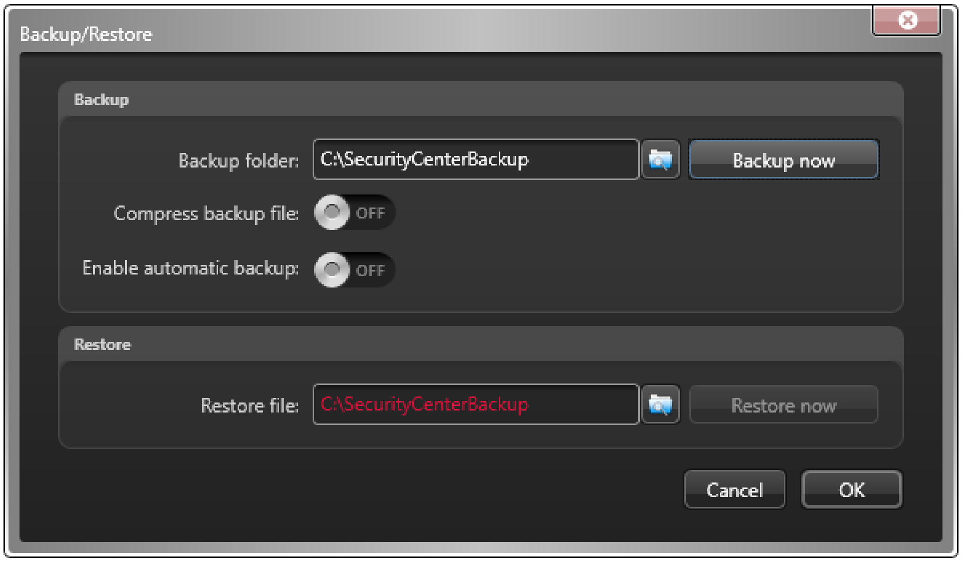
NOTE: The following cases are exceptions:

- To back up the Archiver and Auxiliary Archiver role databases with their associated video files, the backup must be performed from the *Archive transfer* page in the *Video* task.
- To back up the Directory database while the *Backup and restore* failover mode is enabled, the backup must be performed from the Directory Manager role's **Database failover** tab in Config Tool.

- 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 a role's 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.



Backup/Restore

Backup

Backup folder: C:\SecurityCenterBackup

Compress backup file: OFF

Enable automatic backup: OFF

Restore

Restore file: C:\SecurityCenterBackup

NOTE: The path is relative to the server hosting the role, not to the workstation where you are running Config Tool. To select a network drive, enter the path manually, and make sure the service user has write access to this folder.

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

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

   IMPORTANT: The **Compress backup file** option only works if the database is local on the same server.

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 (mm-dd-yyyy).

Upgrading Security Center from 5.5, 5.6, or 5.7 to 5.8

To have the latest version of Security Center, you can upgrade directly from the previous three versions to 5.8.

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 64.

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 LPR Manager, the Archiver it is linked to must also be upgraded. The upgraded LPR Manager would not work if the Archiver is working in backward compatibility mode.

To upgrade from Security Center 5.5, 5.6, or 5.7 to 5.8:

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.
   - 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.
- If AutoVu™ is enabled, migrate the LPR databases to the Security Center 5.8 GA structure.

Related Topics

One or more services failed to install on page 116

Upgrading Security Center from 5.2, 5.3, or 5.4 to 5.8

To maintain backward compatibility while upgrading Security Center 5.2, 5.3, or 5.4 to 5.8, 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 5.8 is backward compatible with the three previous versions. A server or workstation that is three versions behind can connect to the 5.8 Directory, but one that is four versions behind cannot. To retain backward compatibility when upgrading your system in stages, no part of Security Center can be more than three versions apart. For systems that are three to six versions behind, use a two-step upgrade process that maintains backward compatibility.

To upgrade from Security Center 5.2, 5.3, or 5.4 to 5.8:

1. Upgrade your system to the latest Security Center 5.5 release.

   You need a temporary license and the latest Security Center installation package. Ask your representative of Genetec Inc.

   a) Upgrade your main server to Security Center 5.5.

      Follow the upgrade instructions found in the *Security Center Installation and Upgrade Guide 5.5 SR5*.

   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 5.5 release.

      Your entire system runs in version 5.5. This is the second stage. You can split this step into as many stages as necessary, depending on the number of machines you need to upgrade.

2. Upgrade your system to Security Center 5.8.

Related Topics

One or more services failed to install on page 116

Upgrading Failover Directory systems from a previous version or release

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 5.8.
- 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 not able to use Security Desk manually to open doors, etc.
- During the upgrade, each Directory server is upgraded separately. Consequently, the failover feature is not available.
- License upgrades are only necessary for version upgrades (for example, from version 5.x to 5.8). It is not necessary to upgrade the license for service release upgrades (for example, from SRx to SRy).

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 version upgrades) Activate your Security Center 5.8 license by doing one of the following:
   - with the web
   - without Internet access

   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 version upgrades) Reactivate the Security Center 5.8 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: Because adding backward compatible connections slows down the performance of the Directory, it is recommended only as a temporary solution before you are able to upgrade all servers and workstations.

Related Topics

Backward compatibility requirements for Security Center on page 64
One or more services failed to install on page 116

Reactivating the Security Center license for systems with Directory failover

You must reactivate your Security Center license with a new validation key, every time you add or remove servers from the list of Directory servers.

Before you begin

To update your license, you need the following:

- **System ID and password:** The System ID and password are found in the *Security Center License Information* document. Genetec™ Customer Service sends you this document when you purchase the product.

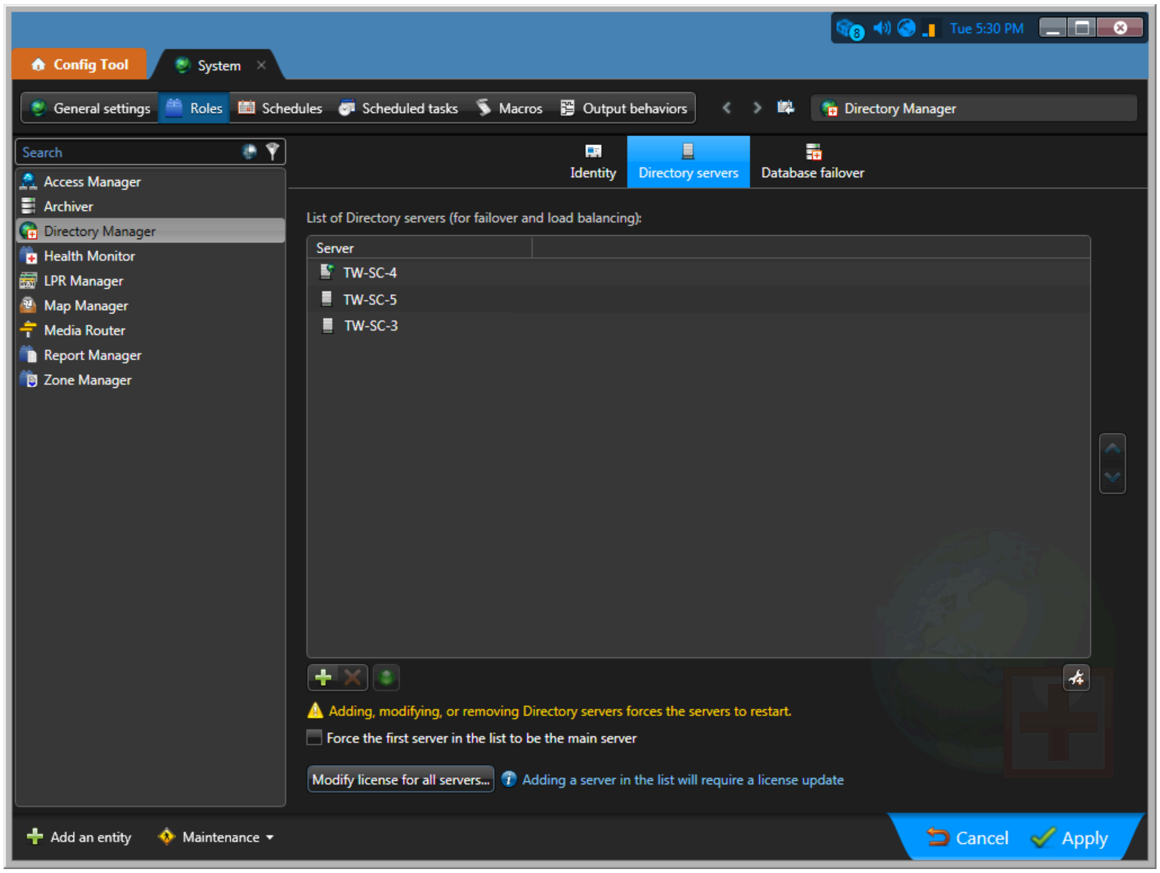
What you should know

IMPORTANT: Server Admin can only be used to activate a single-server license. If you have a multi-Directory server configuration, both the generation of the validation key and the application of the license key must be performed from Config Tool. All Directory servers must be running to update the license from Config Tool.

To activate 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.



List of Directory servers (for failover and load balancing):

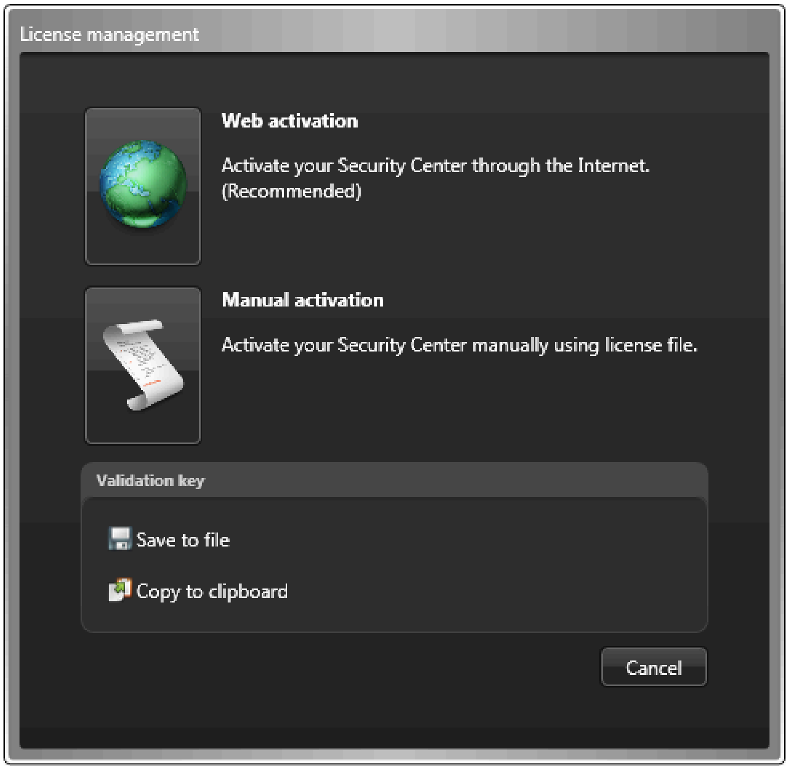
Server
TW-SC-4
TW-SC-5
TW-SC-3

⚠ Adding, modifying, or removing Directory servers forces the servers to restart.

□ Force the first server in the list to be the main server

Modify license for all servers... Adding a server in the list will require a license update

3 Click **Modify license for all servers**.
The **License management** dialog box opens.



License management

Web activation

Activate your Security Center through the Internet. (Recommended)

Manual activation

Activate your Security Center manually using license file.

Validation key

Save to file

Copy to clipboard

Cancel

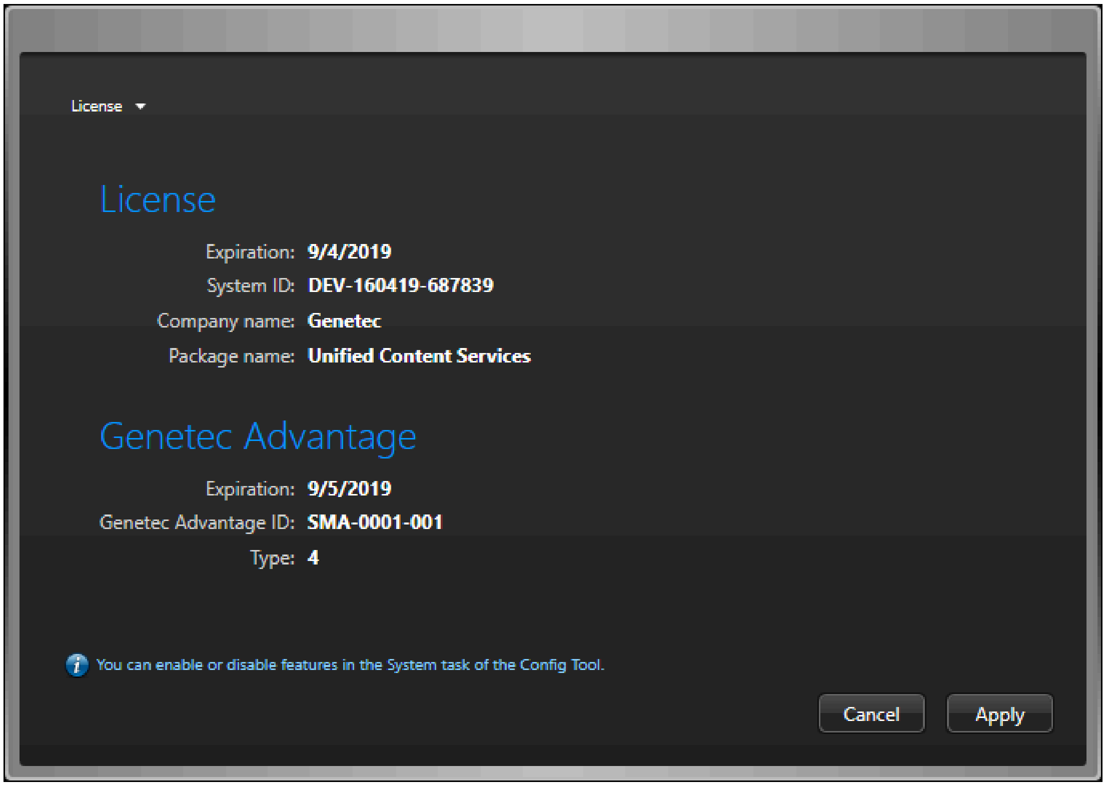
4 In the **License management** dialog box, activate your license in one of the following ways:

- **Web activation:** (Recommended) Reactivate your license from the Internet.

  In the dialog box that appears, enter your *System ID* and *Password*, and click **Activate**.
- **Manual activation:** If your Config Tool workstation has no Internet access, reactivate your Security Center license manually using a license file.

IMPORTANT: Send the composite validation key (comprising all Directory servers); otherwise, the license reactivation fails silently and the Directory failover does not work.

A dialog box showing your license information opens.



License

Expiration: 9/4/2019
System ID: DEV-160419-687839
Company name: Genetec
Package name: Unified Content Services

Genetec Advantage

Expiration: 9/5/2019
Genetec Advantage ID: SMA-0001-001
Type: 4

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

From the **License** drop-down list, you can select an option to view what is included in your license.

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

Reactivating your Security Center license using a license file

To reactivate your Security Center license for the changes you made to the list of Directory servers while the Config Tool workstation has no Internet access, you must use a second workstation to download your license file from GTAP, and then apply the license file using your first workstation.

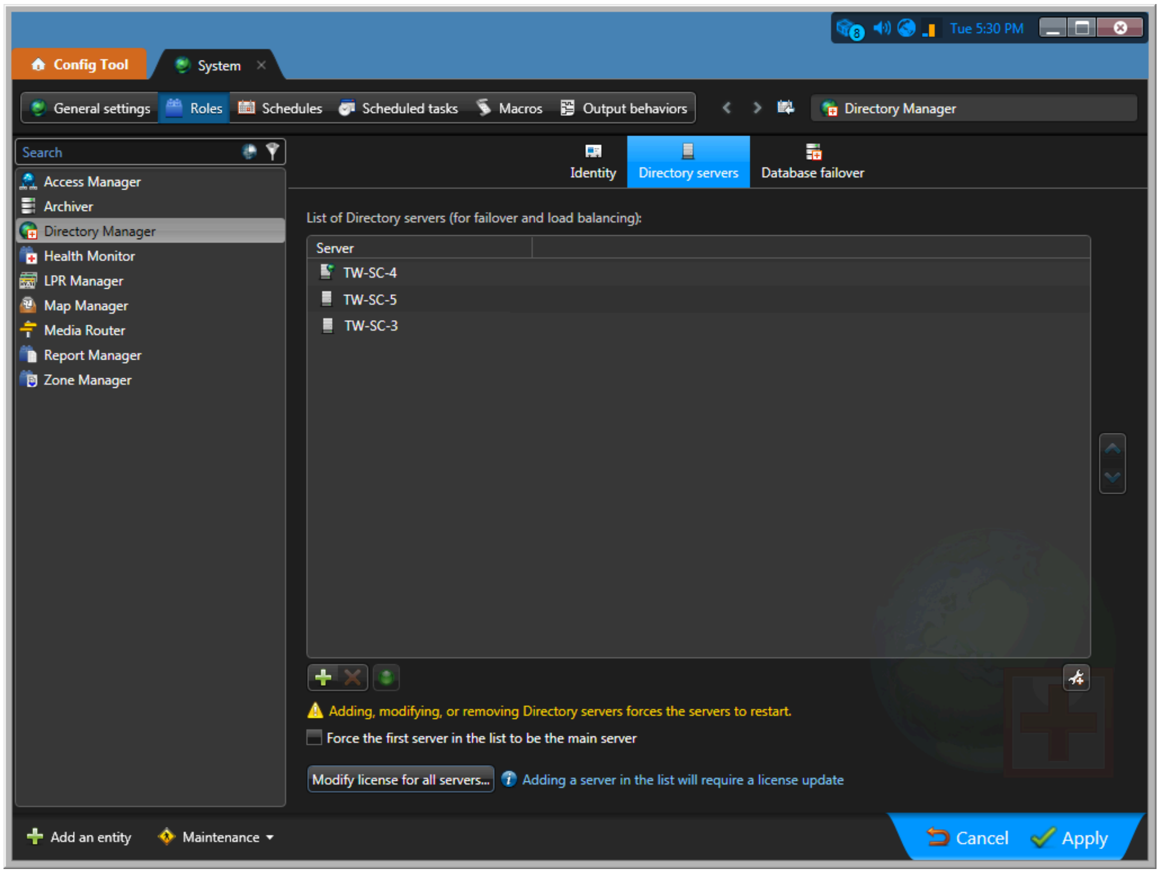
What you should know

IMPORTANT: Server Admin can only be used to activate a single-server license. If you have a multi-Directory server configuration, both the generation of the validation key and the application of the license key must be performed from Config Tool. All Directory servers must be running to update the license from Config Tool.

To update your license using a license file:

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.



List of Directory servers (for failover and load balancing):

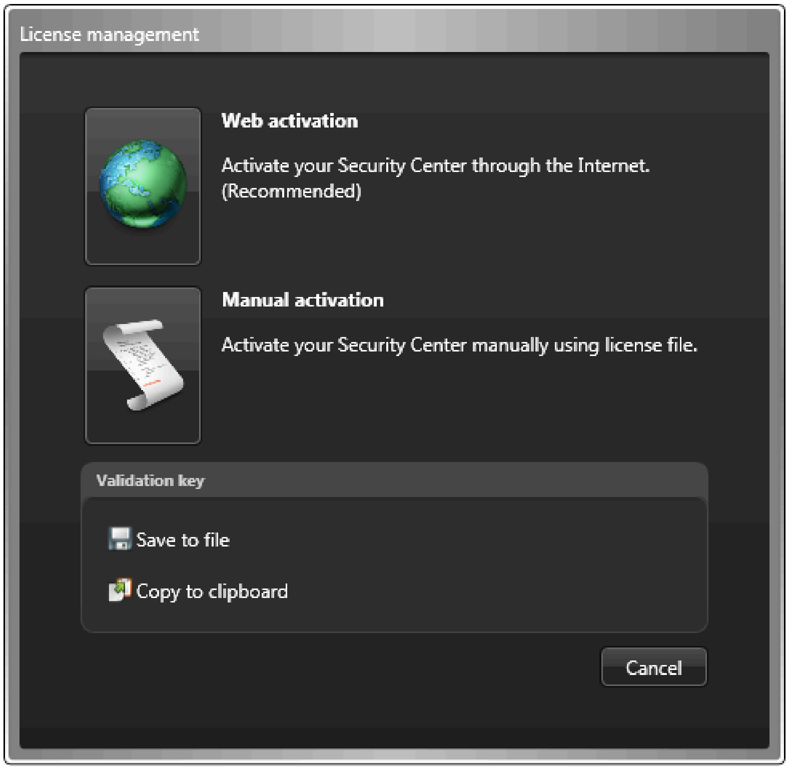
Server
TW-SC-4
TW-SC-5
TW-SC-3

⚠ Adding, modifying, or removing Directory servers forces the servers to restart.

□ Force the first server in the list to be the main server

Modify license for all servers... ⓘ Adding a server in the list will require a license update

3 Click **Modify license for all servers**.
The **License management** dialog box opens.


License management

Web activation

Activate your Security Center through the Internet. (Recommended)

Manual activation

Activate your Security Center manually using license file.

Validation key

Save to file

Copy to clipboard

Cancel

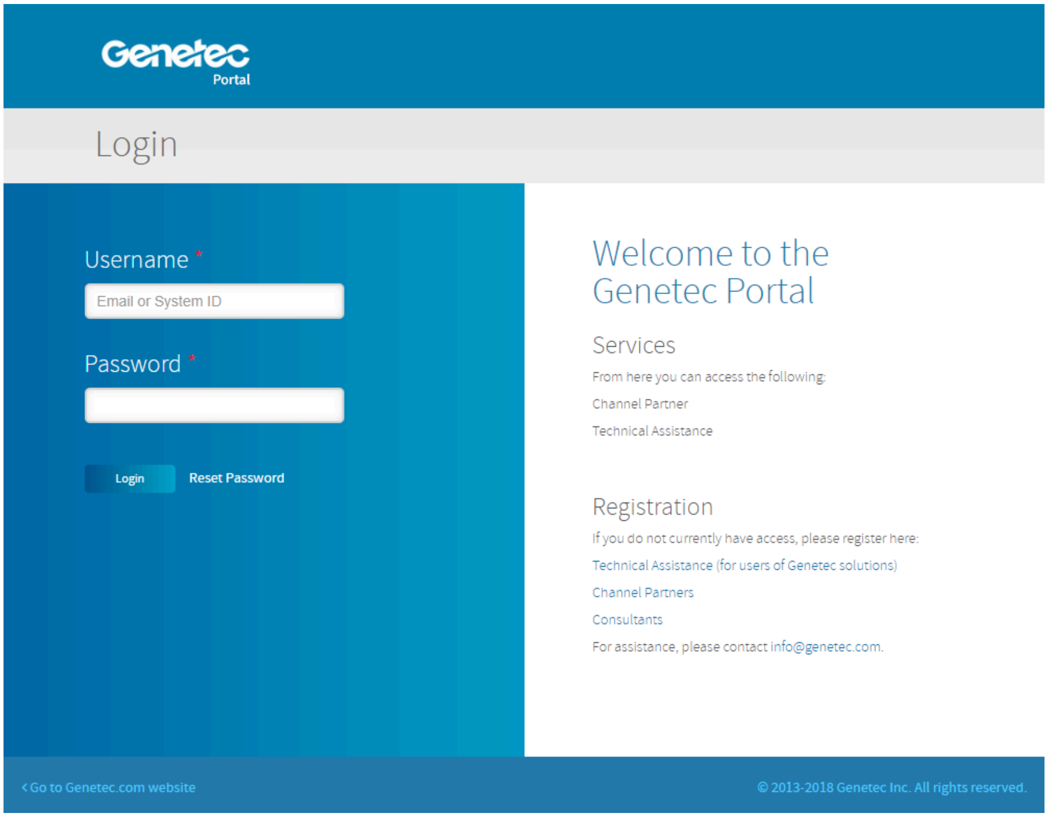
4 In the *License management* dialog box, click **Save to file** to save the composite validation key to a file.

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

A text file named *validation.vk* is saved to your default *Downloads* folder. Make sure you copy this file to a location (this can be a USB key) that you can access from another computer that has Internet access.

5 Move to the computer that has Internet access.

6 From another computer with Internet access, open the Genetec™ Technical Assistance Portal (GTAP) at: https://gtap.genetec.com.



Welcome to the Genetec Portal

Services

From here you can access the following:

Channel Partner

Technical Assistance

Registration

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

Technical Assistance (for users of Genetec solutions)

Channel Partners

Consultants

For assistance, please contact info@genetec.com.

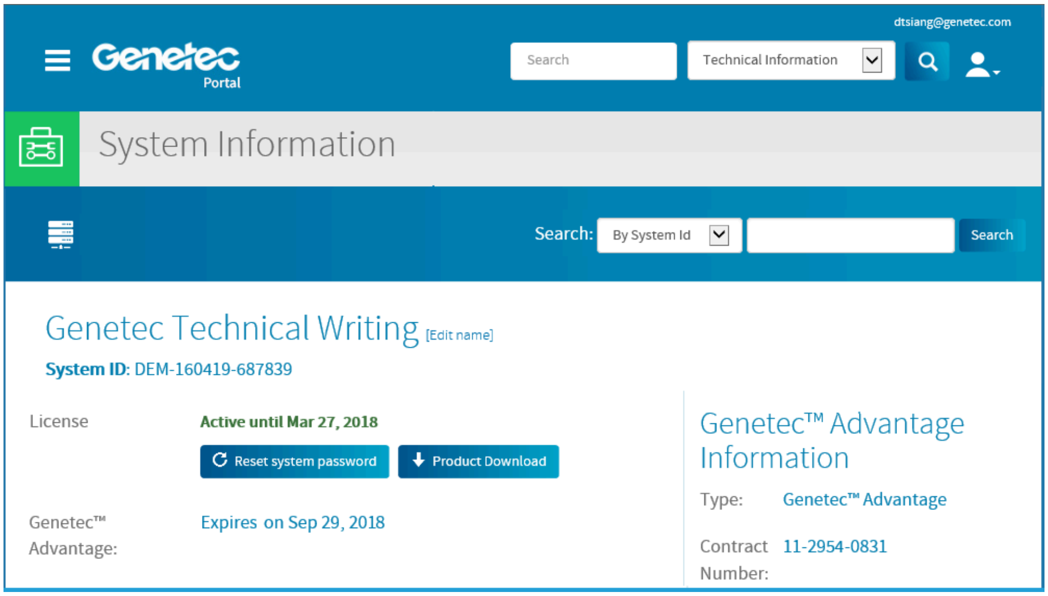
© 2013-2018 Genetec Inc. All rights reserved.

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

- Enter the System ID and the Password specified in the *Security Center License Information* document, and click **Login**.
- Enter your GTAP user account (your email address) and Password, and click **Login**

8 On GTAP, click **Activate new system**, select your system from the **System ID** drop-down list, and click **Submit**.

The the *System Information* page opens.



Genetec Technical Writing [Edit name]

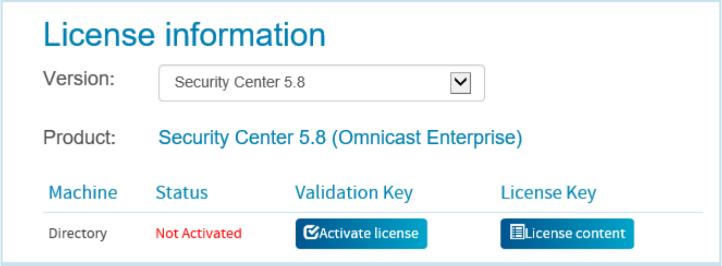
System ID: DEM-160419-687839

License	Active until Mar 27, 2018
Genetec™ Advantage:	Expires on Sep 29, 2018

Genetec™ Advantage Information

Type:	Genetec™ Advantage
Contract Number:	11-2954-0831

9 Scroll down to the *License information* section and click **Activate license**.



License information

Version: Security Center 5.8

Product: Security Center 5.8 (Omnicast Enterprise)

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

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

The message *License activation successful* appears.

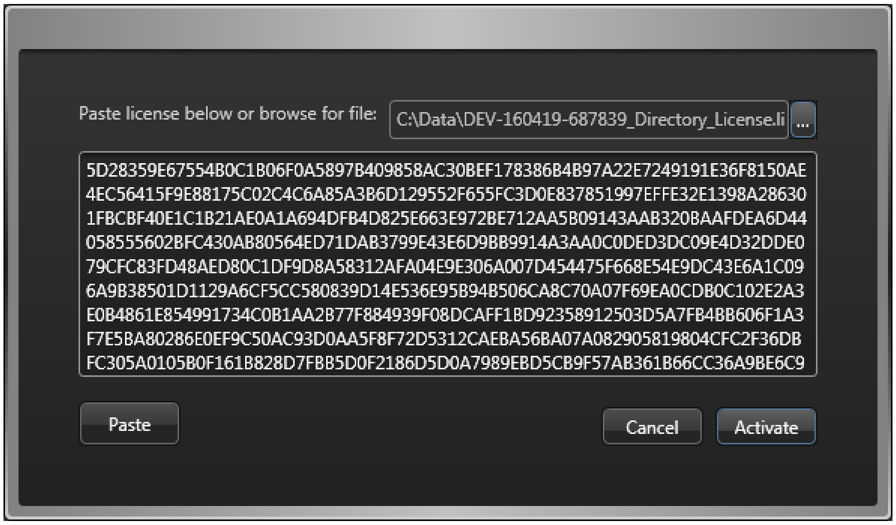
11 Click **Download License**, and save the license key to a file.

The default name is your System ID followed by *_Directory_License.lic*.

12 Return to the Config Tool workstation.

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

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



Paste license below or browse for file: C:\Data\DEV-160419-687839_Directory_License.li

```
5D28359E67554B0C1B06F0A5897B409858AC30BEF178386B4B97A22E7249191E36F8150AE
4EC56415F9E88175C02C4C6A85A3B6D129552F655FC3D0E837851997EFFE32E1398A28630
1FBCBF40E1C1B21AE0A1A694DFB4D825E663E972BE712AA5B09143AAB320BAAFDEA6D44
058555602BFC430AB80564ED71DAB3799E43E6D9BB9914A3AA0C0DED3DC09E4D32DDE0
79CFC83FD48AED80C1DF9D8A58312AFA04E9E306A007D454475F668E54E9DC43E6A1C09
6A9B38501D1129A6CF5CC580839D14E536E95B94B506CA8C70A07F69EA0CDB0C102E2A3
E0B4861E854991734C0B1AA2B77F884939F08DCAFF1BD92358912503D5A7FB4BB606F1A3
F7E5BA80286E0EF9C50AC93D0AA5F8F72D5312CAEBA56BA07A082905819804CFC2F36DB
FC305A0105B0F161B828D7FBB5D0F2186D5D0A7989EBD5CB9F57AB361B66CC36A9BE6C9
```

15 Click **Activate**.

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 apply a 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 can 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 skip the backup.
- 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 5.8 Config Tool to connect it to the 5.8 Directory. If Security Center Client is installed on the main server, upgrade it at the same time.

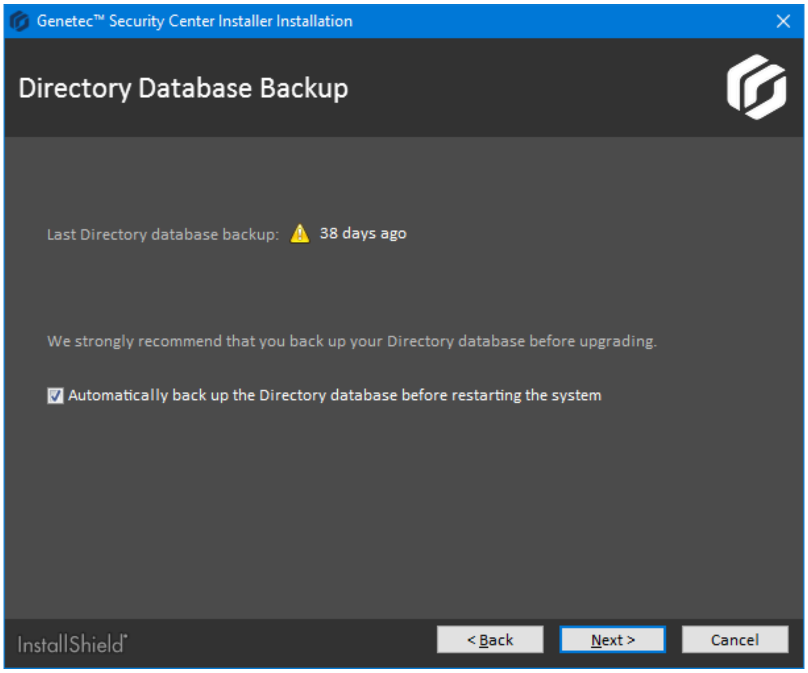
If a reboot warning message box opens during the upgrade, accept the message and continue with the upgrade procedure. You must reboot after completing the upgrade.

To upgrade the main server:

1 Install Security Center 5.8 on your main server.

  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 5.8.

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



Genetec™ Security Center Installer Installation
Directory Database Backup

Last Directory database backup: ⚠ 38 days ago

We strongly recommend that you back up your Directory database before upgrading.

☑ Automatically back up the Directory database before restarting the system

InstallShield
< Back
Next >
Cancel

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

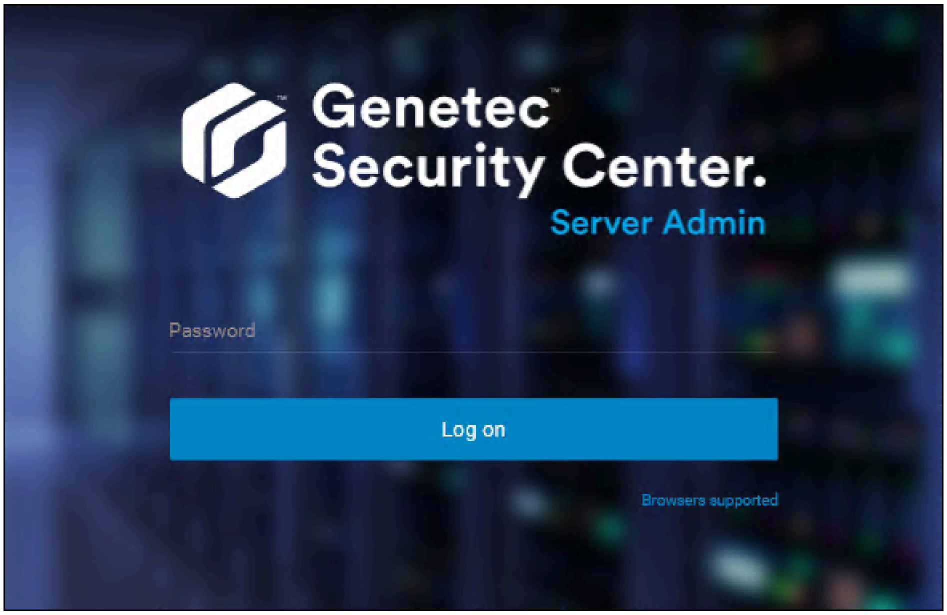
NOTE: For the last Directory database backup date, the Installer does not differentiate between full and incremental backups and does not check whether the backup files are still available. The automatic backup option always performs a full backup.

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.

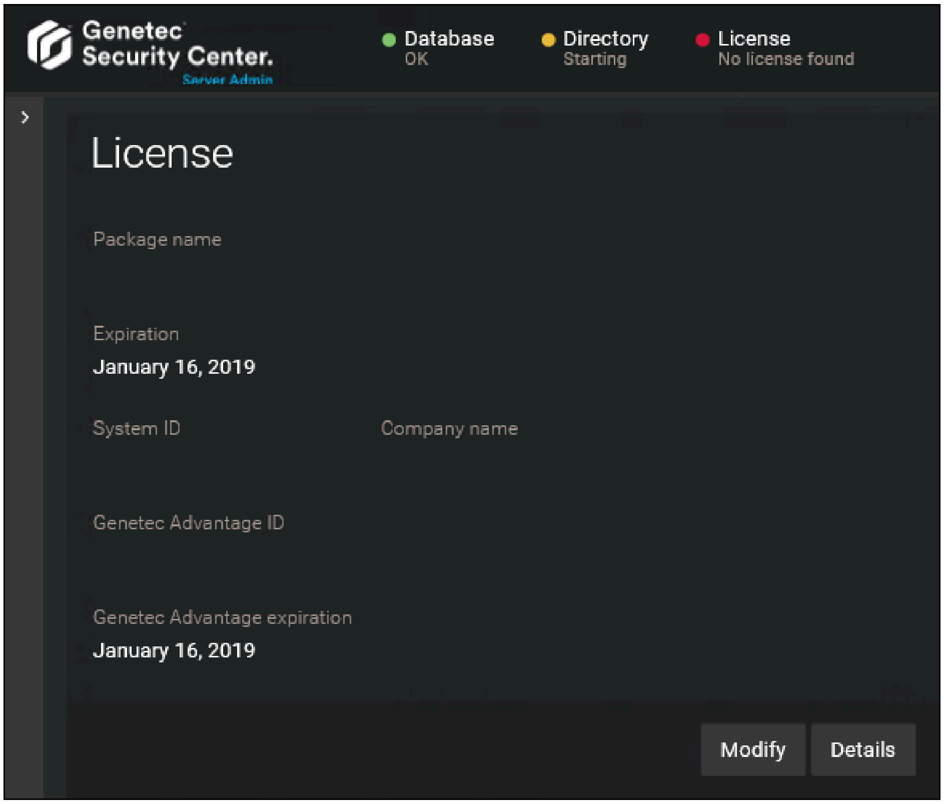
3 Follow the rest of the InstallShield Wizard instructions, and click **Install**.

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.

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



The Server Admin *Overview* page appears.



● Database OK
● Directory Starting
● License No license found

License

Package name

Expiration
January 16, 2019

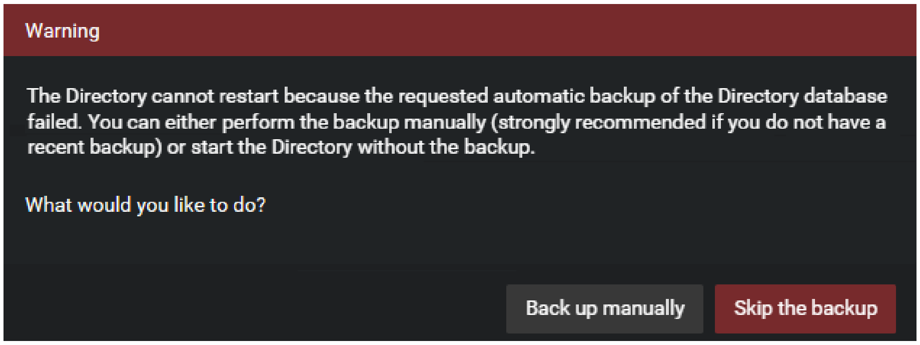
System ID

Company name

Genetec Advantage ID

Genetec Advantage expiration
January 16, 2019

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



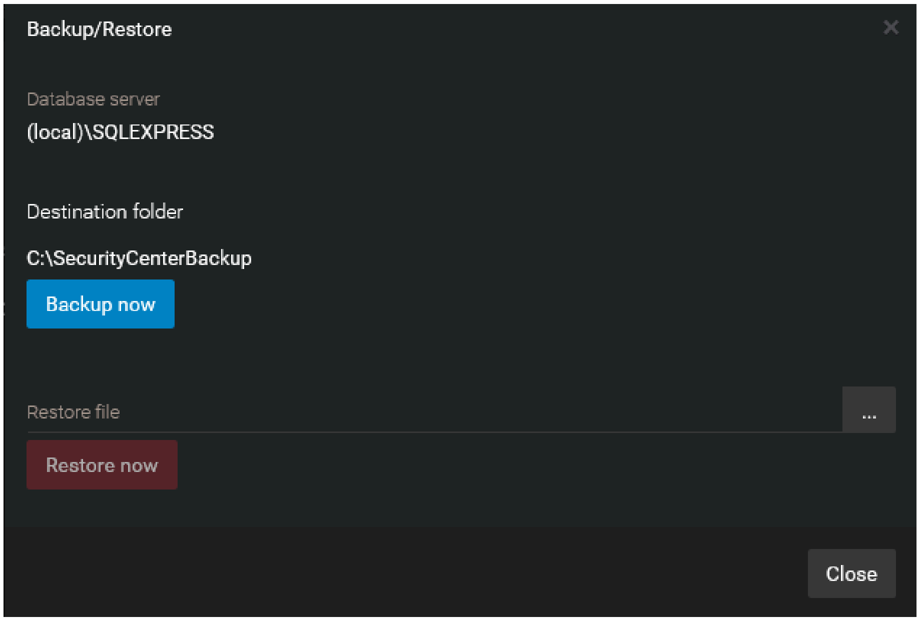
Warning

The Directory cannot restart because the requested automatic backup of the Directory database failed. You can either perform the backup manually (strongly recommended if you do not have a recent backup) or start the Directory without the backup.

What would you like to do?

You must choose one of the following:

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

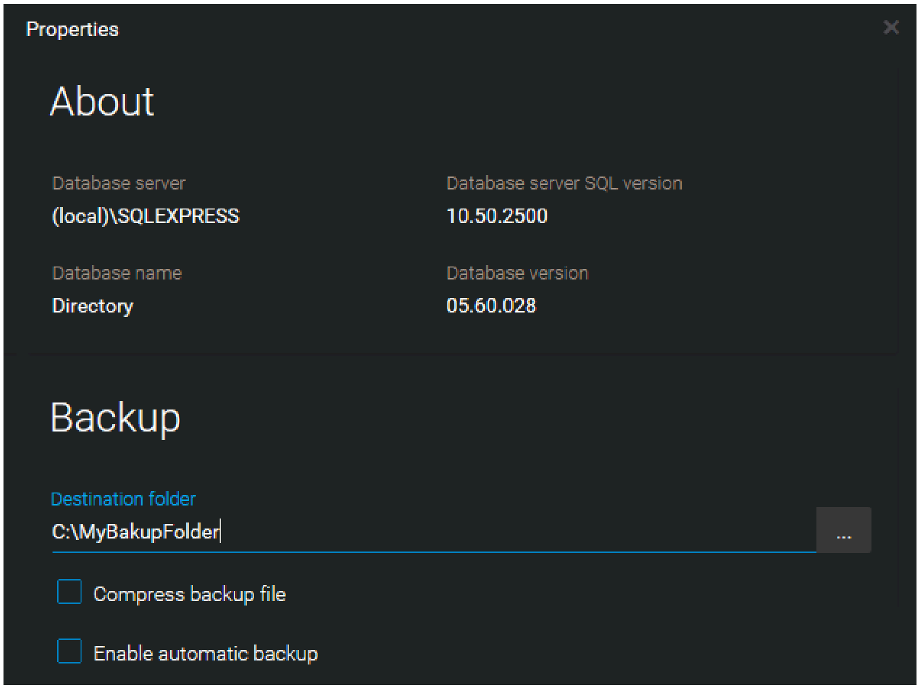


Backup/Restore

Database server: (local)\SQLEXPRESS

Destination folder: C:\SecurityCenterBackup

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**.



Properties

About

Database server
(local)\SQLEXPRESS

Database server SQL version
10.50.2500

Database name
Directory

Database version
05.60.028

Backup

Destination folder
C:\MyBakupFolder

□ Compress backup file

□ Enable automatic backup

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.

6 If you are upgrading from an earlier minor version (X.Y), activate your new Security Center 5.8 license.

7 If an LPR Manager hosted on this server is in the warning state (yellow) after the upgrade, enable it by assigning an Archiver to it.

Related Topics

Backing up databases on page 68
Preparing to upgrade to Security Center 5.8 on page 63
Upgrading the Security Center Directory database on page 91
Activating Security Center license using the web on page 29
Activating Security Center license without Internet access on page 33

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 5.8 on your expansion server.

   Use the **Expansion server** installation type.

   The installer automatically detects an earlier version of Security Center software and upgrades it to 5.8.
2. 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.
3. If an LPR Manager hosted on this server is in the warning state (yellow) after the upgrade, enable it by assigning an Archiver to it.
4. 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 68

Preparing to upgrade to Security Center 5.8 on page 63

Enabling the LPR Manager after an upgrade

To enable an LPR Manager that is in the warning state (yellow) after an upgrade, you must assign an Archiver role to it.

Before you begin

Do the following:

- Read the *Security Center Release Notes* for important information about the differences between LPR Manager 5.5 or earlier and 5.8.
- Set up the Archiver for managing the images associated to the reads and hits.

What you should know

After upgrading the LPR Manager from 5.5 or earlier to 5.8, the LPR Manager continues to manage the image data that were collected before the upgrade. Only the new image data are managed by the Archiver. The old image data remain in the LPR Manager database for as long as their retention period specifies, and then they are deleted. Deleting the old image data frees up space in the LPR Manager database for new LPR metadata, but the database file will not shrink in size.

To enable the LPR Manager after an upgrade:

1 From the Config Tool home page, click **System** > **Roles**.

2 Click the LPR Manager that is in the warning state, and click **Resources**.

3 Click **Images saved to**, and select the Archiver role you created earlier.

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

Setting up the Archiver role for LPR

You must link an Archiver to the LPR Manager to store the LPR images that are associated with the reads and hits.

What you should know

If you need to manage both LPR and video data, we recommend that you create separate Archiver roles, each handling only one function.

Each Archiver role must store video on a separate drive or partition from other Archiver roles. If you are unable to have separate Archiver roles, you can manage both LPR and video data with the same Archiver. Note that by default, the Archiver deletes the oldest files when its disks become full. This means that LPR images might be deleted before their retention period is over. This does not affect LPR metadata or the protected events and images.

To create an Archiver role for LPR:

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

2 Click the menu button beside **Video unit** (➕), and then click **Archiver** (🗄).

The role creation wizard window opens.

3 On the *Specific info* page, set the following fields, and then click **Next**.

- **Server:** This is only shown if you have more than one server in your system. If the LPR Manager is hosted on its own server, we suggest using the same server to host the linked Archiver role. If it is an upgrade from Security Center 5.5 or earlier, make sure you have enough free space on disk to store the LPR images. We recommend using a server where it is possible to configure the Archiver role with its dedicated local disk or disk partition.

- **Database server:** Name of the SQL Server service (default=`(local)\SQLEXPRESS`). If the Archiver is hosted on the same server as the LPR Manager, we recommend using the same database server for both.
- **Database:** Name of the database instance (default=`Archiver`). We suggest using `LPR_Archiver` to differentiate it from video archive databases.

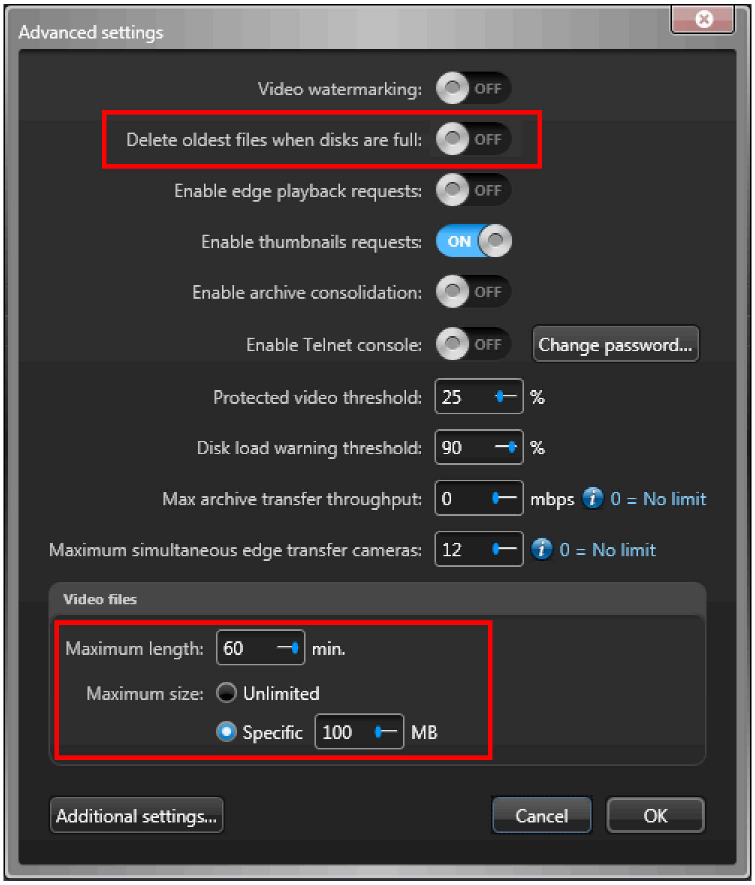
4. On the *Basic information* page, set the following fields, and then click **Next**.
   - **Entity name:** Name of the Archiver role (default=`Archiver`).

     We suggest using `LPR_Achiver` to differentiate it from the Archiver role for video.
   - **Entity description:** Role description. If this Archiver role is shared by many LPR Manager roles, list them here.
   - **Partition:** This is only shown if you have partitions defined in your system. Make sure you create this Archiver in the same partition as the LPR Manager it is linked to. Only users who have access to the selected partition can view the LPR data managed by these roles.
5. Verify that the information displayed in the *Creation summary* page is correct, and then click **Create**.
6. Click **Close**.
7. From the Archiver role's **Resources** tab, configure the archive storage settings.

   IMPORTANT: Ensure you are not using the same disk as another Archiver role in your system, and that you have enough disk space for storing the LPR images. For more information on the storage requirements for LPR images, refer to the *Security Center Release Notes*.

   NOTE: The Archiver follows the **Hit** and **Read image retention period** set for the LPR Manager. If multiple LPR Manager roles are linked to the same Archiver, the LPR Manager with the longest image retention period has precedence. This means that the image data might be kept longer than necessary for some LPR Manager roles, but it does not affect the LPR metadata nor the LPR reports. No LPR data beyond the specified retention periods appear in reports.

8 Click **Advanced settings**, and optimize the settings for storing LPR image data.



Advanced settings

Video watermarking: OFF

Delete oldest files when disks are full: OFF

Enable edge playback requests: OFF

Enable thumbnails requests: ON

Enable archive consolidation: OFF

Enable Telnet console: OFF

Protected video threshold: 25 %

Disk load warning threshold: 90 %

Max archive transfer throughput: 0 mbps 0 = No limit

Maximum simultaneous edge transfer cameras: 12 0 = No limit

Video files

Maximum length: 60 min.

Maximum size: ○ Unlimited

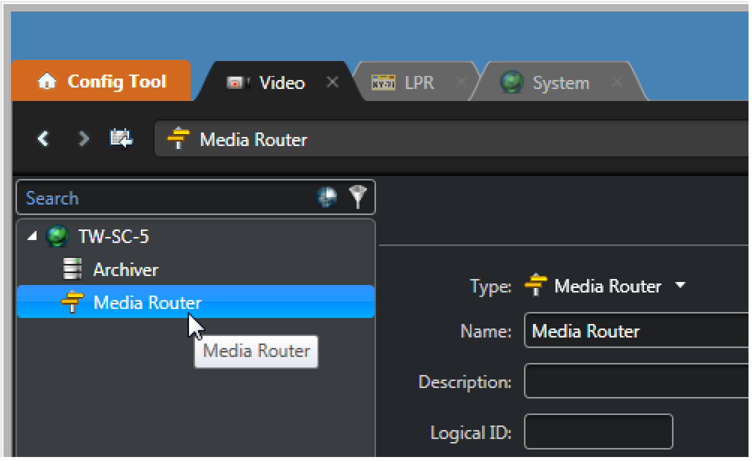
● Specific 100 MB

The recommended values are:

- **Delete oldest file when disks are full:** OFF (default setting for video is ON).
- **Maximum length:** 60 minutes (default value for video is 20 minutes).
- **Maximum size:** 100 MB (default value for video is 500 MB).

9 Click **OK** > **Apply**.

10 In the entity browser (left pane) of the *Video* task, make sure that the Media Router role is running.



Type: Media Router

Name: Media Router

Description:

Logical ID:

11 Click **Media Router** and configure the ports, redirectors, and network cards to make sure that the Archiver can deliver the LPR images to all client workstations on your system.

If all your servers are on the same network, and all your servers have only one network card, the default settings should work without any change.

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 5.8 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.

To upgrade from a previous version of Security Center Client (5.4 and later) to 5.8:

- Install Security Center Client.

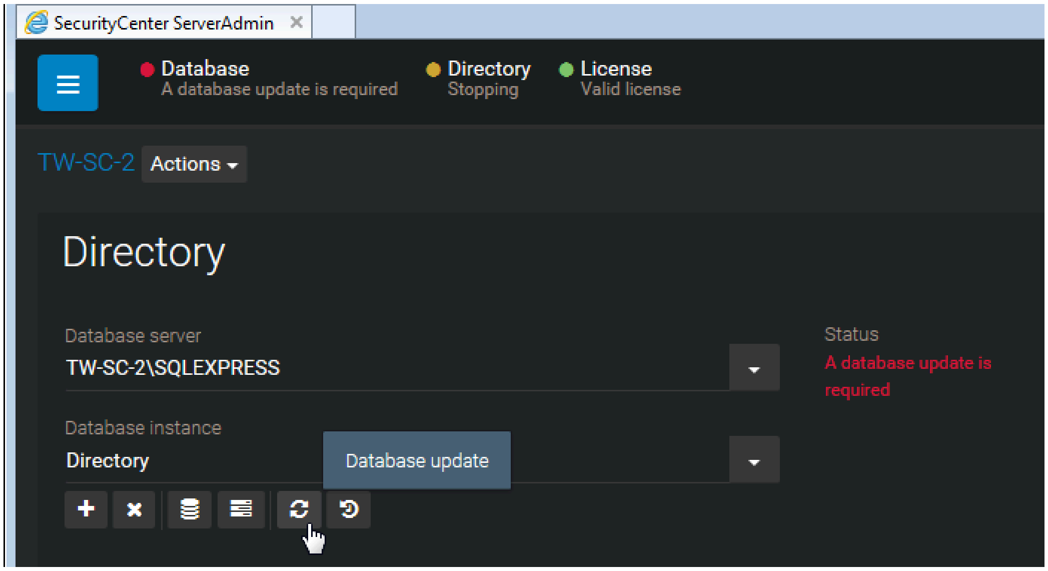
  The installer automatically detects an earlier version of Security Center software and applies the current settings to 5.8.

Upgrading the Security Center Directory database

The Security Center 5.8 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*.



Database server: TW-SC-2\SQLEXPRESS

Status: A database update is required

Database instance: Directory

To upgrade the Directory database:

1 Do one of the following:

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

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

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

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

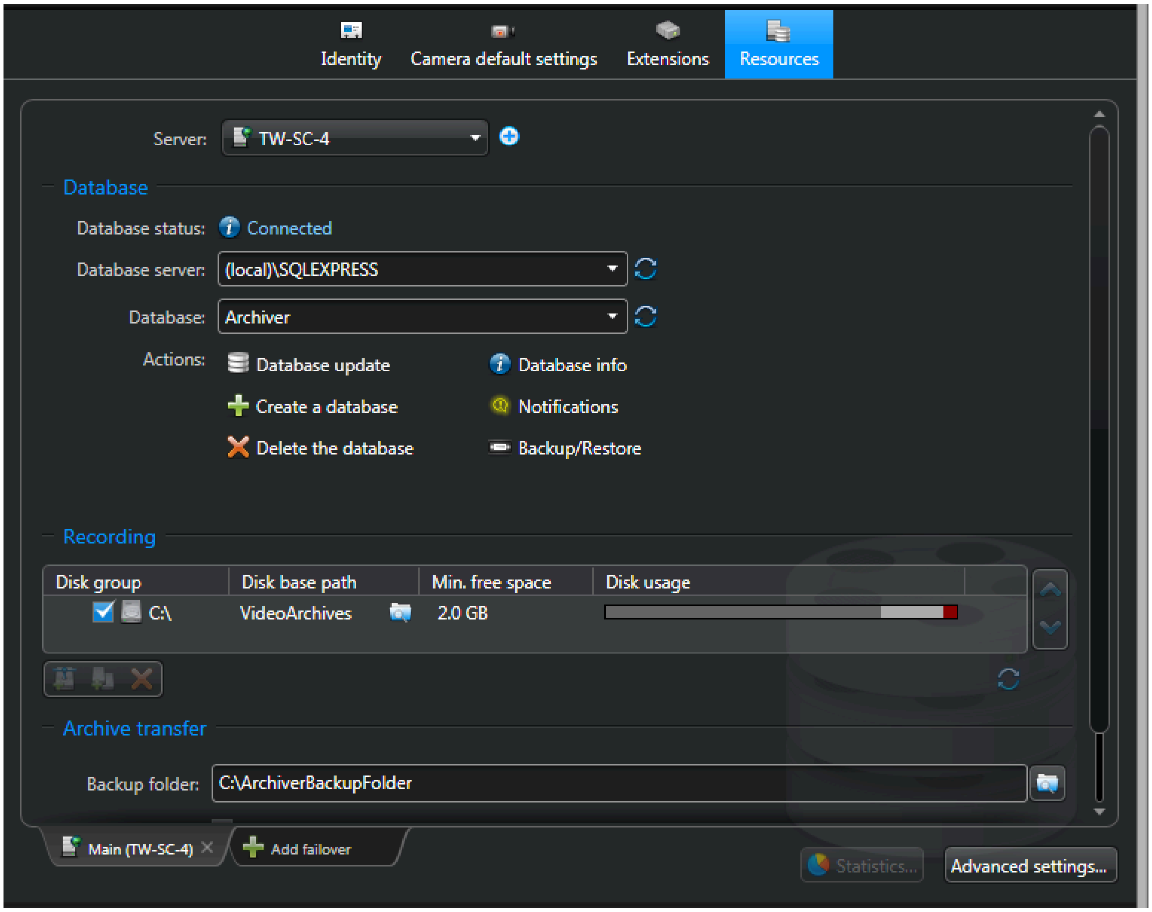
3 Click **Database properties** (≣) to confirm the version of the database and the number of entities in the database.

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

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

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

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



Server: TW-SC-4

Database

Database status: Connected

Database server: (local)\SQLEXPRESS

Database: Archiver

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

Recording

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

Archive transfer

Backup folder: C:\ArchiverBackupFolder

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

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

After you finish

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

Shrinking Security Center databases after an upgrade

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

Before you begin

Not all database upgrades cause the database to grow in size. However, in the case of the Archiver database upgrade from 5.3 to 5.8, we do recommend shrinking the database after the upgrade. 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.

3

LPR database migration

This section includes the following topics:

Migrating an LPR database from Security Center 5.6 GA or earlier

If you are upgrading from Security Center 5.6 GA or earlier to 5.8, you must migrate your existing LPR data to the new database structure.

Before you begin

Upgrade your system to Security Center 5.8 GA.

IMPORTANT: The LPR database migration is not compatible with Microsoft SQL Server 2016 and later. Before attempting the migration, ensure that you are running an earlier version of SQL Server. The following database engines are supported:

- SQL Server 2008 R2 Express/Standard/Enterprise
- SQL Server 2012 Express/Standard/Enterprise
- SQL Server 2014 Express/Standard/Enterprise

After migrating to the new database structure, you can upgrade SQL Server as needed.

What you should know

- The LPR database improvements were released in Security Center 5.6 SR1. This procedure applies to systems upgrading from Security Center 5.6 GA and earlier to Security Center 5.8 GA.
- Starting from Security Center 5.6 SR1, license plate reads and hits are decoupled from the LPR images (license plate, context, and wheel images). As a result, the LPR Manager can store up to 6 millions reads in the SQL Server Express database, which is 25 to 30 times more reads than before. The responsiveness of the LPR reports is also improved because of database enhancements and the *lazy loading* of report images in Security Desk.
- You can migrate the database while the system is in operation; however, we recommend that you perform the migration outside of peak usage hours. Depending on the size of the database, the amount of image data to migrate, and the performance of the Archiver disk, the database migration can take from several hours to several days to complete.
- If the system includes more than one LPR Manager role, we recommend that you migrate one LPR Manager at a time. Upgrading in increments does not affect system functionality.
- While the migration is in progress, you can edit reads that were collected after the Security Center 5.8 GA upgrade.

  CAUTION: Do not attempt to edit or protect old reads and hits (pre-upgrade) until the migration is complete. If you must edit or protect an old read, you can temporarily stop the migration.
- Database cleanup and housekeeping is only done after the database has been migrated and validated.
- You can stop and restart the migration without losing data. For example, you might need to stop the migration if you are experiencing performance issues while migrating the database on a live system and you prefer to perform the migration in stages each night.

  CAUTION: If you experience problems during the migration, you can restart the migration, but do not restore the database. If the system is in operation during the migration, restoring the database causes the loss of all new LPR data that was added after the migration started.

To migrate an LPR database to the Security Center 5.6 structure:

1 Back up the LPR database for each LPR Manager role.

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

   b) Select an LPR Manager role, and click **Resources**.

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

   d) In the *Actions* section, click **Backup/Restore** ().

2 Back up the Directory database.

3 Assign a unique logical ID to each of the LPR Managers in the system. The logical ID is used to reference the LPR Manager role for the migration process.

CAUTION: After the migration starts, do not change the logical ID until the migration is complete.

a) Open the *LPR* task, and select **Roles and units**.

b) Select an LPR Manager.

c) In the **Identity** tab, enter a **Logical ID**.

a) Click **Apply**.

4 Launch the database migration.

a) Start the **Security Center Server Admin** () application.

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

The Server Admin *Overview* page is displayed.

c) Select your server from the *Servers* list.

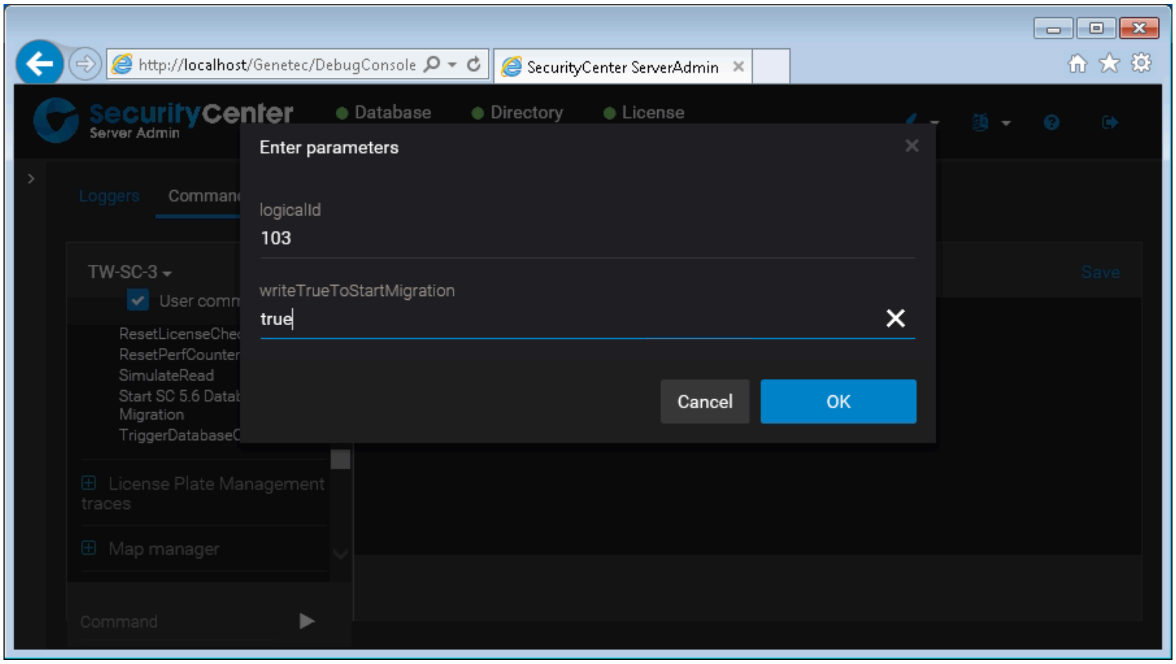
d) From the **Actions** drop-down list, select **</> Console**.

e) Select the **Commands** tab.

f) From the commands list, expand **License Plate Management commands** and select **Start SC 5.6 Database Migration**. The *Enter parameters* window is displayed.

g) Enter the **logical ID** of the LPR Manager role whose database you want to migrate.

h) In the **writeTrueToStartMigration** field, type `true` and click **OK**.



logicalId
103

writeTrueToStartMigration
true

The system starts the migration on the selected LPR Manager role.

After you finish

To view the progress of your database migration in Server Admin, from the commands list, expand **License Plate Management commands** and select **Database Migration Status**. Enter the **logical ID** of the LPR Manager role whose database you are migrating, and then click **OK**.

Stopping the Security Center 5.6 LPR database migration

While migrating an LPR Manager database to the Security Center 5.6 structure, you can stop and restart the migration at any point without losing data.

What you should know

You might need to stop the migration if you are experiencing performance issues while migrating the database on a live system and you prefer to perform the migration in stages each night.

To stop the LPR database migration:

1 Start the **Security Center Server Admin** ( ) application.

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

The Server Admin *Overview* page is displayed.

3 Select your server from the *Servers* list.

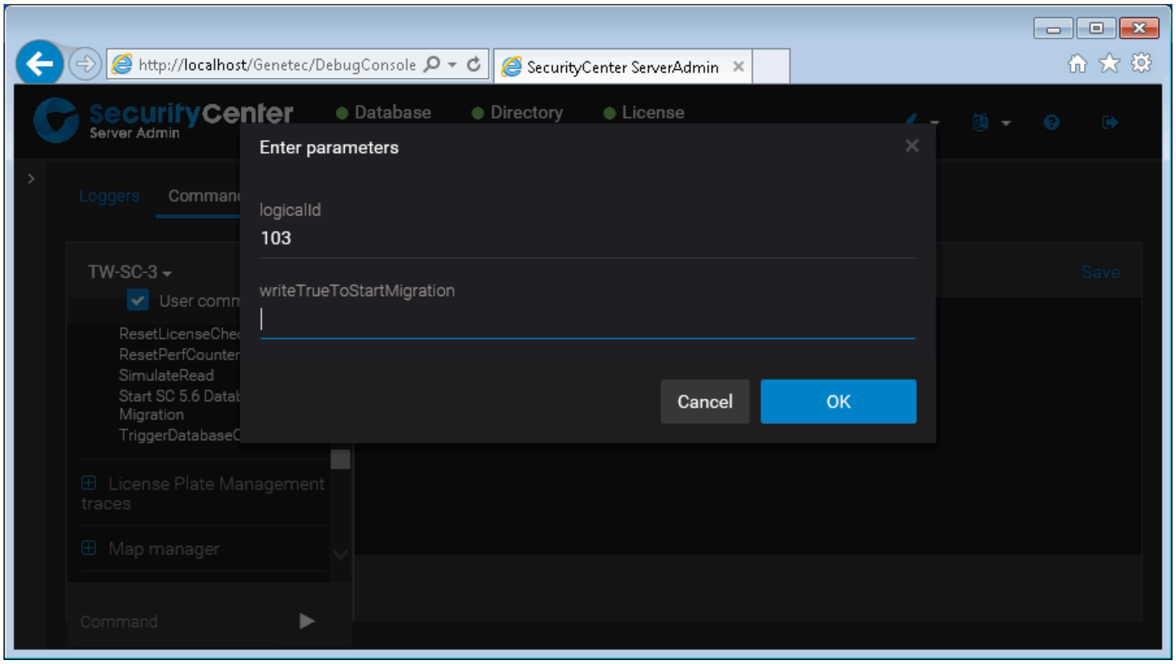
4 From the **Actions** drop-down list, select **</> Console**.

5 Select the **Commands** tab.

6 From the commands list, expand **License Plate Management commands** and select **Start SC 5.6 Database Migration**. The *Enter parameters* window is displayed.

7 Enter the **logical ID** of the LPR Manager role where the database migration is in progress.

8 Leave the **writeTrueToStartMigration** field blank, and click **OK**.



Enter parameters

logicalId

103

writeTrueToStartMigration

Cancel

OK

The migration of the LPR Manager database stops.

After you finish

To view the progress of your database migration in Server Admin, from the commands list, expand **License Plate Management commands** and select **Database Migration Status**. Enter the **logical ID** of the LPR Manager role whose database you are migrating, and then click **OK**.

4

Automating Security Center installation

This section includes the following topics:

Silent installation in 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.

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 on a separate drive on page 14

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> <setup_options> <msi_options>
```

where:

- `<setup_exe>`**:** This 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.
- `<setup_options>`**:** These are the setup options. They all start with a forward slash (/).
- `<msi_options>`**:** These are the Installer (MSI) options. They are all written in capital letters.

The following table lists the setup options.

Setup option	Description
`/ISInstallDir`	Specifies the root folder where the product subfolder (*Genetec Security Center 5.8*) will be created. **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.
`/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 MSI 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
<msi_options>	Sets the Security Center Installer (MSI) 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

Installer (MSI) options on page 103

Installer (MSI) options

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

The following table lists the Security Center Installer (MSI) options. All installer 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: Beginning with Security Center 5.6, 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.

Installer (MSI) 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`
`COLLECTPOLICY`	Configure the data collection policy for our Product Improvement Program. The possible 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`
`CREATE_FIREWALL_RULES`	Add the installed Security Center applications to the Windows Firewall exceptions list. Possible values are 0 or 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. Possible values are 0 or 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`

Installer (MSI) option	Description
`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`
`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.

Installer (MSI) option	Description
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
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 possible 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 possible 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.

Installer (MSI) option	Description
SERVICEPASSWORD	Specify the password to use in the services. **EXAMPLE**: SERVICEPASSWORD=anypassword User and password need to be created first with the right credentials before using those properties. If not specified, the default is blank.
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
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**: • SQL_INSTANCE_NAME=(local)\SQLEXPRESS2 (WRONG) • SQL_INSTANCE_NAME=SQLEXPRESS2 (CORRECT)
SQLSERVER_GROUP	Specify if a new or an existing SQL server is silently installed. The possible 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 5.8 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
  ```

5

Troubleshooting

This section includes the following topics:

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".
- You install Security Center on a 64-bit version of Windows 7 SP1 or Windows Server 2008 R2 SP1. To enhance performance, you must install hotfix 2588507.

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.

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.

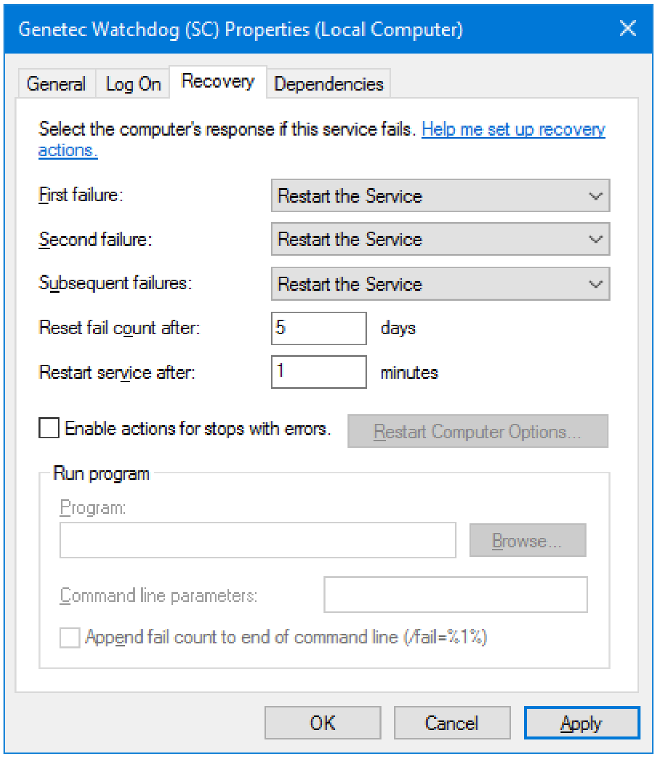
To manually create Security Center services:

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 5.8*. This path must be changed if Security Center was installed to another location.

```
sc create GenetecWatchdog binPath= "C:\Program Files (x86)\Genetec Security
                                Center 5.8\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**.


Genetec Watchdog (SC) Properties (Local Computer)
General
Log On
Recovery
Dependencies
Restart Computer Options...
Run program
Browse...
OK
Cancel
Apply

Select the computer's response if this service fails. Help me set up recovery actions.

First failure: Restart the Service

Second failure: Restart the Service

Subsequent failures: Restart the Service

Reset fail count after: 5 days

Restart service after: 1 minutes

□ Enable actions for stops with errors.

Program:

Command line parameters:

□ Append fail count to end of command line (/fail=%1%)

   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 5.8\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 5.8*. This path must be changed if Security Center was installed to another location.

```
sc create GenetecServer binPath= "C:\Program Files (x86)\Genetec Security
                                Center 5.8\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 allows you to configure access control roles, units, rules, cardholders, credentials, and related entities and settings.

Access control health history

Access control health history is a type of maintenance task that reports on malfunction events for access control units.

access control unit

An access control unit is an entity that 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

Access control unit events is a type of 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

Access rule configuration is a type of 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. It is also a type of role that enables Security Center to receive claims from an external ADFS server.

Activity trails
Activity trails is a type of maintenance task that reports on the user activity related to video, access control, and LPR 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 is a type of entity that describes a particular 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 it, who must be notified, how it must be displayed to the user, and so on.

alarm acknowledgement
An alarm acknowledgement is a user response to an alarm. In Security Center, the default acknowledgement and alternate 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

Alarm monitoring is a type of operation task that allows you to monitor and respond to alarms (acknowledge, forward, snooze, and so on) in real time, as well as review past alarms.

Alarm report

Alarm report is a type of investigation task that allows you to search and view current and past alarms.

Alarms

The *Alarms* task is an administration task that allows you to configure alarms and monitor groups.

AutoVu™ Managed Services

With AutoVu™ Managed Services (AMS), your license plate recognition (LPR) 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.

analog monitor

An analog monitor is a type of entity that 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.

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

Archiver events is a type of 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

Archives is a type of investigation task that allows you to find and view available video archives by camera and time range.

Archive storage details

Archive storage details is a type of 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, and which allows you to change the protection status of those files, among other things.

Archive transfer

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, the *Archive transfer* task is part of 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.

area 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 Area activities is a type of investigation task that reports on access control events pertaining to selected areas.

Area presence Area presence is a type of 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 allows you 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 is a type of entity that represents any valuable object with an RFID tag attached, thus allowing it to be tracked by an asset management software.

asynchronous video An asynchronous video is a type of entity that represents any valuable object with an RFID tag attached, thus allowing it to be tracked by an asset management software.

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 Audit trails is a type of maintenance task that reports on the configuration changes of the selected entities in the system and 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 the term used for *license plate recognition (LPR)* in Europe.

AutoVu™

Security Center AutoVu™ is the automatic license plate recognition (ALPR) system that automates license plate reading and identification. Deployed in both fixed and mobile installations, it lets you extend your physical security into your parking lots and perimeter, so you are always aware of vehicles moving in and out of your facilities.

AutoVu™ LPR Processing Unit

AutoVu™ LPR Processing Unit is the processing component of the SharpX system. The LPR 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 LPR Processing Unit is sometimes referred to as the *trunk unit* because it is typically installed in a vehicle's trunk.

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

Badge designer is a tool that allows you to design and modify badge templates.

badge template

A badge template is a type of entity used to configure a printing template for badges.

block face (2 sides)

A block face (2 sides) is a type of 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 body 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

Bookmarks is a type of 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

Camera configuration is a type of 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

Camera events is a type of 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 a type of 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 is a type of entity that 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

Cardholder access rights is a type of maintenance task that reports on which cardholders and cardholder groups are granted or denied access to selected areas, doors, and elevators.

Cardholder activities

Cardholder activities is type of investigation task that reports on cardholder activities, such as access denied, first person in, last person out, antipassback violation, and so on.

Cardholder configuration

Cardholder configuration is a type of 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 a type of entity that configures the common access rights of a group of cardholders.

Cardholder management

Cardholder management is a type of operation task that allows you to create, modify, and delete cardholders. In this task, you can also manage a cardholder's 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.

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 and of the Navigator is mandatory.

claim

A *claim* is a statement that one subject makes about itself or another subject. The statement can be about a name, identity, key, group, privilege, or capability, for example. Claims are issued by a provider, and they are given one or more values and then packaged in security tokens that are issued by an *issuer*, commonly known as a *security token service* (STS).

claims-based authentication

Claims-based authentication is the process of authenticating a user based on a set of claims about its identity contained in a trusted token. Such a token is often issued and signed by an entity that is able to authenticate the user by other means, and that is trusted by the entity doing the claims-based authentication.

claims provider

A software component or service that generates security tokens upon request. Also known as the issuer of claims.

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 Archives

Cloud Archives is a service from Genetec Inc. that enables organizations to maintain video recordings in the cloud, while continuing to leverage their existing Security Center system.

cloud platform

A cloud platform provides remote computing and storage services through centralized data centers that are accessible via the Internet.

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, LPR units, and hardware devices.

Conflict resolution utility 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 LPR unit that produces a wider angle color image of the vehicle whose license plate was read by the LPR camera.

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™ Applicance 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.

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 is a type of entity that 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 Credential activities is a type of investigation task that reports on credential related activities, such as access denied due to expired, inactive, lost, or stolen credential, 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 Credential configuration is a type of maintenance task that reports on credential properties, such as status, assigned cardholder, card format, credential code, custom properties, and so on.

Credential management Credential management is a type of operation task that allows you to create, modify, and delete credentials. It also allows you to 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 Credential request history is a type of investigation task that reports on which users requested, cancelled, or printed cardholder credentials.

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 to an entity type and is used to store additional information that is useful to your particular organization.

cyphertext In cryptography, cyphertext is the encrypted data.

Daily usage per Patroller Daily usage per Patroller is a type of 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.

dashboard A dashboard is one of the three panels that belong to the canvas in Security Desk. It contains the graphical commands (or widgets) pertaining to the entity displayed in the current tile.

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.

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 of time (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 Mercury and 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.

digital certificate

A digital certificate, also known as an *identity certificate* or *encryption certificate*, is an electronic "passport" that allows a person, computer, or organization to exchange information securely over the Internet using the public key infrastructure (PKI).

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 in order 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, LPR 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 type of 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

Door activities is a type of investigation task that 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

Door troubleshooter is a type of 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.

edge recording

Edge recording is the process of recording and storing recorded videos locally, 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 a type of entity that provides access control properties to elevators. For an elevator, each floor is considered an access point.

Elevator activities Elevator activities is a type of 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 via a Federation™ role, so that the local users can view and control its entities, as if they belong to the local system.

Federation™

The Federation™ feature joins multiple, independent Genetec™ IP security systems into a single virtual system. With this feature, Security Center users can view and control entities that belong to remote systems, directly from their local Security Center system.

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.

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

Forensic search is a type of investigation task that searches for video sequences based on video analytics events.

four-port RS-485 module

A four-port RS-485 module is a RS-485 communication component of Synergis™ Master Controller with four ports (or channels) named A, B, C, and D. The number of interface modules you can connect to each channel depends on the type of hardware you have.

free access

A free access is an access point state where no credentials are necessary to enter a secured area. The door is unlocked. This is typically used during normal business hours, as a temporary measure during maintenance, or when the access control system is first powered up and is yet to be configured.

free exit

A free exit is an access point state where no credentials are necessary to leave a secured area. The person releases the door by turning the doorknob, or by pressing the REX button, and walks out. An automatic door closer shuts the door so it can be locked after being opened.

fusion stream

Fusion stream is a proprietary data structure of Genetec Inc. for streaming multimedia. Each fusion stream is a bundle of data (video, audio, and metadata) streams and key streams related to a single camera. Fusion streams are generated on specific client requests. The key streams are included only if the data streams are encrypted.

fusion stream encryption

Fusion stream encryption is a proprietary technology of Genetec Inc. used to protect the privacy of your video archives. The Archiver uses a two-level encryption strategy to ensure that only authorized client machines or users with the proper certificates on smart cards can access your private data.

G64

G64 is a Security Center format used by archiving roles (Archiver and Auxiliary Archiver) to store video sequences issued from a single camera. This data format supports audio, bookmarks, metadata overlays, timestamps, motion and event markers, and variable frame rate and resolution.

G64x

G64x is a Security Center format used to store video sequences from multiple cameras that are exported or backed up simultaneously. This data format supports audio, bookmarks, metadata overlays, timestamps, motion and event markers, variable frame rate and resolution, and watermarking.

Genetec Clearance™ Uploader

Genetec Clearance™ Uploader is an application that is used to automatically upload media from a body-worn camera or sync folder, or other devices into Genetec Clearance™ or a Security

Center video archive depending on the *.json* config file that 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. Genetec Mission Control™ empowers organizations to move beyond simple event and alarm management by collecting and qualifying data from thousands of sensors and security devices, spotting the most complex situations and incidents, and guiding security teams in their response following organization-specific processes and compliancy requirements. To learn more about Genetec Mission Control™, refer to the Genetec.com resource hub.

Genetec™ Mobile

Official name of the map-based Security Center mobile application for Android and iOS devices.

Genetec™ Protocol

Genetec™ Protocol is a standard protocol developed by Genetec Inc. that third-party video encoder and IP camera manufacturers can use to integrate their products to Security Center Omnicast™.

Genetec™ Server

Genetec™ Server is the Windows service that is at the core of Security Center architecture, and that must be installed on every computer that is part of the Security Center's pool of servers. Every such server is a generic computing resource capable of taking on any role (set of functions) you assign to it.

Genetec™ Update Service

The Genetec™ Update Service (GUS) is automatically installed with most Genetec™ products and enables you to update products when a new release becomes available.

Genetec™ Video Player

Genetec™ Video Player is a 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 is the process of finding associated geographic coordinates (latitude and longitude) from a street address.

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 is an entity automatically created by the LPR Manager when the AutoVu™ license includes the XML Import module. In Security Center, all LPR data must be associated to a Genetec Patroller™ entity or an LPR unit corresponding to a fixed Sharp camera. When you import LPR data from an external source via a specific LPR Manager using the XML Import module, the system uses the ghost entity to represent the LPR 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 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*.

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

Hardware inventory is a type of 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 LPR units in your system.

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.

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 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.

Health history

Health history is a type of 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

Health statistics 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

Hit rule is a type of LPR 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

Hits is a type of 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

Hotlist and permit editor is a type of operation task used 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, users can edit, add, or delete items from the list, and the original text file is updated with the changes.

hotspot

Hotspot is a type of 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, also known as a *digital certificate* or *public key certificate*, is a digitally signed document that allows a computer or an organization to exchange information securely over a public network. The certificate includes information about the owner's identity, the *public key* used to encrypt future messages sent to the owner, and the digital signature of the certificate authority (CA).

identity provider

An Internet site that administers user accounts and is responsible for generating and maintaining user authentication and identity information. For example, Google administers Gmail accounts to its users, which allows single sign-on access to other websites using one account.

illuminator

An illuminator is a light in the Sharp unit that illuminates the plate, thereby improving the accuracy of the images produced by the LPR camera.

Import tool

Import tool is a tool that allows you 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 (Mission Control)

A Genetec Mission Control™ incident is an unusual or undesirable situation that requires actions to resolve.

incident category

An incident category is a type of entity that represents a grouping of incident types that have similar characteristics.

Incident configuration

The *Incident configuration* task is the administration task that you can use to configure the incident types, the incident categories, and the support documents for 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 incident workflows and keeps track of all user activities that are related to incidents.

Incident monitoring

The *Incident monitoring* task is a type of 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 a type of investigation task that you can use to search, review, and analyze 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 a sequence of rules that are applied by the Genetec Mission Control™ Rules Engine to automatically detect and trigger incidents. The Rules Engine looks for specific combinations of events (type, time, correlation, and frequency) in the system in order to determine whether an incident must be triggered.

incident type

An incident type is an entity that represents a situation that requires specific actions to resolve it. The incident type entity can also be used to automate the incident detection in Mission Control and to enforce the standard operating procedures that your security team must follow.

incident workflow

An incident workflow is a series of activities associated to an incident type. These activities are performed by the system during the life cycle of an incident. The activities can change the incident state and properties, affect other entities in the system, or simply wait for a condition to become true. The workflows help automate the simple tasks, such as exporting the incident when it is resolved, so operators can focus on more complex ones.

Incidents

Incidents is a type of investigation task that allows you to search, review, and modify incident reports.

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 door to be open at any given time.

Intrusion detection

The *Intrusion detection* task is an administration task that allows you to configure intrusion detection roles and units.

intrusion detection area

An intrusion detection area is an entity that represents a zone (sometimes called an area) or a partition (group of sensors) on an intrusion panel.

Intrusion detection area activities

Intrusion detection area activities is a type of 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 is an entity that 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

Intrusion detection unit events is a type of 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) 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

Inventory management is a type of operation task that allows you to add and reconcile license plate reads to a parking facility inventory.

Inventory report

Inventory report is a type of investigation task that allows you 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

I/O configuration is a type of 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™ Intrusion Detector

(Obsolete) In KiwiVision™ video analytics, KiwiVision™ Intrusion Detector is the module that adds the intrusion detection analytics capability to Security Center.

KiwiVision™ Privacy Protector™

KiwiVision™ Privacy Protector™ is a Security Center platform 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 is an entity that 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 LPR technology.

license plate recognition

License plate recognition (LPR) is an image processing technology used to read license plate numbers. LPR converts license plate numbers cropped from camera images into a database searchable format.

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

Logons is a type of investigation task that reports on the logon records of a selected patrol vehicle.

long term

Long term is a type of parking regulation characterizing an overtime rule. The *long term* 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.

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 LPR Manager role.

LPR camera

A License Plate Recognition (LPR) camera is a camera connected to an LPR unit that produces high resolution close-up images of license plates.

LPR context

An LPR context is an LPR 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).

LPR Manager

The LPR Manager role manages and controls the patrol vehicle software (Genetec Patroller™), Sharp cameras, and parking zones. The LPR Manager stores the LPR data (reads, hits, timestamps, GPS coordinates, and so on) collected by the devices.

LPR rule

LPR rule is a method used by Security Center and AutoVu™ for processing a license plate read. An LPR rule can be a hit rule or a parking facility.

LPR

The *LPR* task is an administration task that allows you to configure roles, units, hotlists, permits, and overtime rules for LPR, and related entities and settings.

LPR unit

An LPR unit is a device that captures license plate numbers. An LPR unit typically includes an LPR camera and a context camera. These cameras can be incorporated to the unit or external to the unit.

macro

A macro is a type of 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.

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 LPR.

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 allows you 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 to all client applications that require 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 of AutoVu™ and Genetec Mission Control™, and requires a license for one of these products.

map object

Map objects are graphical representations of Security Center entities or geographical features, such as cities, highways, rivers, and so on, on your maps. 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

Maps is a type of 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 is the central role that handles all stream requests (audio and video) in Security Center. It establishes streaming sessions between the stream source (camera or 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).

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 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 a type of 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 a type of 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

Motion search is a type of investigation task that searches for motion detected in specific areas of a camera's field of view.

motion zone

A motion zone is a user defined areas within a video image where motion should be detected.

Move unit

Move unit tool is used to move units from one manager role to another. The move preserves all unit configurations and data. After the move, the new manager immediately takes on the command and control function of the unit, while the old manager continues to manage the unit data collected before the move.

multi-factor authentication

Multi-factor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

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 allows you 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.

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 a type of entity that defines a custom output signal format, such as a pulse with a delay and duration.

overtime rule

An overtime rule is a type of 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 Enforcement Essential

Parking Enforcement Essential is a Genetec Patroller™ software installation configuration that is similar to the City Parking Enforcement configuration, but excludes features such as shared permits, zone auto-selection, Plate link, and wheel imaging. You can configure the system for either overtime enforcement or permit enforcement, but you cannot configure both enforcement types.

parking facility

A parking facility is a type of entity that 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 a type of investigation task that allows you 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 a type of investigation task that allows you 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 a type of entity 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.

partition administrator

(Obsolete) Beginning in Security Center 5.7 GA, privileges that used to be exclusive to administrators can now be granted individually, making the concept of *partition administrator* obsolete.

passive authentication

Passive authentication (also known as web-based 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.

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

1. Genetec Patroller™ is the AutoVu™ software application installed on an in-vehicle computer. Genetec Patroller™ connects to Security Center and is controlled by the LPR Manager. Genetec Patroller™ verifies license plates read from LPR cameras against lists of vehicles of interest (hotlists) and vehicles with permits (permit lists). It also collects data for time-limited parking enforcement. Genetec Patroller™ alerts you of hotlist or permit hits so that you can take immediate action.
2. Type of entity that 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

Patroller tracking is a type of investigation task that allows you 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

People counting is a type of 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 a type of 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 a type of 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

Plan Manager is a module of Security Center that provides interactive mapping functionality to better visualize your security environment.

Plate Reader

Plate Reader is the software component of the Sharp unit that processes the images captured by the LPR 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 LPR 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 allows you to configure plugin-specific roles and related entities.

primary server

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 some 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 made known and available to 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 both 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

Reads is a type of investigation task that reports on license plate reads performed within a selected time range and geographic area.

Reads/hits per day

Reads/hits per day is a type of investigation task that reports on license plate reads performed within a selected time range and geographic area.

Reads/hits per zone

Reads/hits per zone is a type of 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.

recording mode

Recording mode is the criteria by which the Archiver schedules the recording of video streams. There are four possible recording modes:

- Off (no recording allowed)
- Manual (record only on user requests)
- Continuous (always record)
- On motion/manual (record according to motion detection settings or on user request)

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)*.

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 that allows a copy of all the video streams of an Archiver role to be archived simultaneously on the standby server as a protection against data loss.

Remote
Remote is a type of operation task that allows you to remotely monitor and control other Security Desks that are part of your system, using the Monitoring task and the Alarm monitoring task.

Remote configuration
The *Remote configuration* task is an administration task that allows you 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
Report Manager is a type of role that automates report emailing and printing based on schedules.

report pane
Report pane is one of the panes found in the Security Desk task 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 an AutoVu™ feature that translates a pair of latitude and longitude into a readable street address.

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
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 Same position 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 in order to enforce this type of regulation.

schedule A schedule is a type of 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 a type of 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 allows an SDK application (or plugin) 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, 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. That way, the remote system's entities and events can be used in your local system.

Security Center Mobile (Deprecated) Security Center Mobile is the feature that you can use to remotely connect to your Security Center system over a wireless IP network using a smartphone.

Security Center Mobile application (Deprecated) 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 Center Web (Deprecated) Security Center Web is the feature that lets you remotely connect to your Security Center system using a web browser.

Security Center Web Client (Deprecated) See Web Client.

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 token service Security token service (STS) is a claims provider implemented as a web service that issues security tokens. Active Directory Federation Services (ADFS) is an example of a security token service. Also known as an issuer.

self-signed certificate A self-signed certificate is an identity certificate that is signed by the same entity whose identity it certifies.

server A server is a type of entity that represents a server machine on which the Genetec™ Server service is installed.

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 allows you to configure the settings of Genetec Server. Server Admin also allows you 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

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 EX

Sharp EX is the Sharp unit that includes an integrated image processor and supports two standard definition NTSC or PAL inputs for external cameras (LPR and context cameras).

Sharp Portal

Sharp Portal is a web-based administration tool used to configure Sharp cameras for fixed or mobile 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 LPR context (e.g. Alabama, Oregon, Quebec, etc), selecting the read strategy (e.g. fast moving or slow moving vehicles), viewing the Sharp's live video feed, and more.

Sharp unit

The Sharp unit is a proprietary LPR unit of Genetec Inc. that integrates license plate capturing and processing components, as well as digital video processing functions, inside a ruggedized casing.

Sharp VGA

Sharp VGA is a Sharp unit that integrates the following components: an infrared illuminator; a standard definition (640 x 480) LPR camera for plate capture; an integrated image processor; an NTSC or PAL color context camera with video streaming capabilities.

Sharp XGA

Sharp XGA is a Sharp unit that integrates the following components: an infrared illuminator; a high-definition (1024 x 768) LPR camera for plate capture; an integrated image processor; an NTSC or PAL color context camera with video streaming capabilities and optional internal GPS.

SharpOS

SharpOS is the software component of a Sharp or SharpX unit. SharpOS is responsible for everything related to plate capture, collection, processing, and analytics. For example, a SharpOS update can include new LPR 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 LPR camera (1024 x 946 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The LPR data captured by the SharpX camera unit is processed by a separate hardware component called the AutoVu™ LPR Processing Unit.

SharpX VGA

SharpX VGA is the camera component of the SharpX system. The SharpX VGA camera unit integrates a pulsed LED illuminator that works in total darkness (0 lux), a monochrome LPR camera (640 x 480 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The LPR data captured by the SharpX VGA camera unit is processed by a separate hardware component called the AutoVu™ LPR 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) allows end-users to develop custom applications or custom application extensions for Security Center.

standalone mode

Standalone mode is an offline operation mode of the interface module where it operates autonomously, making decisions based on the access control settings previously downloaded from the Synergis™ unit. 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 type of schedule entity that may be used in all situations. Its only limitation is that it does not support daytime or nighttime coverage.

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

An SV appliance is a turnkey appliance that comes with an embedded operating system and Security Center pre-installed. You can use SV appliances to quickly deploy a unified or standalone video surveillance and access control system.

SV-16

The SV-16 is a subcompact all-in-one appliance that comes with Microsoft Windows, Security Center, and the SV Control Panel pre-installed. The SV-16 is for small-scale, single server installations, and can support both cameras and access control readers.

SV-32

The SV-32 is a compact all-in-one appliance that comes with Microsoft Windows, Security Center, and the SV Control Panel pre-installed. With built-in analog encoder capture cards, the SV-32 is a turnkey appliance that enables you to quickly deploy a standalone system (video surveillance or access control) or unified system (video surveillance and access control).

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.

SV-PRO

The SV-PRO is a rackmount appliance that comes with Microsoft Windows, Security Center, and the SV Control Panel pre-installed. The SV-PRO is for small to mid-scale, single or multiple server installations, and can support both cameras and access control readers.

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. Supporting an ever-growing portfolio of third-party door control hardware and electronic locks, it allows you to 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 preinstalled with Synergis™ Softwire and can be 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, as well as 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™ IX

Synergis™ IX (pronounced "eye-ex") is a family of hybrid controllers and interface 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 a variety of third-party interface modules over IP and RS-485. SMC is seamlessly integrated with Security Center and is capable of making access control decisions independently of the Access Manager.

Synergis™ Softwire

Synergis™ Softwire is the access control software developed by Genetec Inc. to run on a variety of IP-ready security appliances. Synergis™ Softwire lets these appliances communicate with third-party interface modules. A security appliance running Synergis™ Softwire can be 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

System Availability Monitor (SAM) enables you to collect health information and view the health status of your Security Center systems so that you can 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 allows you 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

System status is a type of maintenance task that monitors the status of all entities of a given type in real time, and allows you to interact with them.

tailgating

Tailgating designates one of the following: *tailgating (access control)* or *tailgating (analytics)*.

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 appear 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.

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

Time and attendance is a type of 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 type of 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
- LPR units, managed by the LPR Manager role
- Intrusion detection units, managed by the Intrusion Manager role

Unit discovery tool

Starting with Security Center 5.4 GA the Unit discovery tool has been replaced by the Unit enrollment tool.

Unit enrollment tool

The Unit enrollment tool allows you 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). Once discovered, the units can be added to your system.

Unit replacement

Unit replacement is a tool that is used 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

A unreconciled read is a MLPI license plate read that has not been committed to an inventory.

user

A user is a type of 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 a type of 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 allows you 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

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 Video file explorer is a type of investigation task that browses through your file system for video files (G64 and G64x) and allows you 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 allows you to configure video management roles, units, analog monitors, and cameras.

video unit A video unit is a type of video encoding or decoding device that is capable of communicating over an IP network and can incorporate one or more video encoders. The high-end encoding models also include their own recording and video analytic capabilities. Cameras (IP or analog), video encoders, and video decoders are all examples of video units. In Security Center, a video unit refers to a type of entity that represents a video encoding or decoding device.

video watermarking Video watermarking adds a digital signature (watermark) to each recorded video frame to ensure its authenticity. If the video is later changed by adding, deleting or modifying a frame, the signatures for the modified content will no longer match, showing that the video has been tampered with.

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 Visit details is a type of investigation task that reports on the stay (check-in and check-out time) of current and past visitors.

Visitor activities

Visitor activities is a type of 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

Visitor management is a type of operation task that allows you 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 Desk feature that allows you to follow an individual across different areas of your company without ever losing sight of that individual, as long as the places this person goes through are monitored by cameras. This feature displays transparent overlays on the video to show you where you can click to switch to adjacent 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

Watchdog is a Security Center service installed alongside the Genetec Server service on every server computer. The watchdog monitors the Genetec Server service, and restarts it if abnormal conditions are detected.

Wearable Camera Manager

Wearable Camera Manager is the role that is used to configure and manage body-worn camera (BWC) devices in Security Center. This includes configuring cameras or camera stations, adding users, uploading content to an Archiver, and setting the retention period for uploaded evidence.

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

The 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 for the purpose of granting 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 across multiple machines connected by a network, to communicate. Genetec Patroller™ uses WCF to communicate wirelessly with Security Center.

X.509 certificate

Identity verification, asymmetric cryptography and the security of data in transit are all enabled by X.509 certificates, which are made up of a user or computer’s identity and public key. X.509 certificates are the basis for the HTTPS protocol.

zone

A zone is a type of 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

Zone activities is a type of investigation task that reports on zone related activities (zone armed, zone disarmed, lock released, lock secured, and so on).

Zone Manager

Zone Manager is a type of role that 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

Zone occupancy is a type of 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 explain 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://gtap.genetec.com.
- 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://gtap.genetec.com to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.