Security Center Installation and Upgrade
Guide
5.5 SR3

Click here for the most recent version of this document.
Copyright notice

© Genetec Inc., 2016

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

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

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

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

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein. The use of this document is subject to the disclaimer of liability found in the end-user license agreement.

Genetec, Omnicast, Synergis, AutoVu, Federation, Stratocast, Sipelia, Citywise, the Genetec Logo, the Mobius Strip Logo, the Omnicast Logo, the Synergis Logo, the AutoVu Logo, and the Stratocast Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

All specifications are subject to change without notice.

Document information

Document title: Security Center Installation and Upgrade Guide 5.5 SR3
Document number: EN.500.002-V5.5.C3(1)
Document update date: September 27, 2016
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:** Topics appearing in this guide that reference information found on third-party websites were accurate at the time of publication, however, this information is subject to change without prior notice to Genetec.
## Preface: Preface

<table>
<thead>
<tr>
<th>Copyright notice</th>
<th>ii</th>
</tr>
</thead>
<tbody>
<tr>
<td>About this guide</td>
<td>iii</td>
</tr>
</tbody>
</table>

## Chapter 1: Installing Security Center

<table>
<thead>
<tr>
<th>Preparing to install Security Center</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activating .NET Framework 3.5.1</td>
<td>3</td>
</tr>
<tr>
<td>Activating the Media Foundation feature</td>
<td>3</td>
</tr>
<tr>
<td>Security Center 5.5 system requirements</td>
<td>4</td>
</tr>
<tr>
<td>Installing SQL Server on a separate drive</td>
<td>5</td>
</tr>
<tr>
<td>Granting SQL Server permissions</td>
<td>9</td>
</tr>
<tr>
<td>Security Center installation packages</td>
<td>10</td>
</tr>
<tr>
<td>Installing Security Center</td>
<td>11</td>
</tr>
<tr>
<td>Unblocking files manually</td>
<td>12</td>
</tr>
<tr>
<td>Installing Security Center on the main server</td>
<td>13</td>
</tr>
<tr>
<td>Activating Security Center license using the web</td>
<td>22</td>
</tr>
<tr>
<td>Activating Security Center license without Internet access</td>
<td>26</td>
</tr>
<tr>
<td>Installing Security Center on an expansion server</td>
<td>32</td>
</tr>
<tr>
<td>Connecting expansion servers to the main server</td>
<td>39</td>
</tr>
<tr>
<td>Installing Security Center Client</td>
<td>42</td>
</tr>
<tr>
<td>Default ports used by Security Center</td>
<td>45</td>
</tr>
<tr>
<td>Common communication ports</td>
<td>45</td>
</tr>
<tr>
<td>Omnicast-specific ports</td>
<td>46</td>
</tr>
<tr>
<td>Synergis-specific ports</td>
<td>47</td>
</tr>
<tr>
<td>AutoVu-specific ports</td>
<td>48</td>
</tr>
<tr>
<td>Installing BeNomad</td>
<td>49</td>
</tr>
<tr>
<td>Disabling backward compatibility</td>
<td>50</td>
</tr>
<tr>
<td>Uninstalling Security Center</td>
<td>51</td>
</tr>
<tr>
<td>Completing the installation process</td>
<td>53</td>
</tr>
</tbody>
</table>

## Chapter 2: Upgrading to Security Center 5.5

| Supported upgrades from earlier versions of Security Center | 56 |
| Preparing to upgrade from an earlier release of Security Center 5.5 | 57 |
| Preparing to upgrade from Security Center 5.4 to 5.5 | 58 |
| Preparing to upgrade from Security Center 5.3 to 5.5 | 59 |
| Preparing to upgrade from Security Center 5.2 to 5.5 | 60 |
| Differences between Server Admin 5.x and 5.5 | 61 |
| Differences between Security Center 5.x and 5.5 partitions | 63 |
| Upgrading the Public partition from 5.x to 5.5 | 66 |
Installing Security Center

This section includes the following topics:

- "Preparing to install Security Center" on page 2
- "Security Center 5.5 system requirements" on page 4
- "Installing SQL Server on a separate drive" on page 5
- "Granting SQL Server permissions" on page 9
- "Security Center installation packages" on page 10
- "Installing Security Center" on page 11
- "Unblocking files manually" on page 12
- "Installing Security Center on the main server" on page 13
- "Activating Security Center license using the web" on page 22
- "Activating Security Center license without Internet access" on page 26
- "Installing Security Center on an expansion server" on page 32
- "Installing Security Center Client" on page 42
- "Default ports used by Security Center" on page 45
- "Installing BeNomad" on page 49
- "Disabling backward compatibility" on page 50
- "Uninstalling Security Center" on page 51
- "Completing the installation process" on page 53
Preparing to install Security Center

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

**Before installing Security Center:**

1. Read the Security Center Release Notes for any known issues, supported upgrade paths, and other information about the release. Click here for the most recent version of this document.
2. Review your system requirements to ensure that the minimum hardware requirements (servers and workstations) and software requirements (Windows, web browser, and so on) are met.
3. Install the latest video and network drivers for your servers and workstations.
4. Make sure that the servers are not domain controllers.
5. Disable the power saving feature on all servers.
6. Make sure that Windows Update is not configured to automatically reboot your servers after installation of updates.
7. On each server, in the Adapters and Bindings settings where connections are listed in the order in which they are accessed by network services, make sure that the network interface cards (NICs) to be used by Security Center are located at the top of the list.
8. Verify the network connections between your servers, workstations, and units.
9. Verify the unicast and multicast network connections and settings.
10. Read the Security Center Client and Server installation prerequisites available on GTAP. 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. If you are upgrading:
   a) Check the Security Center backward compatibility requirements.
   b) Make sure the upgrade or migration path is supported. For more information, see the Security Center Release Notes.
   c) Back up your Directory and role-specific databases. For more information, see the Security Center Administrator Guide for the current version of your system.
12. 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 Technical Support sends you this document when you purchase the product.
13. 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.
14. (For Directory failover or VSS operation) Install SQL Server on a separate drive.
15. Grant the service users all necessary SQL server permissions.
17. (Windows 7 only) Activate .NET Framework 3.5.1.
   For Windows 8 and Windows 2012, the .NET Framework feature is automatically enabled by the InstallShield Wizard if you have an active Internet connection.
18 (Windows 2012 only) **Activate the Media Foundation feature.**
19 Download the Security Center installation package.
20 **Unblock any blocked files.**

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

**After you finish**
Install Security Center.

**Activating .NET Framework 3.5.1**

If you want to install Security Center on a computer running Windows 7, you have to manually activate .NET Framework 3.5.1.

**What you should know**

For Windows 8 and Window 2012, the .NET Framework feature is automatically enabled by the InstallShield Wizard if you have an active Internet connection.

**To activate .NET Framework 3.5.1.**
1 Click **Start > Control Panel > Programs and Features.**
2 In the **Programs and Features** dialog box, click **Turn Windows features on or off.**
3 In the **Windows Features** dialog box, select the **Microsoft .NET Framework 3.5.1** option, and click **OK.**

**Activating the Media Foundation feature**

If you want to install Security Center on a computer running Windows 2012, you have to manually activate the Media Foundation feature.

**To activate the Media Foundation feature:**
1 Open **Server Manager** and click **Add roles and features.**
2 If the **Before you begin** page is displayed, click **Next.**
3 Select **Role-based or feature-based installation** as the installation type and click **Next.**
4 Select the appropriate server, and click **Next.**
5 On the **Select server roles** page, click **Next.**
6 On the **Select features** page, select **Media Foundation** and click **Next > Install.**
7 Select the option **Restart the destination server automatically if required** for the server to automatically restart and apply changes after completing the installation.
Security Center 5.5 system requirements

System requirements are the recommended hardware and software components that are required for your product and system to run optimally.

For the latest Security Center 5.5 system requirements, click here.
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:
     1. In Windows, navigate to the SQL installation package folder.
     2. Double-click `Setup.exe`.
   - If you are installing SQL Server Express:
     1. In Windows, navigate to the Security Center installation package folder.
     2. Click `SC Packages` > `SQLExpress`.
     3. Double-click one of the following:
        - If you are on a 64-bit computer: `SQLEXRWTT_x64_ENU.exe`.
        - If you are on a 32-bit computer: `SQLEXRWTT_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**.
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. For a complete list of all reserved keywords, see https://msdn.microsoft.com/en-us/library/ms189822.aspx.
- 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 (_).
- Embedded spaces or other special characters are not allowed: backslash (\), comma (,), colon (:), semi-colon (;), single quotation mark (‘), ampersand (&), number sign (#), and at sign (@).

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

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
Granting SQL Server permissions

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

What you should know

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

For more information about 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:
    1. Right-click on the appropriate SQL server instance and select Properties.
    2. Click the Permissions page.
    3. Under Logins or roles, select the user or role you want to modify.
    4. In the Permissions section, click the Explicit tab and select the Grant check box beside the View server state permission.
    5. Click OK.

After you finish

For users that are granted the permission locally on the Genetec 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 website 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, 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. For more information, see Silent installation in Security Center on page 99.

  **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.
Installing Security Center

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

**Before you begin**

- Read the *Security Center Release Notes* for any known issues and other information about the release.
  
  Click [here](#) for the most recent version of this document.
- 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 (dedicated database server)

  View your [system requirements](#) to ensure that the minimum hardware requirements (servers and workstations) and software requirements (Windows, web browser, and so on) are met.
- 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 Security Center downloaded package. Using the *Change* option from *Programs and Features* will not install the SQL Express component you need.
- The Security Center Installer does not support using mapped drives in your path specifications.

**To install Security Center:**

1. **(Optional) Install SQL Server on a separate drive from the OS drive.**
   
   SQL Server 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.**
   
   For a list of default ports used by Security Center, see [Default ports used by Security Center](#) on page 45.
5. **(Optional) Install Security Center components on any expansion servers** that will connect to the main server to add processing power to your Security Center system.
6. **Install Security Center Client** (Config Tool, Security Desk, or both).
7. **Unblock any blocked files.**

**After you finish**

Go through the post-installation list.
Unblocking files manually

After downloading a Security Center installation package, you might have to unblock some of the files.

What you should know

• Not all versions of Windows Server require ZIP files to be unblocked before their contents can be extracted. The Unblock button described in the following steps might not be present.

• 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.

To unblock files from the Security Center installation package:

1. Right-click the ZIP file in Windows Explorer and choose Properties.
2. In the General tab, click Unblock.
3. Click OK.

Related Topics
Troubleshooting: Files remain blocked after unblocking them manually on page 114
Installing Security Center on the main server

The main server is the only server in your Security Center system that hosts the Directory role. You must install the main server first so that other servers can connect to it. You must also activate your Security Center license on the main server.

**Before you begin**

Prepare to install Security Center.

**IMPORTANT:** If you are not logged on to Windows as administrator, you must right-click the setup executable file and click **Run as administrator**.

**What you should know**

The main server installation procedure installs the following:

- The Genetec Server service *with* the Directory role.
  
  When installing Genetec Server, the Directory database server (optionally SQL Server Express 2014), the Server Admin, and the Watchdog are also installed. This installed software takes care of the creation or the upgrade of all the databases your system requires. You must only specify the name of your database server. If you do not have one, Microsoft SQL Server 2014 Express Edition is installed by default.

- (Optional) Client applications (Config Tool, Security Desk, or both).

- (Optional) Omnicast compatibility packs to view video from federated Omnicast systems.

**To install Security Center on the main server:**

1. Double-click either `setup.exe` (standalone version) or `SecurityCenterWebSetup.exe` (web version) to launch the Security Center Installer.

   **NOTE:** Only the standalone InstallShield Wizard is illustrated in this procedure.

2. On the **Setup Language** selection page, select either English or French, and click **Next**.

   The **Welcome to the InstallShield Wizard** screen appears.
3 On the Welcome page, click **Next**.

Links are provided to view relevant Security Center documentation online, or in PDF format.

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

5 On the Custom Setup page, select the Security Center applications you want to install.

You can choose from the following:

- **Server**: Installs the Genetec Server service, the SQL Server databases, the Server Admin, and the Watchdog service.

- **(Optional) Client**: Installs the Security Center Client applications: You can choose either Config Tool, Security Desk, or both.
- **(Optional) Omnicast Compatibility Packs:** If Omnicast systems will be federated, select the required Omnicast compatibility packs.

6 To change the installation folder, click **Change** to change the installation folder, and click **Next**.

7 On the **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 the installation, you can change the user interface language any time using the *Language Tool* found in the Tools subfolder of the Genetec Security Center program group.

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

   **IMPORTANT:** You must not use the **Main server** installation type more than once per system. If your Security Center license supports additional Directory servers, all Directory servers that are not your main server must be installed as expansion servers. For more information, see the *Security Center Administrator Guide*.

9 On the **System Availability Monitor** page, select one of the following options:
• **Collect data anonymously:** (Default) No activation code is required. Health data is sent to a dedicated Health Monitoring Service where the entity names are disguised and cannot be traced. This data is used only by Genetec for statistics and cannot be accessed through GTAP.

• **Collect data and associate it to my system:** Your system must be covered by Genetec™ Advantage, and an activation code is required. For more information about generating an activation code, see the *System Availability Monitor User Guide*.

• **Do not collect data:** The System Availability Monitor Agent is installed but does not collect any data.

  a) (Optional) Click **View confidentiality agreement** to view the privacy statement that explains what information is transmitted to Genetec and how it is used.

  b) (Optional) Click **Print** to print a copy of the Confidentiality Agreement.

  c) Click **OK**.

10 On the *Database Server* page, select one of the following options:
• **Use an existing database server:** Select an existing Microsoft SQL Server instance to install the database on.
  
  As a best practice, replace (local) with your machine name. Stating explicitly your machine name is necessary if you are configuring the Directory for load balancing.

• **Install a new database server:** Installs Microsoft SQL Server 2014 Express Edition. 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. For a complete list of all reserved keywords, see https://msdn.microsoft.com/en-us/library/ms189822.aspx.
  - 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 (_).
  - Embedded spaces or other special characters are not allowed: backslash (\), comma (,), colon (:), semi-colon (;), single quotation mark (’), ampersand (&), number sign (#), and at sign (@).

11 Click **Next**.

12 On the **Service Logon Parameters** page, select one of the following options:
• **Use default name and password:** Use the default username (Local System) to run the Security Center services. This option works in most cases.

• **Specify the username and password for all services:** Enter a valid domain username and password.

  **IMPORTANT:** Be sure that the service user is a member of the Administrators group, has the rights to the local or remote database, and has *Log on as service* user rights. If this server is to host the Active Directory role, the specified user must have Read and Write access to the Active Directory you want the server to connect to.

13 Click **Next**.

14 On the **Server Parameters** page, enter the following fields:
• **Web server port**: The HTTP port that is used for the web-based Server Admin. If you change the default port, then 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**: Be aware of conflicts with other software running on the server that may also use port 80 (for example any other web browser).

• **Server port**: The TCP port through which the servers in your system communicate.

• **Server password/Confirm password**: Enter and confirm the password (minimum 8 characters) 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.

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

15 Click **Next**.

16 On the **Firewall Rules** page, select **Allow Genetec Security Center 5.5 to create necessary firewall rules for its applications**, and click **Next**.

  This option ensures that the internal Windows Firewall security rules are configured correctly.

  **NOTE**: You must also configure the Security Center ports on your corporate Firewall after the installation.

17 On the **WinPcap Installation** page, select the **Install WinPcap** option and click **Next**.

  This dialog box does not appear if WinPcap 4.1.3 is already installed. This option allows you to capture diagnostic data for units and other services in Security Center. This data is used by the Genetec™ Technical support team if you require assistance. If the WinPcap installation does not start immediately you will be prompted to install it at a later time.

18 On the **Security Settings** page, configure the following options:
• **Turn on Directory authentication:** 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 (default=off).

**BEST PRACTICE:** If you choose to enable Directory authentication, it is best to use a certificate issued by a trusted certificate authority (CA). Otherwise, the first time a connection is made from this computer 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 camera authentication 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 authentication cannot be used in Security Center.

**NOTE:** If necessary, you can configure this option individually for each camera manufacturer extension in Config Tool from the Archiver’s Extensions tab.

19 Select **I acknowledge that I have read and understood the implications of selecting these security settings**, and click **Install**.

The Genetec Security Center 5.4 Installer opens and starts the installation.

20 If you chose to install WinPcap 4.1.3 the WinPcap 4.1.3 Setup Wizard opens:

a) In the WinPcap 4.1.3 Setup Wizard, follow the installation instructions.

b) On the Installation options page, select the **Automatically start the WinPcap driver at boot time** option, and click **Install**.

c) Click **Finish**, and continue with the Security Center installation.

21 (Optional) When the Installation Completed page opens, click **View Installation logs** to open the folder that contains the Installation logs that can be viewed in Notepad.

22 Click **Finish**.
If you selected the **Launch Server Admin** option at the end of the installation, the Server Admin browser window appears.

If you selected the **Connect me to GTAP for the latest updates now** option, your Internet browser opens to the Genetec Product Download page on GTAP. You need a login and a password to connect to GTAP.

Security Center is now installed on the main server.

**After you finish**

Do the following:

- Activate your product license from the Server Admin.
- Install Security Center on the expansion servers.

**Related Topics**

- [Activating Security Center license using the web](#) on page 22
- [Activating Security Center license without Internet access](#) on page 26
- [Installing Security Center on an expansion server](#) on page 32
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 26.
- **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 DNS name or the IP address of your 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 server password that you set during the server installation, and click **Log on**.
The Server Admin Overview page appears.

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.

5  Click Activate.

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

6  Click Details to view your license options in a dialog box.
Your license options are divided into six 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 DNS name or the IP address of your 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 server password that you set during the server installation, and click **Log on**.
The Server Admin Overview page appears.

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.

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, log on to GTAP at: https://gtap.genetec.com

6 On the GTAP 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.

   1 On the Genetec Portal - Home page, click Activate new system.
   2 From the System ID drop-down list, select your system, and click Submit.

   The browser opens to the System Information page.
7 Scroll down to the License information section and click Activate license.

8 In the dialog box that opens, browse to your validation key (.vk file), and click Submit. The message License activation successful appears.

9 Click Download License, and save the license key to a file. The default name is your System ID followed by _Directory_License.lic.

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

11 In the License management dialog box, do one of the following:
   - Paste your license information from the license key file (open with a text editor).
   - Browse for the license key (.lic file), and click Open.
12 Click **Activate**.

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

13 Click **Details** to view your license options in a dialog box.
Your license options are divided into six tabs. For more information, see the Security Center Administrator Guide.

14 Click Close, and then close your browser window.
Installing Security Center on an expansion server

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

**Before you begin**

- Prepare to install Security Center.
- Install Security Center on the main server, and make sure the server is up and running.

**What you should know**

The expansion server installation procedure installs the following:

- The Genetec Server service *without* the Directory role.
  - When installing Genetec Server, the Directory database server (optionally SQL Server Express 2014), the Server Admin, and the Watchdog server are also installed.
- (Optional) Client applications (Config Tool, Security Desk, or both).

**To install Security Center on an expansion server:**

1. Double-click either `setup.exe` (standalone version) or `SecurityCenterWebSetup.exe` (web version) to launch the Security Center Installer.
   
   **NOTE:** Only the standalone InstallShield Wizard is illustrated in this procedure.

2. On the Setup Language selection page, select either English or French, and click **Next**. The *Welcome to the InstallShield Wizard* screen appears.

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

   Links are provided to view relevant Security Center documentation online, or in PDF format.
4 On the License Agreement page, read the terms in the Genetec Software License Agreement, select I accept the terms in the license agreement, and then click Next.

5 On the Custom Setup page, select the Security Center applications you want to install.

You can choose from the following:

- **Server**: Installs the Genetec Server service, the SQL Server databases, the Server Admin, and the Watchdog service.
- **(Optional) Client**: Installs the Security Center Client applications: You can choose either Config Tool, Security Desk, or both.
- **(Optional) Omnicast Compatibility Packs**: If Omnicast systems will be federated, select the required Omnicast compatibility packs.

6 To change the installation folder, click Change to change the installation folder, and click Next.

7 On the 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 the installation, you can change the user interface language any time using the Language Tool found in the Tools subfolder of the Genetec Security Center program group.

8 On the Installation Type page, select Expansion server, and click Next.
9 On the **Database Server** page, select one of the following options:

- **Use an existing database server**: Select an existing Microsoft SQL Server instance to install the database on.
  
  As a best practice, replace (local) with your machine name. Stating explicitly your machine name is necessary if you are configuring the Directory for load balancing.

- **Install a new database server**: Installs Microsoft SQL Server 2014 Express Edition. 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. For a complete list of all reserved keywords, see https://msdn.microsoft.com/en-us/library/ms189822.aspx.

• 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 (_).

• Embedded spaces or other special characters are not allowed: backslash (\), comma (,), colon (:), semi-colon (;), single quotation mark (‘), ampersand (&), number sign (#), and at sign (@).

10 Click Next.

11 On the Service Logon Parameters page, select one of the following options:

- **Use default name and password:** Use the default username (Local System) to run the Security Center services. This option works in most cases.

- **Specify the username and password for all services:** Enter a valid domain username and password.

**IMPORTANT:** Be sure that the service user is a member of the Administrators group, has the rights to the local or remote database, and has Log on as service user rights. If this server is to host the Active Directory role, the specified user must have Read and Write access to the Active Directory you want the server to connect to.

12 Click Next.

13 On the Server Parameters page, enter the following fields:
• **Web server port**: The HTTP port that is used for the web-based Server Admin. If you change the default port, then 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**: Be aware of conflicts with other software running on the server that may also use port 80 (for example any other web browser).

• **Server port**: The TCP port through which the servers in your system communicate.

• **Server password/Confirm password**: Enter and confirm the password (minimum 8 characters) 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.

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

14 Click **Next**.

15 On the **Connection parameters to the main server** page, enter the following fields:
• **Main server name or IP address**: The DNS name or IP address of the main server.

  If you changed the port number (4502) on the main server, you must append the port number to the server name, separated by a colon (:`).

• **Main server password**: Enter the same password that was used to configure the main server.

16 On the **Firewall Rules** page, select *Allow Genetec Security Center 5.5 to create necessary firewall rules for its applications*, and click **Next**.

This option ensures that the internal Windows Firewall security rules are configured correctly.

**NOTE**: You must also configure the Security Center ports on your corporate Firewall after the installation.

17 On the **WinPcap Installation** page, select the **Install WinPcap** option and click **Next**.

This dialog box does not appear if WinPcap 4.1.3 is already installed. This option allows you to capture diagnostic data for units and other services in Security Center. This data is used by the Genetec™ Technical support team if you require assistance. If the WinPcap installation does not start immediately you will be prompted to install it at a later time.

18 On the **Security Settings** page, configure the following options:
• **Turn on Directory authentication:** 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 (default=off).

  **BEST PRACTICE:** If you choose to enable Directory authentication, it is best to use a certificate issued by a trusted certificate authority (CA). Otherwise, the first time a connection is made from this computer 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 camera authentication 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 authentication cannot be used in Security Center.

  **NOTE:** If necessary, you can configure this option individually for each camera manufacturer extension in Config Tool from the Archiver’s **Extensions** tab.

19 Select **I acknowledge that I have read and understood the implications of selecting these security settings**, and click **Install**.

The **Genetec Security Center 5.4 Installer** opens and starts the installation.

20 If you chose to install WinPcap 4.1.3 the **WinPcap 4.1.3 Setup Wizard** opens:

   a) In the **WinPcap 4.1.3 Setup Wizard**, follow the installation instructions.

   b) On the **Installation options** page, select the **Automatically start the WinPcap driver at boot time** option, and click **Install**.

   c) Click **Finish**, and continue with the Security Center installation.

21 (Optional) When the **Installation Completed** page opens, click **View Installation logs** to open the folder that contains the Installation logs that can be viewed in Notepad.
22 Click **Finish**.

If you selected the **Launch Server Admin** option at the end of the installation, the Server Admin browser window appears.

If you selected the **Connect me to GTAP for the latest updates now** option, your Internet browser opens to the Genetec Product Download page on GTAP. You need a login and a password to connect to GTAP.

Security Center is now installed on the expansion server.

**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 on your system to the new computer.

**Before you begin**

After completing an expansion server installation, the expansion server automatically connects to the main server. You must only go through the steps of connecting your expansion server to your main server 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 while the expansion server was down.
- 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 by doing one of the following:
   - In the address bar of your web browser, type `http://computer:port/Genetec`, where `computer` is the DNS name or the IP address of your 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 server password that you set during the server installation, and click **Log on**.

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’s DNS name 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 logging back on to Server Admin, if you get the message that the identity of the Directory cannot be verified, click **Main server connection**.

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

   ![Accept certificate dialog box](image)

   **IMPORTANT:** Once accepted, the 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 the burden of having to accept the certificate of your main server every time someone tries to connect to it from a new machine, only use certificates signed by a certification authority that is trusted by your company’s IT.

8. Click **Save**.

9. 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 will remain connected, even when you change the certificate, on either one or both of the servers, as long as the two servers are connected while the change is being made.
Installing Security Center Client

The Security Center Client installation option installs Config Tool and Security Desk by default.

To install Security Center Client:

1. Double-click either setup.exe (standalone version) or SecurityCenterWebSetup.exe (web version) to launch the Security Center Installer.

   **NOTE:** Only the standalone InstallShield Wizard is illustrated in this procedure.

2. On the Setup Language selection page, select either English or French, and click **Next**. The Welcome to the InstallShield Wizard screen appears.

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

   Links are provided to view relevant Security Center documentation online, or in PDF format.

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

5. On the Custom Setup page, select **Client**, and the client applications you want to install. You can choose from the following:

   - **Config Tool:** Allows you to configure all Security Center components.
   - **Security Desk:** Allows you to efficiently control and monitor multiple security and public safety applications.
   - **Omnicast Compatibility Packs:** If Omnicast systems will be federated, select the required Omnicast compatibility packs.
6 To change the installation folder, click **Change** to change the installation folder, and click **Next**.

7 On the **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 the installation, you can change the user interface language any time using the **Language Tool** found in the Tools subfolder of the Genetec Security Center program group.

8 On the **Firewall Rules** page, select **Allow Genetec Security Center 5.5 to create necessary firewall rules for its applications**, and click **Next**.

   This option ensures that the internal Windows Firewall security rules are configured correctly.

   **NOTE:** You must also configure the Security Center ports on your corporate Firewall after the installation.

9 On the **Security Settings** page, configure the following options:
• **Turn on Directory authentication:** 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 (default=off).

  **BEST PRACTICE:** If you choose to enable Directory authentication, it is best to use a certificate issued by a trusted certificate authority (CA). Otherwise, the first time a connection is made from this computer 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 camera authentication 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 authentication cannot be used in Security Center.

  **NOTE:** If necessary, you can configure this option individually for each camera manufacturer extension in Config Tool from the Archiver’s *Extensions* tab.

10 Select **I acknowledge that I have read and understood the implications of selecting these security settings**, and click **Install**.

  The *Genetec Security Center 5.4 Installer* opens and starts the installation.

11 Click **Finish**.

**After you finish**

Do the following:

• Configure the Security Center ports on your corporate firewall.
Default ports used by Security Center

After installing Security Center, you must ensure that all the correct ports are open and redirected for firewall and network address translation purposes, so all the Security Center components can communicate properly.

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 make sure that all the ports used by Security Center are open.

You can configure different port numbers than the ones that are used by default.

### Common communication ports

The following table lists the default network ports used by Security Center applications:

<table>
<thead>
<tr>
<th>Computer</th>
<th>Inbound</th>
<th>Outbound</th>
<th>Port usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main server</td>
<td>TCP 5500</td>
<td>TCP 5500</td>
<td>Directory connection requests</td>
</tr>
<tr>
<td>Client workstations (Security Desk and Config Tool)</td>
<td>TCP 5500</td>
<td>TCP 5500</td>
<td>Directory connection requests</td>
</tr>
<tr>
<td>Client workstations (Config Tool)</td>
<td>TCP 443</td>
<td>TCP 443</td>
<td>Communication with GTAP for SMA validation/sending feedback</td>
</tr>
<tr>
<td>Servers (new installation)</td>
<td>TCP 5500</td>
<td>TCP 5500</td>
<td>Communication with other servers</td>
</tr>
<tr>
<td></td>
<td>TCP 4502</td>
<td>TCP 4502</td>
<td>Backward compatibility. For connections from servers running Security Center 5.3 and earlier.</td>
</tr>
<tr>
<td></td>
<td>HTTP 80</td>
<td>TCP 8012</td>
<td>Connection through Server Admin</td>
</tr>
<tr>
<td>Servers (upgraded from 5.3 an earlier)</td>
<td>TCP 4502</td>
<td>TCP 4502</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>TCP 4503</td>
<td>TCP 4503</td>
<td>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.</td>
</tr>
<tr>
<td>Map Manager</td>
<td>HTTP 8012</td>
<td></td>
<td>Communication with client applications for map downloads.</td>
</tr>
</tbody>
</table>
### Computer Port Usage

<table>
<thead>
<tr>
<th>Computer</th>
<th>Inbound Port</th>
<th>Outbound Port</th>
<th>Port Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Availability Monitor Agent (SAMA)</td>
<td>TCP 4592</td>
<td>TCP 443</td>
<td>Connection from Security Center servers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TCP 443</td>
</tr>
<tr>
<td>Genetec Update Service (GUS)</td>
<td>TCP 4595</td>
<td>TCP 4595</td>
<td>Connection from Security Center applications and communication with other GUS servers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP 443</td>
<td>Connection to the Internet.</td>
</tr>
</tbody>
</table>

### Omnicast-specific ports

The following table lists the default network ports used by Omnicast applications in Security Center.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Inbound Port</th>
<th>Outbound Port</th>
<th>Port Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archiver</td>
<td>TCP 555</td>
<td></td>
<td>Live and playback stream requests</td>
</tr>
<tr>
<td></td>
<td>UDP 15000–20000</td>
<td>UDP 15000–20000</td>
<td>Live unicast audio and video streams</td>
</tr>
<tr>
<td></td>
<td>TCP &amp; UDP</td>
<td></td>
<td>Vendor specific ports for events and unit discovery</td>
</tr>
<tr>
<td></td>
<td>UDP 47806</td>
<td>UDP 47806</td>
<td>Live multicast audio and video streams</td>
</tr>
<tr>
<td></td>
<td>UDP 47807</td>
<td>UDP 47807</td>
<td>Live multicast audio and video streams</td>
</tr>
<tr>
<td></td>
<td>TCP 554 or HTTP 80</td>
<td></td>
<td>Typical port used to request video from a unit</td>
</tr>
<tr>
<td>Telnet</td>
<td>5602</td>
<td></td>
<td>Telnet Console connection requests</td>
</tr>
<tr>
<td>Auxiliary Archiver</td>
<td>TCP 558</td>
<td></td>
<td>Playback stream requests</td>
</tr>
<tr>
<td>Media Router</td>
<td>TCP 554</td>
<td></td>
<td>Live and playback stream requests</td>
</tr>
<tr>
<td>Redirector</td>
<td>TCP 560</td>
<td></td>
<td>Live and playback stream requests</td>
</tr>
<tr>
<td></td>
<td>UDP 8000–12000</td>
<td></td>
<td>Live unicast audio and video streams</td>
</tr>
<tr>
<td></td>
<td>UDP 47806</td>
<td>UDP 47806</td>
<td>Live multicast audio and video streams</td>
</tr>
<tr>
<td></td>
<td>TCP 555</td>
<td></td>
<td>Communication with Archiver</td>
</tr>
</tbody>
</table>
### Computer

<table>
<thead>
<tr>
<th>Computer</th>
<th>Inbound</th>
<th>Outbound</th>
<th>Port usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTSP Media Router</td>
<td>TCP 654</td>
<td></td>
<td>Live and playback stream requests</td>
</tr>
<tr>
<td></td>
<td>UDP 51914</td>
<td>UDP 51914</td>
<td>Live multicast audio and video streams</td>
</tr>
<tr>
<td>Omnicast Federation</td>
<td>UDP 1024-2048</td>
<td></td>
<td>Security Desk when viewing video from an Omnicast Federation in Security Center</td>
</tr>
<tr>
<td>Client workstations</td>
<td>UDP 6000–6500</td>
<td></td>
<td>Live unicast audio and video streams</td>
</tr>
<tr>
<td>(Security Desk and Config Tool)</td>
<td>UDP 47806</td>
<td></td>
<td>Live multicast video streams</td>
</tr>
<tr>
<td></td>
<td>UDP 47807</td>
<td></td>
<td>Live multicast audio streams</td>
</tr>
<tr>
<td></td>
<td>TCP 554–560</td>
<td></td>
<td>Live and playback audio and video requests</td>
</tr>
</tbody>
</table>

1 You can have multiple Archiver agents per server. Each Archiver agent assigns a unique UDP port to each video unit it controls. In order to make sure that each UDP port on a server is unique, each new Archiver agent on a server adds 5000 to its start UDP port number. For example, the first Archiver agent uses ports 15000-20000, the second one uses ports 20000-25000, the third one uses ports 25000-30000, and so on.

### Synergis-specific ports

The following table lists the default network ports used by Synergis applications in Security Center.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Inbound</th>
<th>Outbound</th>
<th>Port usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Manager</td>
<td>UDP/TCP 4070</td>
<td>UDP/TCP 4070</td>
<td>HID VertX/Edge controllers</td>
</tr>
<tr>
<td></td>
<td>TCP 20</td>
<td>TCP 21, 23</td>
<td>HID VertX/Edge controllers</td>
</tr>
<tr>
<td></td>
<td>TCP 4050</td>
<td></td>
<td>HID VertX/Edge controllers</td>
</tr>
<tr>
<td></td>
<td>TCP 22</td>
<td></td>
<td>HID VertX/Edge EVO controllers</td>
</tr>
<tr>
<td></td>
<td>TCP 2000</td>
<td></td>
<td>Default Synergis unit discovery port (this port can be modified in Config Tool)</td>
</tr>
</tbody>
</table>

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](http://www.HIDglobal.com).
AutoVu-specific ports

The following table lists the default network ports used by AutoVu applications in Security Center.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Inbound</th>
<th>Outbound</th>
<th>Port usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>LPR Manager</td>
<td>UDP 5000</td>
<td>TCP 8731</td>
<td>Fixed Sharp unit discovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP 8832</td>
<td>Fixed Sharp units and Patrollers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP 8787</td>
<td>Patroller hotfix requests</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pay-by-Plate</td>
</tr>
</tbody>
</table>
Installing BeNomad

If your Security Center license supports mapping, you can use the default mapping solution *BeNomad* to provide map and reverse geocoding information.

**What you should know**

- When your license is created, you receive an email with a zip file containing the BeNomad maps for your geographic location, and a unique `.glic` file that contains your license information. You'll need both these files to install BeNomad.
- BeNomad must also be installed on any client machines running Security Desk.

**To install BeNomad:**

1. Unzip the contents of the BeNomad zip file to your computer. A folder called BeNomad is created.
2. Copy the BeNomad folder to the main program folder where Security Center is installed. In a default Security Center installation this folder is: `C:\Program Files (x86)\Genetec Security Center 5.5`.
3. Copy the `.glic` license file from the email to the BeNomad folder. *BeNomad* maps are enabled when you start Security Center.
Disabling backward compatibility

Older versions of Security Center (prior to 5.4) do not support the Transport Layer Security protocol. Therefore, supporting them makes your system more vulnerable to network attacks. To increase the security of your system, you can disable backward compatibility.

What you should know

Backward compatibility is enabled by default at system installation. This option applies to the entire system.

**CAUTION:** Mobile Server 4.0 does not support TLS. Disabling backward compatibility means that the Mobile apps and the Web Clients will no longer be able to connect to Security Center. All expansion servers that have not yet been upgraded to version 5.5 will also cease to work.

**To disable backward compatibility:**
1. Connect to Server Admin of your main server with a web browser.
2. Click the main server (throat) in the server list.
3. Under Secure communication, clear the **Allow connection of previous versions** option.
4. Click **Save**.

Backward compatibility is disabled. The next time someone tries to connect to your system with an older Security Center application, they will get the **Client-server versions are incompatible** error.
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 5.5 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. In Server Admin, backup the Directory database by clicking **Backup/Restore** under the Database section in the **Directory** tab.
2. Backup the database of each role configured in the system.
4. Click **Start > Control Panel > Programs and Features**.
5. In the **Programs and Features** window, right-click **Genetec Security Center 5.5 Installer**, and then click **Uninstall**.
6. In the **Remove the Program** dialog box, click **Remove**.
7. When the message **Uninstallation Completed** appears, click **Finish**.
   Genetec Security Center 5.5, the installer program, and all Omnicast Compatibility Packs, are removed.
8. (Optional) If you do not want to keep database information, including video archives, uninstall the SQL Server.
9. In the Windows **Start** menu, type **regedit**, and then press **ENTER**.
10. 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**
11. 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 5.5**
   - On 64-bit systems: **C:\Program Files (x86)\Genetec Security Center 5.5**
   - On all systems:
     - **C:\ProgramData\Genetec Security Center**
     - **C:\ProgramData\Genetec Security Center 5.5**
     - **C:\ProgramData\Genetec Update Service**
     - **C:\ProgramData\AppData\Local\Genetec Security Center 5.5**
     - **C:\Users\<username>\AppData\Local\Genetec Inc**
     - **C:\Users\<username>\AppData\Local\Genetec Security Center 5.5**
     - **C:\Users\<username>\AppData\Local\IsolatedStorage**
NOTE: You may not be able to delete this folder if other applications are using it.

12 (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 on the main server, and check the following in the **Directory** tab:
   - Directory is started.
   - Directory database is connected.
   - License is activated with all features confirmed.
   - SMA number is confirmed with expiration date.
   - Automatic backup of the Directory database is enabled and configured.

2. Click the **Genetec Server** tab, and check the following:
   - Authentication and Console passwords are set.
   - Network interface card (NIC) is properly selected.
   - Mail server is configured (if required).

3. Log on to Server Admin on each expansion server, and check the following:
   - Expansion server is connected to the main server.
   - NIC is properly selected.

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, that is, 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 check the following:
   - User groups and partitions are configured according to deployment requirements.
   - The *Admin* user has a password configured.
• Partitions in use are configured according to deployment requirements.

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.

After you finish

Depending on your deployment requirements, configure your system for:
   • Video surveillance/management
   • Access control
   • License Plate Recognition

For more information about deploying your system, see the Security Center Administrator Guide.
Upgrading to Security Center 5.5

This section includes the following topics:

- "Supported upgrades from earlier versions of Security Center" on page 56
- "Preparing to upgrade from an earlier release of Security Center 5.5" on page 57
- "Preparing to upgrade from Security Center 5.4 to 5.5" on page 58
- "Preparing to upgrade from Security Center 5.3 to 5.5" on page 59
- "Preparing to upgrade from Security Center 5.2 to 5.5" on page 60
- "Differences between Server Admin 5.x and 5.5" on page 61
- "Differences between Security Center 5.x and 5.5 partitions" on page 63
- "Upgrading the Public partition from 5.x to 5.5" on page 66
- "Backward compatibility requirements for Security Center" on page 67
- "Supported federations for Security Center 5.5 SR3" on page 71
- "Upgrading from an earlier release of Security Center 5.5" on page 72
- "Upgrading from Security Center 5.4 to 5.5" on page 73
- "Upgrading from Security Center 5.3 to 5.5" on page 74
- "Upgrading from Security Center 5.2 to 5.5" on page 75
- "Upgrading from Security Center 5.1 to 5.5" on page 76
- "Upgrading from Security Center 5.0 to 5.5" on page 77
- "Upgrading from Security Center 4.0 to 5.5" on page 78
- "Upgrading Failover Directory systems from a previous version or release" on page
- "Reactivating the Security Center license for Failover Directory systems" on page 82
- "Upgrading the Security Center main server" on page 88
- "Upgrading expansion servers in Security Center" on page 90
- "Upgrading Security Center Client" on page 91
- "Back up databases" on page 92
- "Upgrading the Security Center Directory database" on page 93
- "Shrinking Security Center databases after an upgrade" on page 95
- "About the Genetec Update Service" on page 96
- "Logging on to the Genetec Update Service" on page 97
Supported upgrades from earlier versions of Security Center

It is important to know which earlier versions of Security Center can be upgraded to Security Center 5.5 SR3.

A one-step upgrade is supported for the following Security Center releases:

- Security Center 5.3 GA/SR1/SR2/SR3/SR4
- Security Center 5.4 GA/SR2/SR3
- Security Center 5.5 GA/SR1/SR2

For Security Center 5.1 and earlier, a two-step upgrade is required.
Preparing to upgrade from an earlier release of Security Center 5.5

If you need to upgrade from an earlier release of Security Center 5.5 to the SR3 release, you must prepare the following.

**What you should know**

**To prepare to upgrade from an earlier release of Security Center 5.5 to release SR3:**

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

You'll have to re-enter the same values when you install Security Center Server 5.5 SR3.
Preparing to upgrade from Security Center 5.4 to 5.5

If you need to upgrade your 5.4 system to 5.5, you must prepare the following.

**What you should know**

- Different versions of Security Center Client can coexist on the same machine, but different versions of Security Center Server cannot. Not all current settings are retained 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 from Security Center 5.4 to 5.5:**

1. If you are running Windows Server 2008, Windows 7, or Windows Server 2008 R2, you must install Microsoft hotfix KB2588507.
   
   **NOTE:** This hotfix is not required for SV appliances.

2. If you are running Microsoft SQL Server 2005, install a more recent version of the database server. Security Center 5.5 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.

3. 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.
Preparing to upgrade from Security Center 5.3 to 5.5

If you need to upgrade your 5.3 system to 5.5, you must prepare the following.

**What you should know**

- Different versions of Security Center Client can coexist on the same machine, but different versions of Security Center Server cannot. Not all current settings are retained 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 from Security Center 5.3 to 5.5:**

1. If you are running Windows Server 2008, Windows 7, or Windows Server 2008 R2, you must install Microsoft hotfix KB2588507.
   
   **NOTE:** This hotfix is not required for SV appliances.

2. If you are running Microsoft SQL Server 2005, install a more recent version of the database server. Security Center 5.5 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.

3. 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.
Preparing to upgrade from Security Center 5.2 to 5.5

If you need to upgrade your 5.2 system to 5.5, you must prepare the following.

What you should know

• Different versions of Security Center Client can coexist on the same machine, but different versions of Security Center Server cannot. Not all current settings are retained 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 from Security Center 5.2 to 5.5:

1. If you are running Windows Server 2008, Windows 7, or Windows Server 2008 R2, you must install Microsoft hotfix KB2588507.
   
   NOTE: This hotfix is not required for SV appliances.

2. If you are running Microsoft SQL Server 2005, install a more recent version of the database server. Security Center 5.5 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.

3. 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.
Differences between Server Admin 5.x and 5.5

Beginning in Security Center 5.5, Server Admin comes with a completely revamped user interface, works with all web browsers (on desktop and mobile devices), supports multi-server connections, and offers a secure connection (HTTPS).

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Server Admin 5.4 and earlier</th>
<th>Server Admin 5.5 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported browsers</td>
<td>Internet Explorer 8, 9, 10, and 11. Must have Microsoft Silverlight plugin installed.</td>
<td>All browsers (on desktop and mobile devices). Microsoft Silverlight is no longer required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection URL</td>
<td>http://&lt;server&gt;/Genetec where &lt;server&gt; is the DNS name or the IP address of the server.</td>
<td>https://&lt;server&gt;/Genetec where &lt;server&gt; is the DNS name or the IP address of the server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-server connection</td>
<td>No. Connects to one server at a time.</td>
<td>Yes. Shows all servers on the system, and allows you to view and change the settings of any of them.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System status overview</td>
<td>Shown in the Directory tab. Only visible when Server Admin is connected to the main server.</td>
<td>Shown on the Dashboard. Three colored LEDd show the status of the system at all times: Database, Directory, and License. Clicking on an error brings you to the section where the problem can be resolved.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global configuration</td>
<td>No. Each server must be configured separately.</td>
<td>Yes. Global settings such as server password, Watchdog, and SMTP settings, are applied to all servers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart Genetec Server service</td>
<td>No.</td>
<td>Yes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User interface language</td>
<td>Set with the Language Tool. Must restart the Genetec Server service and reload the browser page.</td>
<td>Command within Server Admin. No need to restart or reload anything.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set color theme</td>
<td>No.</td>
<td>Choose between Dark (default) and Light.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check software version</td>
<td>From the Config Tool home page, click the button.</td>
<td>Click About.</td>
</tr>
</tbody>
</table>
## Characteristics

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Server Admin 5.4 and earlier</th>
<th>Server Admin 5.5 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deactivate Directory</strong></td>
<td>1. Connect Server Admin to the main server. &lt;br&gt;2. From the <strong>Directory</strong> tab, click <strong>Deactivate Directory</strong>.</td>
<td>From the server list on the left, select the main server (.), and then click <strong>Actions &gt; Deactivate</strong>.</td>
</tr>
<tr>
<td><strong>Activate Directory</strong></td>
<td>1. Connect Server Admin to an expansion server. &lt;br&gt;2. From the <strong>Genetec Server</strong> tab, click <strong>Activate Directory</strong>.</td>
<td>From the server list on the left, select an expansion server, and then click <strong>Actions &gt; Activate</strong>.</td>
</tr>
<tr>
<td><strong>Debug console</strong>&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Not integrated into Server Admin.</td>
<td>Integrated into Server Admin, with many enhancements.</td>
</tr>
<tr>
<td>Access to the debug console</td>
<td>Can be disabled and password protected for each server.</td>
<td>The debug console shares the same password as Server Admin, and cannot be disabled separately.</td>
</tr>
</tbody>
</table>

<sup>1</sup> The debug console is reserved for Genetec™ Technical Support engineers.
## Differences between Security Center 5.x and 5.5 partitions

Starting with Security Center 5.3 there were many changes made that affect how partitions are used and configured.

The following table summarizes the changes to partitions that apply to Security Center version 5.3 and later:

**NOTE:** For more information on creating and configuring partitions in Security Center 5.5, see the *Security Center Administrator Guide*.

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Security Center 5.0, 5.1, or 5.2</th>
<th>Security Center 5.3 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accepted users</strong></td>
<td>Partition manager</td>
<td>Authorized users</td>
</tr>
<tr>
<td><strong>Partition manager</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security configuration</th>
<th>Security Center 5.0, 5.1, or 5.2</th>
<th>Security Center 5.3 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security task</strong></td>
<td>Allows you to configure users, user groups, and partitions in three separate tabs.</td>
<td><strong>User management task</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Partition configuration</th>
<th>Security Center 5.0, 5.1, or 5.2</th>
<th>Security Center 5.3 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can only be created in the <strong>Partitions</strong> tab of the <strong>Security</strong> task in Config Tool.</td>
<td>Can be created from any administration task where an entity hierarchy is shown.</td>
<td></td>
</tr>
<tr>
<td>Partitions are always shown in the <strong>Partitions</strong> tab of the <strong>Security</strong> task in Config Tool.</td>
<td>Users can choose to show or hide partitions in any administration tasks by clicking <strong>Show partitions</strong> ( Delaware-M疾病的 in the <strong>Search</strong> box. Partitions are completely hidden if no user-created partitions exist.</td>
<td></td>
</tr>
<tr>
<td>The content of a partition can only be modified in the partition’s <strong>Properties</strong> tab.</td>
<td>The content of partitions can be modified directly in any entity tree by dragging-and-dropping the entities into the partitions you want them to be a member of.</td>
<td></td>
</tr>
</tbody>
</table>
### Partition access rights configuration

<table>
<thead>
<tr>
<th>Security Center 5.0, 5.1, or 5.2</th>
<th>Security Center 5.3 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users’ access rights for partitions are configured in the <strong>Accepted users</strong> tab of each partition entity.</td>
<td>Users’ access rights for partitions are configured in the <strong>Access rights</strong> tab of each individual user and user group entity.</td>
</tr>
<tr>
<td>Access rights are implicitly inherited from parent user groups. User group members have access to the partition even though they are not shown in the <strong>Accepted users</strong> tab.</td>
<td>Access rights are explicitly inherited from parent user groups and are clearly indicated in the user’s <strong>Access rights</strong> tab.</td>
</tr>
<tr>
<td>Access rights granted for a parent partition are also granted for the child partitions.</td>
<td>Access rights granted for a parent partition are granted by default for the child partitions, but can be denied on a case by case basis.</td>
</tr>
</tbody>
</table>

### Partition membership configuration

<table>
<thead>
<tr>
<th>Security Center 5.0, 5.1, or 5.2</th>
<th>Security Center 5.3 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>An entity cannot belong to more than three partitions.</td>
<td>There is no limit to the number of partitions an entity can belong to.</td>
</tr>
<tr>
<td>There are no rules governing the partition memberships of related entities. Each entity’s membership to a partition must be configured individually. For example, adding a cardholder group to a partition does not automatically add the group members to that partition.</td>
<td>The system automatically applies a set of rules concerning the partition memberships of related entities, based on the most common practices. For example, adding a cardholder group to a partition automatically adds the group members to that partition. The partition administrator can always change the automatically applied memberships on a case by case basis.</td>
</tr>
</tbody>
</table>
# Security Center 5.0, 5.1, or 5.2

- All users can see the entities in the **Public partition** in entity lists, even non accepted users.
- Only accepted users with administrative privileges can view the properties of the entities in the **Public partition**.
- The **Public partition** cannot be renamed nor deleted.

# Security Center 5.3 and later

- The **Public partition** no longer exists.
- When partitions are not required, the **root** partition (named after your **main server**) contains everything you create and is accessible to all users by default.
- When you upgrade a system with multiple partitions to 5.5, the **Public partition** is migrated, but the features of the **Public partition** in 5.5 are different.
  - Users who were not accepted users of the **Public partition** in 5.0, 5.1, or 5.2 will have no access to the **Public partition** in 5.5.
  - You can rename, modify and delete the **Public partition** in 5.5.

## System partition

- The **System** partition is a hidden partition with the unique characteristic that only administrators can access its content.
- Entities that do not belong to a user-created partition implicitly belong to the **System** partition.
- The **System** partition is used to hold all entities that must be accessible to all users at all times. For example, the **Always** schedule, the **Health Monitor** role, and the **Media Router** role, all belong to the **System** partition.
- The **System** partition is exclusively managed by the system. Not even administrators can change it.
- Entities that do not belong to a user-created partition automatically belong to the **root** partition.
Upgrading the Public partition from 5.x to 5.5

After upgrading a Security Center 5.0, 5.1, or 5.2 system that uses multiple partitions to 5.5, you may have to grant access rights over the Public partition to certain users for them to have all the access rights they need in 5.5. This does not apply if you are upgrading from 5.3 and later to 5.5.

Before you begin

- Upgrade Security Center Server to 5.5.
- Upgrade Security Center Client to 5.5.

What you should know

If the Public partition is the only partition in your previous system, then everything is migrated to the root partition in 5.5, and the partitions are hidden. If other partitions exist in your previous system, the Public partition is migrated with the following differences:

- Users who were not accepted users of the Public partition in 5.x will have no access to the Public partition in 5.5.
- You can rename, modify and delete the Public partition in 5.5.

To ensure that all users have the access rights they need after an upgrade from 5.x to 5.5:

1. Identify the users and user groups that need to refer to entities found in the Public partition who are not authorized users of that partition.
   
   **Example:** You may have schedule entities in the Public partition that only administrators are allowed to modify. Other users may only need to refer to these schedules to configure access rules or motion detection on cameras. In a 5.0, 5.1, or 5.2 system, those users do not need to be accepted users of the Public partition, but in 5.3 and later, they do.
   
   If you have no such users in your system, no further action is required.

2. Open the User management task.

3. Create a user group and name it PublicPartitionUsers (or any other name easy to remember), and grant this user group access rights over the Public partition.
   
   Do not create this user group under any parent user group and do not grant it any privileges.

4. Click the Properties tab and add to the user group, the users and user groups that need to refer to the entities found in the Public partition that you identified earlier.

5. Click Apply.
Backward compatibility requirements for Security Center

Because Security Center 5.5 SR3 is backward compatible with many Security Center 5.x components, you can upgrade your Security Center system in stages.

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 5.5 SR3, 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 5.5 SR3, you must upgrade all Directory servers to 5.5 SR3.

- **SQL Server:** Because Security Center 5.5 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 release of Security Center 5.5 includes new role features that might 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.

<table>
<thead>
<tr>
<th>5.5 role</th>
<th>Backward compatible with 5.3 through 5.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Manager</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Directory</td>
<td>No</td>
</tr>
<tr>
<td>Archiver</td>
<td>Yes</td>
</tr>
<tr>
<td>Auxiliary Archiver</td>
<td>Yes</td>
</tr>
<tr>
<td>Directory Manager</td>
<td>No</td>
</tr>
<tr>
<td>Global Cardholder Synchronizer</td>
<td>Yes</td>
</tr>
<tr>
<td>Health Monitor</td>
<td>No</td>
</tr>
<tr>
<td>Intrusion Manager</td>
<td>Yes</td>
</tr>
</tbody>
</table>
5.5 role | Backward compatible with 5.3 through 5.4
---|---
LPR Manager | Yes
Media Router | No
Omnicast Federation | Yes
Plugin (all instances) | No
Point of Sale | No
Report Manager | Yes
RTSP Media Router | Yes
Security Center Federation | Yes
Zone Manager | Yes

**Backward compatibility with Security Center tasks**

The Security Center 5.5 tasks that are backward compatible with Security Desk 5.3 and 5.4 are summarized in the following table.

<table>
<thead>
<tr>
<th>Task category</th>
<th>Task type</th>
<th>Backward compatible with Security Desk 5.3 through 5.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Monitoring</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cardholder management</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Visitor management</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>People counting</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Credential management</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Hotlist and permit editor</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Inventory management</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Remote</td>
<td>No</td>
</tr>
<tr>
<td>Alarm management</td>
<td>Alarm monitoring</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Alarm report</td>
<td>Yes</td>
</tr>
<tr>
<td>Investigation</td>
<td>Incidents</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Transactions</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Zone activities</td>
<td>Yes</td>
</tr>
<tr>
<td>Task category</td>
<td>Task type</td>
<td>Backward compatible with Security Desk 5.3 through 5.4</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Investigation &gt; Access control</td>
<td>Area activities</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Door activities</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cardholder activities</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Visitor activities</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Area presence</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Time and attendance</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Credential activities</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Credential request history</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Elevator activities</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Visit details</td>
<td>Yes</td>
</tr>
<tr>
<td>Investigation &gt; Asset management</td>
<td>Asset activities</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Asset inventory</td>
<td>No</td>
</tr>
<tr>
<td>Investigation &gt; Intrusion detection</td>
<td>Intrusion detection area activities</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Intrusion detection unit events</td>
<td>Yes</td>
</tr>
<tr>
<td>Investigation &gt; LPR</td>
<td>Hits</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Hits (Multi-region)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Reads</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Reads (Multi-region)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Route playback (5.2 and earlier)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Patroller tracking (5.3 and later)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Inventory report</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Daily usage per Patroller</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Logons per Patroller</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Reads/hits per day</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Reads/hits per zone</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Zone occupancy</td>
<td>Yes</td>
</tr>
<tr>
<td>Task category</td>
<td>Task type</td>
<td>Backward compatible with Security Desk 5.3 through 5.4</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Investigation &gt; Video</td>
<td>Archives</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Bookmarks</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Motion search</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Camera events</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Forensic search</td>
<td>Yes</td>
</tr>
<tr>
<td>Maintenance</td>
<td>System status</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Audit trails</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Activity trails</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Health history</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Health statistics</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Hardware inventory</td>
<td>Yes</td>
</tr>
<tr>
<td>Maintenance &gt; Access control</td>
<td>Access control health history</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Access control unit events</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cardholder access rights</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Door troubleshooter</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Access rule configuration</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cardholder configuration</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Credential configuration</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>I/O configuration</td>
<td>Yes</td>
</tr>
<tr>
<td>Maintenance &gt; Video</td>
<td>Camera configuration</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Archiver events</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Archiver storage details</td>
<td>Yes</td>
</tr>
</tbody>
</table>

\[^a\]Includes live video and playback video.
Supported federations for Security Center 5.5 SR3

Security Center 5.5 SR3 can federate and be federated with other Security Center systems running different versions.

Security Center 5.5 can federate the following:

- Security Center 5.5, 5.4, 5.3, and 5.2 systems.
- Omnicast 4.6, 4.7 and 4.8 systems.
- Stratocast™ 1.7 systems.

Security Center 5.5 can be federated by the following:

- Security Center 5.4 and 5.5 systems.

**IMPORTANT:** As a general rule, a system running the most current release of Security Center can:

- Federate systems up to three versions back
- Be federated by a system running the previous version of Security Center.

For example, Security Center 5.5 systems can federate Security Center 5.4, 5.3, and 5.2. A Security Center 5.3 system can only federate a 5.4 system, not a 5.5 system.

For more information about the limitations of federated entities, see the About federated entities section of the Security Center Administrator Guide. These limitations apply to both forward and backward federations.
Upgrading from an earlier release of Security Center 5.5

To have the latest release of Security Center 5.5, you can upgrade from an earlier release of 5.5 to SR3 after you have completed the preparation steps.

**Before you begin**

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

**What you should know**

You do not need to change your license when you upgrade from an earlier release of the same version of Security Center.

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

**To upgrade from an earlier release of Security Center 5.5 to release SR3:**

1. Install Security Center 5.5 SR3 on your main server.
2. Install Security Center 5.5 SR3 on your expansion servers, according to your priorities.
3. Install Security Center Client 5.5 SR3 on your client workstations, according to your priorities.

**After you finish**

If you used the file `AllowedSynchronizationConfiguration.xml` to set the synchronization times of your HID VertX units, you must manually reapply the settings from Config Tool after the upgrade.

**TIP:** Configure one unit with the required synchronization settings, and then use the Copy configuration tool to set the same settings on multiple units.
Upgrading from Security Center 5.4 to 5.5

To have the latest version of Security Center, you can upgrade from your 5.4 system to 5.5 after you have completed the preparation steps.

**Before you begin**

- Read the things you need to know and do before you upgrade.
- Read about backward compatibility.

**What you should know**

For supported upgrade paths, see the *Security Center Release Notes*.

**To upgrade from Security Center 5.4 to 5.5:**

1. If Omnicast systems were federated to your previous Security Center system, uninstall the previously installed compatibility packs.
2. Upgrade your main server.
3. Upgrade the expansion servers and client workstations in your system according to your priorities and schedule.
   - 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 as used for your previous installation: passwords, database, 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.
Upgrading from Security Center 5.3 to 5.5

To have the latest version of Security Center, you can upgrade from your 5.3 system to 5.5 after you have completed the prerequisite steps.

Before you begin

- Read the things you need to know and do before you upgrade.
- Read about backward compatibility.

What you should know

For supported upgrade paths, see the Security Center Release Notes.

To upgrade from Security Center 5.3 to 5.5:

1. If Omnicast systems were federated to your previous Security Center system, uninstall the previously installed compatibility packs.
2. Upgrade your main server.
3. Upgrade the expansion servers and client workstations in your system according to your priorities and schedule.

   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 that were used for your previous installation: passwords, databases, ports, general properties, and so on.

After you finish

If you used the file `AllowedSynchronizationConfiguration.xml` to set the synchronization times of your HID VertX units, you must manually reapply the settings from Config Tool after the upgrade.

**TIP:** Configure one unit with the required synchronization settings, and then use the Copy configuration tool to set the same settings on multiple units.
Upgrading from Security Center 5.2 to 5.5

To have the latest version of Security Center, you can upgrade from your 5.2 system to 5.5 after you have completed the prerequisite steps.

Before you begin

- Read the things you need to know and do before you upgrade.
- Read about backward compatibility.
- Read about the differences between Security Center 5.x and 5.4 partitions.

What you should know

For supported upgrade paths, see the Security Center Release Notes.

If no partition other than the Public partition was used in your old system, then all entities are moved to the root partition after the upgrade to 5.5, and all partitions are hidden. All users have access to the root partition.

If partitions other than the Public partition were used in your old system, then all old partitions are migrated to 5.5 with the same content and same accepted users (called authorized users in 5.5). The following also apply:

- All entities that were hidden in 5.x are moved to the root partition in 5.5.
- Only the administrators have access to the root partition.
- Only accepted users with administrative privileges can view the properties of the entities in the Public partition.
- You can rename, modify and delete the Public partition in 5.5.

To upgrade from Security Center 5.2 to 5.5:

1. If Omnicast systems were federated to your previous Security Center system, uninstall the previously installed compatibility packs.
2. Upgrade your main server.
3. If partitions other than the Public partition were used in your old system, upgrade the Public partition.
4. Upgrade the expansion servers and client workstations in your system according to your priorities and schedule.
   - 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 that were used for your previous installation: passwords, databases, ports, general properties, and so on.

After you finish

If you used the file AllowedSynchronizationConfiguration.xml to set the synchronization times of your HID VertX units, you must manually reapply the settings from Config Tool after the upgrade.

**TIP:** Configure one unit with the required synchronization settings, and then use the Copy configuration tool to set the same settings on multiple units.
Upgrading from Security Center 5.1 to 5.5

Direct upgrades from Security Center 5.1 to 5.5 are not supported. First you need to upgrade your system to Security Center 5.3, and then to 5.5.

**To upgrade from Security Center 5.1 to 5.5:**

1. Upgrade your Security Center 5.1 system to version 5.3.
   For more information, see the *Security Center Installation and Upgrade Guide 5.3* of the latest service release.
2. Prepare to upgrade from Security Center 5.3 to 5.5.
3. Upgrade to Security Center 5.5.
Upgrading from Security Center 5.0 to 5.5

Direct upgrades from Security Center 5.0 to 5.5 are not supported. First you need to upgrade your system to Security Center 5.3, and then to 5.5.

To upgrade from Security Center 5.0 to 5.5:

1. Upgrade your Security Center 5.0 system to version 5.3.
   For more information, see the Security Center Installation and Upgrade Guide 5.3 of the latest service release.
2. Prepare to upgrade from Security Center 5.3 to 5.5.
3. Upgrade to Security Center 5.5.
Upgrading from Security Center 4.0 to 5.5

Direct upgrades from Security Center 4.0 to 5.5 are not supported. First you need to upgrade your system to Security Center 5.2, and then to 5.5.

**To upgrade from Security Center 4.0 to 5.5:**

1. Upgrade your Security Center 4.0 system to version 5.2.
   
   For more information, see the *Security Center Installation and Upgrade Guide 5.2* of the latest service release.

2. Prepare to upgrade from Security Center 5.2 to 5.5.

3. Upgrade to Security Center 5.5.
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 any known issues, limitations, supported firmware, and other information about this release.
- You need a one-hour 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 5.5). 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 (①), 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 5.5 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 ②). 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 5.5 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 67

**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 Security Center features that 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 Security Center features that 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.
Reactivating the Security Center license for Failover Directory systems

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.
3 Click **Modify license for all servers**.
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 dialog box](image)

Click the colored tabs to view your license options.

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**

This procedure fits in the context of *reactivating your Security Center license on a Failover Directory system*.
To update your license using a license file:

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

   ![License management dialog box](image)

   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.

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

   ![License management dialog box](image)

   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.

3 From another computer with Internet access, log on to GTAP at: https://gtap.genetec.com

![Login page](https://genetec.com/Login.png)

4 On the GTAP 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**.
  1. On the Genetec Portal - Home page, click **Activate new system**.
  2. From the **System ID** drop-down list, select your system, and click **Submit**.

The browser opens to the System Information page.
5 Scroll down to the License information section and click Activate license.

6 In the dialog box that opens, browse to your validation key (.vk file), and click Submit. The message License activation successful appears.

7 Click Download License, and save the license key to a file. The default name is your System ID followed by _Directory_License.lic.

8 Return to the Config Tool workstation.

9 In the License management dialog box, click Manual activation.

10 In the Manual activation dialog box, browse for the license key (.lic file), and click Open.
11 Click **Activate**.
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.

What you should know

You need the Security Center 5.5 Config Tool to connect it to the 5.5 Directory. If Security Center Client was installed on the main server, upgrade it at the same time.

**NOTE:** Client upgrade from Security Center 5.1 to Security Center 5.5 is not supported. Security Center 5.5 Client is installed side-by-side with previous Security Center Client versions. After it has been installed, you can delete the older version.

If a reboot warning message appears 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 5.5 on your main server.**  
   Use the **Main server** installation type.  
   The InstallShield Wizard automatically detects an earlier version of Security Center and upgrades it to Security Center 5.5.

2. **When prompted to confirm that you have a current backup of your databases, click the confirmation checkbox, click Next, and follow the rest of the InstallShield Wizard instructions.**

The installer updates your Security Center software and the schema of your Directory database.
3  Activate your new Security Center 5.5 license.

**Related Topics**
- Backing up databases on page 92
- Upgrading the Security Center Directory database on page 93
- Activating Security Center license using the web on page 22
- Activating Security Center license without Internet access on page 26
- Preparing to upgrade from Security Center 5.4 to 5.5 on page 58
- Preparing to upgrade from Security Center 5.3 to 5.5 on page 59
- Preparing to upgrade from Security Center 5.2 to 5.5 on page 60
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

- If you are migrating from Omnicast 4.x, see the Omnicast Migration Guide.
- Back up all role databases accessed from the expansion server you are upgrading.

What you should know

If a reboot warning message appears 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 5.5 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 5.5.
2. Repeat the steps for all expansion servers in your system.

After you finish

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

Related Topics

- Backing up databases on page 92
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

Client upgrade from Security Center 5.1 to Security Center 5.5 is not supported. Security Center 5.5 Client is installed side-by-side with previous Security Center Client versions. After it has been installed, you can delete the older version.

To upgrade from Security Center 5.1 to 5.5:

1  Install Security Center Client.

   NOTE: The user workspace configuration is not preserved. In previous versions of Security Center, the user workspace was saved as a workstation configuration. Starting from 5.4, the user workspace is saved as part of the user profile in the Directory. The upgrade does not convert these settings for you.

2  From the Windows Control Panel, uninstall the older version of Security Center Client.

To upgrade from Security Center 5.2, 5.3, or 5.4 to 5.5:

1  Install Security Center Client.

   The installer automatically detects an earlier version of Security Center software and upgrades it to 5.5.
Backing up databases

You can protect the data in a role’s database by regularly backing up the database. Also, it is always best practice to backup your databases before an upgrade.

**What you should know**

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 very 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, see [Transferring video archives manually](#).
- To back up the Directory database while the *Backup and restore* failover mode is enabled, see [Generating full Directory database backup](#).
- 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.
   
   **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.

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 the Security Center Directory database

The Security Center 5.5 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.

To upgrade the Directory database:

1. Do one of the following:
   - Click Database with the flashing red LED.
   - Click Database update ( ) in the Directory section.

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

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

   When the upgrade is completed, the Status shows OK.

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

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

5. Open the System task, and select Roles.

6. Select the Archiver role, and click Resources.

7. In the Actions section, click Database update ( ) .
After the upgrade is complete, the **Database status** indicates *Connected*.

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

**After you finish**

*Shrink the Archiver database*, and if necessary, other databases that you have upgraded.
Shrinking Security Center databases after an upgrade

After a database upgrade, its disk usage may significantly 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 5.4, 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 its disk usage with SQL Server Management Studio.

**What you should know**

Depending on the recovery model of your database, a transaction log backup may be required in order to reclaim the unused disk space. For more information, see the following online articles: [Recovery Models (SQL Server)](https://docs.microsoft.com/en-us/sql/database-engine/management/backup-and-recovery/recovery-models) and [Transaction Log Truncation](https://docs.microsoft.com/en-us/sql/database-engine/transaction-log-truncation).

**To shrink a database:**

1. Follow the procedure [Shrink a Database](https://docs.microsoft.com/en-us/sql/database-engine/management/shrink-a-database) published online by Microsoft.
2. Apply the same procedure to all databases that require shrinking.
About the Genetec Update Service

The Genetec Update Service is a web-based service that allows you to update your Security Center products when a new release becomes available.

Starting with Security Center 5.4 GA, the Genetec Update Service is automatically installed with Security Center and enables you to do the following:

- Update your Security Center products, when a new release becomes available.
- Check for updates at regular intervals.
- Automatically download updates when they become available.

**NOTE:** Updates can be configured to be downloaded in the background, but still require manual intervention to be applied.

- View when the last check for updates occurred.
- Configure peer-to-peer sharing with multiple peers connected to the Internet, or a single peer connected to the Internet. Update files are downloaded once and shared with other peer machines.

**IMPORTANT:** For details on how to log on to the Genetec Update Service, see [Logging on to the Genetec Update Service](#) on page 97.
Logging on to the Genetec Update Service

To log on to Genetec Update Service, you must open the application and enter your Genetec Update Service password (if applicable).

**Before you begin**

You need your Genetec Update Service password (if one has been defined).

**What you should know**

The Genetec Update Service can be opened in a web browser by typing `https://localhost:4595`, or from the start menu.

**NOTE:** If you install the Genetec Update Service manually, it cannot be accessed from the Start menu.

To log on to the Genetec Update Service:

1. Do one of the following:
   - Click **Start > All Programs > Genetec Security Center 5.x > Genetec Update Service**.
   - Type `https://localhost:4595` in your web browser.

2. In the **Sign in** dialog box, do one of the following:
   - Log on with the default blank password.
   - Enter your Genetec Update Service password.

   **NOTE:** The Genetec Update Service password can be configured on the **Settings** page under the **Advanced** section.

For more information about using the Genetec Update Service, open the Genetec Update Service and click **Help**.
Automating Security Center installation

This section includes the following topics:

- "Silent installation in Security Center" on page 99
- "Preparing to perform a silent installation" on page 100
- "Silent install command for Security Center" on page 101
- "Installer (MSI) options" on page 103
- "Sample Security Center Server installation commands" on page 108
- "Sample Security Center Client installation commands" on page 110
- "Uninstalling Security Center 5.5 in silent mode" on page 111
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 all software prerequisites.**
   
   Security Center installer automatically verifies and installs the software prerequisites on your system. This may cause your system to restart. Therefore, it is best practice to manually install the software prerequisites before launching the silent installer.

2. 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 5
Silent install command 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 `setup.exe` found in the root folder of the installation package. It is an AutoRun-enabled version of the standalone installer, and as such, it 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.

<table>
<thead>
<tr>
<th>Setup option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ISInstallDir</td>
<td>Specifies the path where the software will be installed.</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLES:</strong></td>
</tr>
<tr>
<td></td>
<td>- /ISInstallDir=C:\MyFolder</td>
</tr>
<tr>
<td></td>
<td>- /ISInstallDir=&quot;D:\Program Files\MyFolder&quot;</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> In the second example, the (&quot;) are required because the value</td>
</tr>
<tr>
<td></td>
<td>contains spaces. If not specified, the default is</td>
</tr>
<tr>
<td></td>
<td>&lt;ProgramFiles&gt;\Genetec Security Center 5.5, where &lt;ProgramFiles&gt; is either</td>
</tr>
<tr>
<td></td>
<td>%PROGRAMFILES% or %PROGRAMFILES(X86)%, depending on the version of your</td>
</tr>
<tr>
<td></td>
<td>operating system.</td>
</tr>
<tr>
<td>/ISFeatureInstall</td>
<td>Specifies the features to be installed. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>- Server (Genetec Server with or without Directory, depends on the</td>
</tr>
<tr>
<td></td>
<td>SERVER_TYPE installer option)</td>
</tr>
<tr>
<td></td>
<td>- Client (Security Desk and Config Tool)</td>
</tr>
<tr>
<td></td>
<td>- SecurityDesk (only Security Desk)</td>
</tr>
<tr>
<td></td>
<td>- ConfigTool (only Config Tool)</td>
</tr>
<tr>
<td></td>
<td>- CompPacks,CompPack4x[,CompPack4x] (Omnicast compatibility packs, you must</td>
</tr>
<tr>
<td></td>
<td>specify at least one pack)</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLES:</strong></td>
</tr>
<tr>
<td></td>
<td>- /ISFeatureInstall=Server,Client (DEFAULT)</td>
</tr>
<tr>
<td>/silent</td>
<td>Sets the Security Center setup.exe program to run in silent mode</td>
</tr>
<tr>
<td></td>
<td>with no user interaction.</td>
</tr>
<tr>
<td>Setup option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| /debuglog<FilePath> | Enables the creation of the debug 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:\DebugLog.log"` |
| /log<FolderPath>    | Enables the creation of log files and specifies the folder path.  
**NOTE:** The `<FolderPath>` must exist. The setup program will not create it.  
**EXAMPLE:** `/log"C:\AllMyLogFiles\"` |
| /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) option list.  
Each option in the 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 (`\`). |
## 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.

<table>
<thead>
<tr>
<th>Installer (MSI) option</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 |
| SQLSERVER_GROUP        | Specify if a new or an existing SQL server is silently installed. The possible values are:  
  - NewServer (must be used with SQL_INSTANCE_NAME)  
  - ExistingServer (DEFAULT)  
| SQL_INSTANCE_NAME      | Specify the new SQL Server instance's name. This option needs to be specified when SQLSERVER_GROUP has a value of NewServer. |
| 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 |
| DATABASE_SERVER        | Same as GLOBAL_SERVER option. This parameter maintains backward compatibility with previous silent installation scripts. |
| DATABASE_INSTANCE      | Used in conjunction with the BACKUP_DATABASE option. Specify the instance name of the Directory database, if different from the default. |
| 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 N.  
  **EXAMPLE:** UPGRADE_DATABASE=Y |
### Installer (MSI) option

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACKUP_DATABASE</td>
<td>Specify that the Directory database must be backed up prior to the installation (and prior to the database upgrade). Configuration Files are also backed up in the same destination folder as the database. If the database does not exist, the database is not backed up but the configuration files still are. Possible values are Y or N. When this option is omitted, the default value is N. When set to Y, the BACKUP_DATABASE_PATH property must be set to a valid folder. <strong>EXAMPLE:</strong> BACKUP_DATABASE=Y</td>
</tr>
<tr>
<td>BACKUP_DATABASE_PATH</td>
<td>Used in conjunction with the BACKUP_DATABASE option. Specify the folder where the database backup must be saved. If the path does not exist, it will be created. <strong>EXAMPLE:</strong> BACKUP_DATABASE_PATH=C:\Backups</td>
</tr>
<tr>
<td>SERVICEUSERNAME</td>
<td>Specify the username to use in the services. <strong>EXAMPLE:</strong> SERVICEUSERNAME=\admin</td>
</tr>
<tr>
<td>SERVICEPASSWORD</td>
<td>Specify the password to use in the services. <strong>EXAMPLE:</strong> SERVICEPASSWORD=anypassword</td>
</tr>
<tr>
<td>SERVERADMIN_PORT</td>
<td>Specify the HTTP port for the web-based Server Admin. <strong>EXAMPLE:</strong> SERVERADMIN_PORT=8080</td>
</tr>
<tr>
<td>SERVERADMIN_PASSWORD</td>
<td>Specify the password (minimum 8 characters) to open the web-based Server Admin.</td>
</tr>
</tbody>
</table>

User and password need to be created first with the right credentials prior to using those properties. If not specified, the default is blank.
<table>
<thead>
<tr>
<th>Installer (MSI) option</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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  
  - Brasilian 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. |
| WEBSERVER_PORT         | Specify the HTTP port for the web-based Server Admin.  
  If not specified, the default is 80. |
| 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 |
<table>
<thead>
<tr>
<th>Installer (MSI) option</th>
<th>Description</th>
</tr>
</thead>
</table>
| MAINSERVER_ENDPOINT         | Used for expansion server installation. Specify the name or IP address of the main server.  

**EXAMPLE:** `MAINSERVER_ENDPOINT=MYMAINSERVER`  

<table>
<thead>
<tr>
<th>MAINSERVER_PASSWORD</th>
<th>Used for expansion server installation. Enter the password of the main server that it is supposed to connect to.</th>
</tr>
</thead>
</table>
| DATACOLLPOLICY              | This option allows the configuration of the Service Availability Monitor (SAM). The possible values are:  

- **Anonymous:** SAM will collect anonymous data (DEFAULT)  
- **On:** SAM will collect data with system information. Requires ACTIVATIONCODE.  
- **Off:** SAM will not collect data.                                                                                                                                                                                                                                           |
| ACTIVATIONCODE              | This is the activation code required to allow SAM to collect system data.  

**EXAMPLE:** `DATACOLLPOLICY=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`  

| 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`
<table>
<thead>
<tr>
<th>Installer (MSI) option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>REBOOT</strong></td>
<td>This option allows you to force or suppress a reboot after the Server installation has ended. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>F</strong> - To force a reboot when your installation is complete.</td>
</tr>
<tr>
<td></td>
<td>• <strong>S</strong> - To suppress any reboot except the one caused by the ForceReboot action.</td>
</tr>
<tr>
<td></td>
<td>• <strong>R</strong> - To suppress any reboot caused by Windows Installer actions. (DEFAULT)</td>
</tr>
<tr>
<td><strong>SKIPSERVICESTART</strong></td>
<td>This option allows you to avoid starting the Security Center services immediately after the installation (default behavior), if for example, you need to install hotfixes right after the full installation. When you use this option, don’t forget to start the Security Center services (NET START GenetecServer and NET START GenetecWatchdog) after the hotfix installation.</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE:</strong> <strong>SKIPSERVICESTART=Y</strong></td>
</tr>
</tbody>
</table>
Sample Security Center Server installation commands

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

Example

Genetec Server with Directory is installed in English with a specific Username and Password for the service to run under. The files are located in a new directory, the database server is specified, and there is no reboot. Setup runs in silent mode without any questions.


Example

A standard installation of Genetec Server as the main server, with Directory, and without any questions. Only the installation path is different.

"Security Center Setup.exe" /language:1033 /silent /ISInstallLDir=c:\GENETEC_PATH /ISFeatureInstall=Server

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 /ISInstallLDir=c:\GENETEC_PATH /ISFeatureInstall=Server SERVER_TYPE=Expansion

Example

A standard installation in French, in silent mode without any questions.

"Security Center Setup.exe" /language:3084 /silent

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" /language:1033 /silent /ISFeatureInstall=Client,Server,CompPacks,CompPack47,CompPack48
Example

A complete installation in English, in silent mode 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:" /debuglog:C:\DebugLog.log"

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 LANGUAGECHOSEN=1025
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.

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

**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
```

**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
```

**Example**

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

```
"Security Center Setup.exe" /language:3084 /silent
```

**Example**

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

```
"Security Center Setup.exe" /language:1033 /silent /IsInstallFeature=Client,Server,CompPacks,CompPack48
```

**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 LANGUAGECHOSEN=1025
```
Uninstalling Security Center 5.5 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
Troubleshooting

This section includes the following topics:

- "Troubleshooting: video stability and performance issues" on page 113
- "Troubleshooting: Files remain blocked after unblocking them manually" on page 114
Troubleshooting: 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 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 machine. To enhance performance you must install hotfix KB2588507.

**To install the Microsoft hotfixes:**

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.
Troubleshooting: 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**

You have to run *streams.exe* only on those files that remain blocked after attempting to manually unblock them fails. The error message that appears during installation resembles: “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*:**

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.

**Related Topics**

*Unblocking files manually* on page 12
### Glossary

#### A

**Access control**
The Access control task is a type of 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 a type of 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**
Access Manager is a type of role that 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 or an elevator floor.

**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 Synergis, 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 is a type of entity that defines a list of cardholders to whom access is either granted or denied based on a schedule. An access rule can be applied to a secured area or to an access point.

**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 Directory**

Active Directory is a directory service created by Microsoft, and a type of role that imports users and cardholders from an Active Directory and keeps them synchronized.

**Active Directory Federation Services**

Active Directory Federation Services (ADFS) is a component of the Microsoft® Windows® operating system that issues and transforms claims, and implements federated identity. 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.

**Alarms**

The Alarms task is a type of administration task that allows you to configure alarms and monitor groups.

**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.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>analog monitor</td>
<td>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.</td>
</tr>
<tr>
<td>antipassback</td>
<td>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.</td>
</tr>
<tr>
<td>Archive transfer</td>
<td>The Archive transfer task is a type of 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.</td>
</tr>
<tr>
<td>archive transfer</td>
<td>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.</td>
</tr>
<tr>
<td>Archiver</td>
<td>The Archiver is a type of role that 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.</td>
</tr>
<tr>
<td>Archiver events</td>
<td>Archiver events is a type of maintenance task that reports on events pertaining to selected Archiver roles.</td>
</tr>
<tr>
<td>Archives</td>
<td>Archives is a type of investigation task that allows you to find and view available video archives by camera and time range.</td>
</tr>
<tr>
<td>Archive storage details</td>
<td>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.</td>
</tr>
<tr>
<td>area</td>
<td>An area is a type of entity that represents a concept or a physical location (room, floor, building, site, and so on) used for grouping other entities in the system.</td>
</tr>
<tr>
<td>Area activities</td>
<td>Area activities is a type of maintenance task that reports on events pertaining to selected Archiver roles.</td>
</tr>
<tr>
<td>Area presence</td>
<td>Area presence is a type of investigation task that provides a snapshot of all cardholders and visitors currently present in a selected area.</td>
</tr>
<tr>
<td>Area view</td>
<td>The Area view task is a type of administration task that allows you to configure areas, doors, cameras, tile plugins, intrusion detection areas, zones, and other entities found in the area view.</td>
</tr>
<tr>
<td>area view</td>
<td>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.</td>
</tr>
</tbody>
</table>
**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.

**AutoVu**

AutoVu is the IP license plate recognition (LPR) system of Security Center that automates the reading and verification of vehicle license plates. AutoVu Sharp cameras capture license plate images, and send the data to Patroller or Security Center to verify against lists of vehicles of interest (hotlists) and vehicles with permits (permit lists). You can install AutoVu in a fixed configuration (e.g. on a pole in a parking lot), or in a mobile configuration (e.g. on a police car). You can use AutoVu for scofflaw and wanted vehicle identification, city-wide surveillance, parking enforcement, parking permit control, vehicle inventory, security, and access control.

**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**

Auxiliary Archiver is a type of role that supplements the video archive produced by the Archiver. Unlike the Archiver, the Auxiliary Archiver 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 depends on the Archiver to communicate with the video units. It cannot operate on its own.

**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.

**bookmark**

A bookmark is a short text that is used to mark a specific position in a recorded video sequence. Once created, you can use bookmarks to search for the video sequences that they pertain to.

**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 Genetec's proprietary connector box 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 is a type of entity that represents a single video source in the system. The video source can either be an IP camera, or an analog camera that is connected 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.
<table>
<thead>
<tr>
<th><strong>camera sequence</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>canvas</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>card and PIN</strong></td>
<td>Card and PIN is an access point mode that requires a cardholder to present their card, and then enter a personal identification number (PIN).</td>
</tr>
<tr>
<td><strong>cardholder</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Cardholder access rights</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Cardholder activities</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Cardholder configuration</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>cardholder group</strong></td>
<td>A cardholder group is a type of entity that configures the common access rights of a group of cardholders.</td>
</tr>
<tr>
<td><strong>Cardholder management</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>cash register</strong></td>
<td>A cash register is a type of entity that represents a single cash register (or terminal) in a point of sale system.</td>
</tr>
<tr>
<td><strong>certificate</strong></td>
<td>Designates one of the following: (1) digital certificate; (2) SDK certificate.</td>
</tr>
<tr>
<td><strong>cyphertext</strong></td>
<td>In cryptography, cyphertext is the encrypted data.</td>
</tr>
<tr>
<td><strong>certificate authority</strong></td>
<td>A certificate authority or certification authority (CA) is an entity or organization that signs identity certificates and attests to the validity of their contents.</td>
</tr>
<tr>
<td><strong>City Parking Enforcement</strong></td>
<td>City Parking Enforcement is a Patroller software installation that is configured for the enforcement of parking permit and overtime restrictions.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>City Parking Enforcement with Wheel Imaging</td>
<td>City Parking Enforcement with Wheel Imaging is a City Parking Enforcement installation of a Patroller application that also includes wheel imaging. The use of maps and of the Navigator is mandatory.</td>
</tr>
<tr>
<td>claim</td>
<td>A claim is a statement, such as a name, identity, key, or group, made by one subject about itself or another subject. Claims are issued by a provider, and they are given one or more values and then packaged in security tokens that are issued by a security token service (STS).</td>
</tr>
<tr>
<td>claims provider</td>
<td>A software component or service that generates security tokens upon request. Also known as the issuer of claims.</td>
</tr>
<tr>
<td>claims-based authentication</td>
<td>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.</td>
</tr>
<tr>
<td>client-specific key stream</td>
<td>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.</td>
</tr>
<tr>
<td>Config Tool</td>
<td>Config Tool is a Security Center administrative application used to manage all Security Center users, and configure all Security Center entities such as areas, cameras, doors, schedules, cardholders, Patroller/LPR units, and hardware devices.</td>
</tr>
<tr>
<td>Conflict resolution utility</td>
<td>Conflict resolution utility is a tool that helps you resolve conflicts caused by importing users and cardholders from an Active Directory.</td>
</tr>
<tr>
<td>context camera</td>
<td>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.</td>
</tr>
<tr>
<td>controlled exit</td>
<td>A controlled exit is when credentials are necessary to leave a secured area.</td>
</tr>
<tr>
<td>controller module</td>
<td>Controller module is the processing component of Synergis Master Controller with IP capability. This module comes pre-loaded with the controller firmware and the web-based administration tool, Synergis Appliance Portal.</td>
</tr>
<tr>
<td>Copy configuration tool</td>
<td>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.</td>
</tr>
<tr>
<td>covert hit</td>
<td>A covert hit is a read (captured license plate) that is matched to a covert hotlist. Covert hits are not displayed on the Patroller screen, but can be displayed in Security Desk by a user with proper privileges.</td>
</tr>
</tbody>
</table>
covert hotlist  A covert hotlist is a hotlist hidden from the AutoVu Patroller users. Reads matching a covert hotlist generate covert hits.

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 Patroller (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).

**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 fish-eye 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**  
Directory is the main role that identifies your system. It manages all entity configurations and system wide settings in Security Center. 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**  
Directory Manager is the role that 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 is a type of entity that 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.

**E**

**edge recording**
Edge recording is the process of recording and storing video recordings 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.

**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.
Glossary

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, and can be programmed to trigger actions. Every event mainly focuses on one entity, 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.

**failover**

A 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 when the primary server becomes unavailable, either through failure or through scheduled downtime.

**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 an 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**
Federation is the virtual system formed by joining multiple, independent Genetec IP security systems. Federation allows the users on your local system to view and control the entities belonging to independent remote systems, as if they were on your 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 Genetec's proprietary data structure 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 created in response to specific client requests. The key streams are included only if the data streams are encrypted.

**fusion stream encryption**
Fusion stream encryption is Genetec's proprietary technology used to protect the privacy of your video archives. The Archiver uses a two-level encryption strategy to ensure that only authorized client machines can access your private data.

**G**

**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 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 is a web-based service that allows you to update your Security Center products when a new release becomes available.

Genetec Video Player
The 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.

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 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
Global Cardholder Synchronizer is a type of role that ensures the two-way synchronization of shared cardholders and their related entities between the local system (sharing participant) 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.

H

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.

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

Health Monitor is the central role that monitors system entities such as servers, roles, units, and client applications for health issues.

Health statistics

Health statistics is a type of maintenance task that gives you an overall view of the health of your system.

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 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 type of entity that defines 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.

**I/O zone**
An I/O zone is a zone entity in which the I/O linking can be spread across multiple Synergis units, while one unit acts as the master unit. All Synergis units involved in an I/O zone must be managed by the same Access Manager. The I/O zone works independently of the Access Manager, but ceases to function if the master unit is down. An I/O zone can be armed and disarmed from Security Desk as long as the master unit is online.

**identity certificate**
An identity certificate, 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 CSV (Comma Separated Values) 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.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents</td>
<td>Incidents is a type of investigation task that allows you to search, review, and modify incident reports.</td>
</tr>
<tr>
<td>interface module</td>
<td>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.</td>
</tr>
<tr>
<td>interlock</td>
<td>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.</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>The Intrusion detection task is a type of administration task that allows you to configure intrusion detection roles and units.</td>
</tr>
<tr>
<td>intrusion detection area</td>
<td>An intrusion detection area is a type of entity that corresponds to a zone or a partition (group of sensors) on an intrusion panel.</td>
</tr>
<tr>
<td>Intrusion detection area activities</td>
<td>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.</td>
</tr>
<tr>
<td>intrusion detection unit</td>
<td>An intrusion detection unit is a type of entity that represents an intrusion panel (or alarm panel) that is monitored and controlled by Security Center.</td>
</tr>
<tr>
<td>Intrusion detection unit events</td>
<td>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.</td>
</tr>
<tr>
<td>Intrusion Manager</td>
<td>Intrusion Manager is a type of role that monitors and controls intrusion panels (or alarm panels). It listens to the events reported by the intrusion panels, provides live reports to Security Center, and logs the events in a database for future reporting.</td>
</tr>
<tr>
<td>intrusion panel</td>
<td>An intrusion 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.</td>
</tr>
<tr>
<td>Inventory management</td>
<td>Inventory management is a type of operation task that allows you to add and reconcile license plate reads to a parking facility inventory.</td>
</tr>
<tr>
<td>Inventory report</td>
<td>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).</td>
</tr>
<tr>
<td>I/O configuration</td>
<td>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.</td>
</tr>
<tr>
<td>I/O linking</td>
<td>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.</td>
</tr>
</tbody>
</table>
Glossary

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 unit incorporating a camera.

IPv4
IPv4 is the first generation IP protocol using a 32-bit address space.

IPv6
IPv6 is a video unit incorporating a camera.

K

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.

L

Law Enforcement
Law Enforcement is a 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.

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. License Plate Recognition (LPR) converts license plate numbers cropped from camera images into a database searchable format.

live hit
A live hit is a hit matched by the Patroller and immediately sent to the Security Center over a wireless network.

live read
A live read is a license plate captured by the Patroller and immediately sent to the 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 Patroller.

**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 is over 24 hours. No more than one overtime rule may use the long term regulation in the entire system.

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

**LPR camera**
A LPR camera is a camera connected to an LPR unit that produces high resolution close-up images of license plates.

**LPR Manager**
LPR Manager is a type of role that manages and controls Patrollers and fixed Sharp units. The LPR Manager stores the data (reads, hits, GPS data, and so on) collected by the LPR units and Patrollers into a central database for reporting. The LPR Manager is also responsible for updating fixed Sharps and Patrollers in the field with hotfixes, hotlist updates, and so on.

**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 unit**
A LPR unit is a type of entity that represents a hardware device dedicated to the capture of license plate numbers. An LPR unit is typically connected to an LPR camera and a context camera. These cameras can be incorporated to the unit or external to the unit.

**M**

**macro**
A macro is a type of entity that encapsulates a C# program that adds custom functionalities to Security Center.

**main server**
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 in order to be part of the same system. In an 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.

**Manufacturer Extension**

Manufacturer extension is the manufacturer specific settings for access control units, video units, and intrusion detection units.

**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**

Map designer is a type of 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**

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 where the main area of the canvas is used to display a geographical map, for the exclusive purpose of showing LPR events.

**Map Object**

Map objects are graphical representations of Security Center entities on your maps. They allow you to interact with your system without leaving your map.

**Map View**

A map view is a defined display position and zoom level for a given 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**

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.

**Media Gateway**

The Media Gateway is a role used by external applications to request live and playback video using the Real Time Streaming Protocol (RTSP), and to receive raw video streams from cameras managed by Security Center systems.

**Media Router**

Media Router is the central role that handles all stream (audio and video) requests 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...
Migration tool
Migration tool is a tool used to migrate Omnicast 4.x systems to Security Center 5. This tool must be executed on every server computer where Omnicast 4.x components are installed.

Mission Control
Mission Control is a Decision Support System that provides organizations with a unified security platform that offers superior situational intelligence, visualization, and complete incident management capabilities. Mission Control guides operators through the incident monitoring and resolution process, allowing them to take control of unusual or undesirable situations, removing emotion from the response and ensuring compliance.

Mobile Admin
Mobile Admin is a web-based administration tool used to configure the Mobile Server.

Mobile app
Mobile app is the client component of Security Center Mobile installed on mobile devices. Mobile app users connect to Mobile Server to receive alarms, view live video streams, view the status of doors, and more, from Security Center.

Mobile Data Computer
Mobile Data Computer is a tablet computer or ruggedized laptop used in patrol vehicles to run the AutoVu 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 is the 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
Mobile Server is the server component of Security Center Mobile that connects Mobile apps and Web Clients to Security Center. The Mobile Server connects to Security Center, and synchronizes the data and video between Security Center and supported Mobile client components.

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
Monitoring is a type of operation task that allows you to monitor and respond to alarms and real time events pertaining to selected entities of interest.

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. |
| **multifactor authentication** | Multifactor 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. |
| **Navigator box** | The Navigator box is Genetec's proprietary in-vehicle device that provides GPS coordinates and odometer readings to Patroller. Because it taps into the vehicle's odometry signal, it is more accurate than a standard GPS device. The Navigator box can be used with any type of AutoVu mobile deployment that requires positioning information, but it is required for City Parking Enforcement with Wheel Imaging. |
| **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 a type of administration task that allows you to configure your networks and servers. |
| **new wanted** | A new wanted is a manually entered hotlist item in Patroller. When you are looking for a plate that does not appear in the hotlists loaded in the 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.

**Omnicast**

Omnicast is the IP video surveillance system of Security Center that provides seamless management of digital video. Omnicast allows for multiple vendors and CODEC (coder/decoder) to be used within the same installation, providing the maximum flexibility when selecting the appropriate hardware for each application.

**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**

Omnicast Federation is a type of role that connects an Omnicast 4.x system to Security Center and imports its entities, so that its cameras and events can be used in your local system.

**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 zone where these restrictions apply.

**P**

**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 zone**

Parking zone is the general concept used to designate the area where a given parking regulation (overtime rule, permit, or permit restriction) is enforced. When used in the context of university parking enforcement, the parking zone must be explicitly defined as a list of parking lots.

**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**

A partition administrator is an authorized user of a partition who has administrative rights over that partition and its members. Partition administrators can add, modify, and delete most entities within their
partitions. This includes users, user groups, and child partitions, with the exception of roles. Partition administrators can modify roles within their partitions, but cannot add or delete roles.

**Patroller**

1. Patroller is the AutoVu software application installed on an in-vehicle computer. Patroller connects to Security Center and is controlled by the LPR Manager. 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. 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 the Patroller software.

**Patroller Config Tool**

Patroller Config Tool is the 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 Patroller.

**Patroller tracking**

Patroller tracking is a type of investigation task that allows you to replay the route followed by a Patroller on a given date on a map, or view the current location of Patroller 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 zone. Permit restrictions are only used by AutoVu Patrollers configured for University Parking Enforcement.

**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 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 is a software module that adds a specific feature or service to a larger system.

Plugin: Plugin is a type of role that hosts a specific plugin.

Plugins: The Plugins task is a type of administration task that allows you to configure plugin-specific roles and related entities.

Point of sale: Point of sale (POS) is a system that typically refers to the hardware and software used for checkouts - the equivalent of an electronic cash register. These systems are used to capture detailed transactions, authorize payments, track inventory, audit sales, and manage employees. Point of sale systems are used in supermarkets, restaurants, hotels, stadiums, casinos, retail establishments.

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.

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 an encryption/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.

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.

**R**

**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.

**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 zone 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.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>redundant archiving</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Remote</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>rendering rate</strong></td>
<td>Rendering rate is the comparison of how fast the workstation renders a video with the speed the workstation receives that video from the network.</td>
</tr>
<tr>
<td><strong>Report Manager</strong></td>
<td>Report Manager is a type of role that automates report emailing and printing based on schedules.</td>
</tr>
<tr>
<td><strong>report pane</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>request to exit</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>reverse geocoding</strong></td>
<td>Reverse geocoding is an AutoVu feature that translates a pair of latitude and longitude into a readable street address.</td>
</tr>
<tr>
<td><strong>role</strong></td>
<td>A role is a software module that performs a specific job within Security Center. Roles must be assigned to one or more servers for their execution.</td>
</tr>
<tr>
<td><strong>roles and units view</strong></td>
<td>The roles and units view is a browser view that lists the roles on your system with the units they control as child entities.</td>
</tr>
<tr>
<td><strong>route</strong></td>
<td>Route is a setting that configures the transmission capabilities between two end points in a network for the purpose of routing media streams.</td>
</tr>
<tr>
<td><strong>S</strong></td>
<td></td>
</tr>
<tr>
<td><strong>same position</strong></td>
<td>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. Patroller must be equipped with GPS capability in order to enforce this type of regulation.</td>
</tr>
<tr>
<td><strong>schedule</strong></td>
<td>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).</td>
</tr>
</tbody>
</table>
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.

Software Development Kit  The Software Development Kit (SDK) allows end-users to develop custom applications or custom application extensions for Security Center.

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 the unified security platform that seamlessly blends Genetec™ security and safety systems within a single innovative solution. The systems unified under Security Center include Genetec™ Omnicast™ IP video surveillance system, Synergis™ IP access control system, and AutoVu™ IP license plate recognition (LPR) system.

Security Center Federation  Security Center Federation is a type of role that connects a remote, independent Security Center system to your local Security Center, so that its entities and events can be used by your local Security Desk users.

Security Center Mobile  Security Center Mobile is a feature of Genetec’s unified platform that lets you remotely connect to your Security Center system over a wireless IP network. Supported Mobile client components include a platform-independent, unified Web Client, as well as various Mobile apps for smartphones and tablets.

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 access (enter or exit) 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’s main systems, Omnicast, Synergis, and AutoVu. Security Desk’s unique task-based design 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 | Secure 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 Genetec Server 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 | Sharing guest is when Security Center system gives the rights to view and modify entities shared by another system.

sharing host | Sharing host is when Security Center system owns partitions that are shared with other Security Center systems.

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).

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 may include new LPR contexts, new firmware, Sharp Portal updates, and updates to the Sharp’s Windows services (Plate Reader, HAL, updater service, and so on).

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

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.

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.

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 (SSO) is the use of a single user authentication across multiple IT systems or even organizations.

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.

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.

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 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.

An SV appliance is a turnkey network security appliance that comes preinstalled with an embedded operating system and Genetec’s
Security Center. 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 sub-compact network security appliance that comes preinstalled with Windows Embedded Standard and Genetec security software. 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-sized network security appliance that comes pre-installed with Windows Embedded Standard and Genetec's Security Center. It enables you to quickly deploy a unified or standalone video surveillance and access control system.

**SV-PRO**

The SV-PRO is a rack-mount appliance that comes preloaded with Genetec security software, and Windows 10 Enterprise LTSB. 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**

Synergis is the IP access control system of the Security Center designed to offer end-to-end IP connectivity, from access control reader to client workstation. Synergis seamlessly integrates a variety of access control capabilities including, but not limited to, badge design, visitor management, elevator control, zone monitoring and more.

**Synergis appliance**

A Synergis appliance is an IP-ready security appliance manufactured by Genetec 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 Genetec’s intelligent and PoE-enabled access control appliance 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 Master Controller**

Synergis Master Controller (SMC) is Genetec's access control appliance 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 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**  
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.

**T**

**tailgating**  
Tailgating is the act of entering a secured area without presenting a credential, by following behind another person who has presented their credential.

**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, dashboard, and Logical view.

**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 Security Desk canvas operating mode where the main area of the canvas is used to display the tiles and the dashboard.

tile pattern
The tile pattern is the arrangement of tiles within the canvas.

tile plugin
A tile plugin is a type of entity that represents an application that runs inside a Security Desk tile.

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
An archive transfer scenario that includes specific settings, such as which cameras or Archivers are included in this transfer, when the archives are transferred, what data is transferred, and so on.

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. Starting with Security Center 5.4 GA the Unit enrollment tool replaces the Unit discovery tool.

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 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 to stay logged on when a threat level is set. The smaller the value, the higher the priority.

User management

The User management task is a type of administration task that allows you to configure users, user groups, and partitions.

V

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 going through a door, license plate recognition, detection of unattended objects, or the direction of people walking or running.

video archive

Video archive includes both the recorded audio and video footage and the database that documents those recordings (source camera, timestamps, events, bookmarks, and so on).

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.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>video sequence</td>
<td>A video sequence is any recorded video stream of a certain duration.</td>
</tr>
<tr>
<td>video stream</td>
<td>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.</td>
</tr>
<tr>
<td>Video</td>
<td>The Video task is a type of administration task that allows you to configure video management roles, units, analog monitors, and cameras.</td>
</tr>
<tr>
<td>video unit</td>
<td>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. Video units are available in a variety of brands and models, some of which support audio and others support wireless communication. 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.</td>
</tr>
<tr>
<td>video watermarking</td>
<td>Video watermarking is the process by which a digital signature (watermark) is added to each recorded video frame to ensure its authenticity. If anyone later tries to make changes to the video (add, delete or modify a frame), the signatures will no longer match, which shows that the video has been tampered with.</td>
</tr>
<tr>
<td>virtual zone</td>
<td>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.</td>
</tr>
<tr>
<td>Visit details</td>
<td>Visit details is a type of investigation task that reports on the stay (check-in and check-out time) of current and past visitors.</td>
</tr>
<tr>
<td>Visitor activities</td>
<td>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).</td>
</tr>
<tr>
<td>visitor escort rule</td>
<td>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 an escort are not granted access through access points until both they and their assigned escort (cardholder) present their credentials within a certain delay.</td>
</tr>
<tr>
<td>Visitor management</td>
<td>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.</td>
</tr>
<tr>
<td>visual tracking</td>
<td>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</td>
</tr>
</tbody>
</table>
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.

**W**

**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.

**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**

Web Client is the client component of Security Center Mobile that provides access to Security Center features from a web browser. Web Client users connect to Mobile Server to configure and monitor various aspects of your Security Center system.

**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.

**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. AutoVu Patroller uses WCF to communicate wirelessly with Security Center.

**Z**

**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 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 zone, and the percentage of occupancy.
Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ Technical Information Site**: The latest documentation is available on the Technical Information Site. To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. 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. Patroller and the Sharp Portal also include context-sensitive help for each screen. 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 Genetec™ customer, you have access to the Genetec™ Technical Information Site, where you can find information and search for answers to your product questions.

- **Genetec™ Technical Information Site:** 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 the Technical Information Site for potential fixes, workarounds, or known issues.
  
  To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. 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: EN_GLM_ASSURANCE and EN_GLM_ADVANTAGE.

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 Genetec™ staff to communicate with each other and discuss a variety of topics, ranging from technical questions to technology tips. You can log in 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.
Index

A
AutoVu deployment 48

B
backing up database manually 92
backward compatibility disabling 50
blocked 12
blocked files 12

C
creating
   Server Admin password 13, 32
   server password 13, 32

D
demo license, acquiring 152
documentation
   Installation and Upgrade Guide 10
   Release Notes 10
document information ii

E
error messages
   blocked 114
   blocked files 114
   unblock 114

F
files
   License.lic 26, 83
   setup.exe 10
   Validation.vk 26, 83
firewalls
   configuring ports 45

G
Genetec Update Service
   basic authentication 97
   closing 97
   connecting 97
   log on 97

I
installation options
   languages 10
   silent mode 10

wizard mode 10
installation packages
   contents 10
installing
   expansion server 32
   main server 13
   Security Center Client 42
   System Availability Monitor 13, 32
   WinPcap 13, 32
installing BeNomad 49
installing hotfix KB2468871 113
installing hotfix KB2494124 113
installing hotfix KB2588507 113
installing Security Center
   postrequisites 53
   prerequisites 2

L
license
   activating 22, 26
   activating from Config Tool 83
   manual activation 26, 83
   web activation 22
license key 26, 83
licensing 152

M
mapping 49
modes
   installation options 10

O
Omnicast
   ports used (default) 46

P
performance issue 113
ports
   AutoVu-specific 48
   prerequisites
      upgrading from an earlier release of Security Center 5.5 57
      upgrading from Security Center 5.2 60
      upgrading from Security Center 5.3 59
      upgrading from Security Center 5.4 58

R
return merchandise authorization RMA 152
returns and repairs 152
S
Security Center
- common ports used 45
Server Admin
- opening 22, 26
silent mode
- install command 101
- installing 101, 103
- installing Genetec server 108, 110
- limitations 99
- option list 101
- preinstallation tasks 99, 100
- prerequisites 99
- Security Center Client 110
- uninstalling Security Center 111
Synergis
- ports used (default) 47

T
technical support, contacting 152
TLS
- backward compatibility 50
troubleshooting
- KB2468871 113
- KB2494124 113
- KB2588507 113
- performance issue 113
- video stability 113

U
unblock 12
uninstalling Security Center components
- from Windows 7 51
- from Windows XP 51
upgrading Directory database 93
upgrading expansion server 90
upgrading main server 88
upgrading Security Center
- from from an earlier release of version 5.4 72
- from version 4.0 78
- from version 5.0 77
- from version 5.1 76
- from version 5.2 75
- from version 5.3 74
- from version 5.4 73
- multiple Directory servers 79
- overview 72, 73, 74, 75, 76, 77, 78
upgrading Security Center Client 91

V
validation key 26, 83
video stability issue 113