Security Center Installation and Upgrade

Guide

5.4 SR2

Click here for the most recent version of this document.
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.
## Contents

**Preface: Preface**

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

**Chapter 1: Installing Security Center**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparing to install Security Center</td>
<td>2</td>
</tr>
<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 5.4 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>25</td>
</tr>
<tr>
<td>Installing Security Center on an expansion server</td>
<td>30</td>
</tr>
<tr>
<td>Connecting expansion servers to the main server</td>
<td>37</td>
</tr>
<tr>
<td>Installing Security Center Client</td>
<td>40</td>
</tr>
<tr>
<td>Default ports used by Security Center</td>
<td>43</td>
</tr>
<tr>
<td>Common communication ports</td>
<td>43</td>
</tr>
<tr>
<td>Omnicast-specific ports</td>
<td>43</td>
</tr>
<tr>
<td>Synergis-specific ports</td>
<td>44</td>
</tr>
<tr>
<td>AutoVu-specific ports</td>
<td>45</td>
</tr>
<tr>
<td>Installing BeNomad</td>
<td>46</td>
</tr>
<tr>
<td>Converting the main server to an expansion server</td>
<td>47</td>
</tr>
<tr>
<td>Converting an expansion server to the main server</td>
<td>48</td>
</tr>
<tr>
<td>Uninstalling Security Center</td>
<td>49</td>
</tr>
<tr>
<td>Completing the installation process</td>
<td>51</td>
</tr>
</tbody>
</table>

**Chapter 2: Upgrading to Security Center 5.4**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported upgrades from earlier versions of Security Center</td>
<td>54</td>
</tr>
<tr>
<td>Preparing to upgrade from an earlier release of Security Center 5.4</td>
<td>55</td>
</tr>
<tr>
<td>Preparing to upgrade from Security Center 5.3 to 5.4</td>
<td>56</td>
</tr>
<tr>
<td>Preparing to upgrade from Security Center 5.2 to 5.4</td>
<td>57</td>
</tr>
<tr>
<td>Preparing to upgrade from Security Center 5.1 to 5.4</td>
<td>58</td>
</tr>
<tr>
<td>Differences between Security Center 5.x and 5.4 partitions</td>
<td>59</td>
</tr>
<tr>
<td>Upgrading the Public partition from 5.x to 5.4</td>
<td>61</td>
</tr>
</tbody>
</table>
Installing Security Center

This section includes the following topics:

- "Preparing to install Security Center" on page 2
- "Security Center 5.4 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 25
- "Installing Security Center on an expansion server" on page 30
- "Installing Security Center Client" on page 40
- "Default ports used by Security Center" on page 43
- "Installing BeNomad" on page 46
- "Converting the main server to an expansion server" on page 47
- "Converting an expansion server to the main server" on page 48
- "Uninstalling Security Center" on page 49
- "Completing the installation process" on page 51
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. 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.
2. Install the latest video and network drivers for your servers and workstations.
3. Make sure that the servers are not domain controllers.
4. Disable the power saving feature on all servers.
5. Make sure that Windows Update is not configured to automatically reboot your servers after installation of updates.
6. 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.
7. Verify the network connections between your servers, workstations, and units.
8. Verify the unicast and multicast network connections and settings.
9. 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.
10. If you are upgrading:
   a) Check the Security Center backward compatibility requirements.
   b) Verify the validity of the upgrade or migration path.
      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.
11. Have your system ID and password in hand to activate your license on the main server. Your System ID and password are found in the Security Center License Information document. Genetec Technical Support sends you this document when you purchase the product.
12. Make sure you have administrative privileges. If not, then the installation setup.exe must be run as administrator.
   You may need to be a Microsoft Windows Domain administrator to access databases and storage on the machines. Check with your IT administrator.
13. Grant the service users all necessary SQL server permissions.
14. (For remote databases) Set up the SQL Server for remote database access.
15. Close Internet Explorer.
16. (Windows 7 only) Activate .NET Framework 3.5.1.
   For Windows 8 and Window 2012, the .NET Framework feature is automatically enabled by the InstallShield Wizard if you have an active Internet connection.
17. (Windows 2012 only) Activate the Media Foundation feature.
18. Download the Security Center installation package.
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 5.4 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 5.4 system requirements, click here.
Installing SQL Server on a separate drive

Depending on your deployment requirements, you can install SQL Server on a separate drive from the OS drive (typically installed on the C: drive). You’ll need to 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.

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: `SQLEXRWT_x64_ENU.exe`.
        - If you are on a 32-bit computer: `SQLEXRWT_x86_ENU.exe`.

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

3. In 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 In 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 In the **Instance Configuration** page, select a name for the SQL Server.

   **NOTE:** The database server name is not case-sensitive, but it must meet 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](https://msdn.microsoft.com/en-us/library/ms189822.aspx).
   - It cannot be longer than 16 characters.
   - The first letter 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 (:), semicolon (;), 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 In the **Server Configuration** page, select the account name for each SQL Server service, and click **Next**.

11 In 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 their Windows credentials, or the specific password you specify here.
12 In the Error Reporting page, specify if you would like to send any 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 84
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' 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 83.

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.

**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 43.
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

ZIP files must be unblocked before their contents are extracted.

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 98
Installing Security Center on the main server

The main server is the only server in your Security Center system that hosts the Directory role. It must be installed 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.

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 server are also installed. The installed software will take care of the creation or the upgrade of all the databases your system requires. You only need to specify the name of your database server. If you don’t 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.

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

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 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, then select the required Omnicast compatibility packs.

6 If necessary, 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 will 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 get a printed 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. This 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 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](https://msdn.microsoft.com/en-us/library/ms189822.aspx).
- It cannot be longer than 16 characters.
- The first letter 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. Moreover, 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 it 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 Server Admin address will need to 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) will automatically include this port.

**CAUTION**: Be careful for conflicts with other software running on the server that may also use port 80. Example: any other web browser.

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

• **Server password/Confirm password**: Leave blank (the default), or type and confirm a new password to open the web-based Server Admin.

**IMPORTANT**: If you lose the server password, then you'll need to call Genetec Technical Support to reset it.

15 Click **Next**.

16 On the **Firewall Rules** page, select **Allow Genetec Security Center 5.4 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’ll also need to 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 will be used by the Genetec Technical support team should you require assistance. 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 will be 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 - 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 update now** option, your Internet browser will open to the Genetec Product Download page on GTAP. You will 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 25)
- [Installing Security Center on an expansion server](on page 30)
Activating Security Center license using the web

The Security Center license is activated on the main server. You have to 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 25.

- **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 was 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 main server, and
     *port* is the web server port specified during the Security Center Server installation.
     
     You may omit the web server port if you are using the default value (80).
   - If connecting to Server Admin from the local host, then double-click **Genetec Server Admin** in the **Genetec Security Center 5.4** folder in the Windows Start menu.

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

3. In the **License** dialog box, click **Modify license**.
4 In the License management dialog box, click Web activation.

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

**NOTE:** To reset the system password, click Reset system password on the System Information page on GTAP.

6 Click Activate.

The details of your license appear in the License dialog box.
7 Click Save to close the License dialog box.
8 Close the browser window.
Activating Security Center license without Internet access

The Security Center license is activated on the main server. You have to 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 both 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 was 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 main server, and `port` is the web server port specified during the Security Center Server installation.
     You may omit the web server port if you are using the default value (80).
   - If connecting to Server Admin from the local host, then double-click **Genetec Server Admin** in the Genetec Security Center 5.4 folder in the Windows Start menu.

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

3. In the License dialog box, click **Modify license**.
4 In the License management dialog box, click Validation key > 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 thus generated can only be applied to the server identified by the validation key.

5 In the Save As dialog box, browse to a location that you can access from another computer (this can be a USB key) that has Internet access, enter a name you can easily remember as File name, and click Save.

**BEST PRACTICE:** To help you remember the file name, use the name of your server.

A text file with the .vk extension is created.

6 From another computer with Internet access, log on to GTAP at: https://gtap.genetec.com
7 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.

8 Scroll down to the **License information** section and click **Activate license**.
9 In the dialog box that opens, browse to your validation key (.vk file), and click **Submit**. The message **License activation successful** appears.

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

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

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

13 In the **Manual activation** 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**.
14 Click **Activate**.

The details of your license appear in the **License** dialog box.

15 Click **Save** to close the **License** dialog box.

16 Close the 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.

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

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 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, then select the required Omnicast compatibility packs.

6 If necessary, 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**.
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. This 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 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 letter 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. Moreover, 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 it to connect to.

12 Click Next.

13 On the Server Parameters page, enter the following fields:
Installing Security Center

• **Web server port**: The HTTP port that is used for the web-based Server Admin. If you change the default port, then Server Admin address will need to 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) will automatically include this port.

  **CAUTION**: Be careful for conflicts with other software running on the server that may also use port 80. Example: any other web browser.

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

• **Server password/Confirm password**: Leave blank (the default), or type and confirm a new password to open the web-based Server Admin.

  **IMPORTANT**: If you lose the server password, then you'll need to 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 used to configure the main server.

16 On the **Firewall Rules** page, select **Allow Genetec Security Center 5.4 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’ll also need to 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 will be used by the Genetec Technical support team should you require assistance. 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:
36

• **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 will be prompted to confirm the identity of the Directory server.

  For more information on Directory authentication, see the *Security Center Administrator Gude*.

• **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 - **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 update now option, your Internet browser will open to the Genetec Product Download page on GTAP. You will 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

If you need to change the connection parameters you set during an expansion server installation, you must connect that expansion server to the main server. Or, if you have just converted an expansion server to the main server, you must connect all the other expansion servers on your system to the new main server.

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 main server, and port is the web server port specified during the Security Center Server installation.
     You may omit the web server port if you are using the default value (80).
   - If connecting to Server Admin from the local host, then double-click Genetec Server Admin in the Genetec Security Center 5.4 folder in the Windows Start menu.

2 Enter the server password that you set during the main server installation, and click Log on.
3 Under **Main server connection** in the Genetec Server page of the Server Admin, type the following information:

- **Security Center Directory**: The main server’s DNS name (or IP address).
- **Password**: The password to log on to the Server Admin on the main server. This password was specified during the main server installation.

4 If **is enabled on this machine, and your Directory certificate is not signed by a trusted**, you need to verify and accept the certificate.

**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. For more information, see [What is Directory authentication?](#).

5 Click **View certificate details** to verify the authenticity of the certificate.
**TIP:** If in doubt, you can send the thumbprint of the certificate to your IT department for verification.

6 Click **Accept certificate** to trust the main server.

**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.

7 Click **Apply**.

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.

**Related Topics**

*Converting an expansion server to the main server* on page 48
Installing Security Center Client

The Security Center Client installation option installs Config Tool and Security Desk. By default, both client applications are installed.

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.

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

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 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, then select the required Omnicast compatibility packs.
6 If necessary, 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 5.4 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’ll also need to 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 will be 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 - 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></td>
<td>Directory connection requests</td>
</tr>
<tr>
<td>Client workstations</td>
<td>TCP 5500</td>
<td></td>
<td>Directory connection requests</td>
</tr>
<tr>
<td>(Security Desk and Config Tool)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client workstations</td>
<td>TCP 443</td>
<td></td>
<td>Communication with GTAP for SMA validation/sending feedback</td>
</tr>
<tr>
<td>(Config Tool)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All servers</td>
<td>TCP 5500</td>
<td>TCP 5500</td>
<td>Communication between servers</td>
</tr>
<tr>
<td></td>
<td>TCP 4502</td>
<td>TCP 4502</td>
<td>Backward and Silverlight communication</td>
</tr>
<tr>
<td></td>
<td>HTTP 80</td>
<td></td>
<td>Connection via Server Admin</td>
</tr>
<tr>
<td>Servers upgraded from an earlier version</td>
<td>TCP 4503</td>
<td>TCP 4503</td>
<td>Communication with servers of an earlier version</td>
</tr>
<tr>
<td>Intrusion Manager</td>
<td>TCP 3001</td>
<td>TCP 3001</td>
<td>Bosch intrusion panels</td>
</tr>
<tr>
<td>REST service</td>
<td>TCP 4592</td>
<td>TCP 4592</td>
<td>Communication between System Availability Monitor Agent (SAMA) and Directory server</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</th>
<th>Outbound</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>
</tbody>
</table>
### Computer

<table>
<thead>
<tr>
<th>Inbound</th>
<th>Outbound</th>
<th>Port usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP 15000–16000</td>
<td>UDP 15000–16000</td>
<td>Live unicast audio and video streams</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td></td>
<td>Vendor specific ports for events and unit discovery</td>
</tr>
<tr>
<td>UDP 47806</td>
<td>UDP 47806</td>
<td>Live multicast audio and video streams</td>
</tr>
<tr>
<td>UDP 47807</td>
<td>UDP 47807</td>
<td>Live multicast audio and video streams</td>
</tr>
<tr>
<td>TCP 554 or HTTP 80</td>
<td></td>
<td>Typical port used to request video from a unit</td>
</tr>
<tr>
<td>Telnet 5602</td>
<td></td>
<td>Telnet Console connection requests</td>
</tr>
<tr>
<td><strong>Auxiliary</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Archiver</strong></td>
<td>TCP 558</td>
<td>Playback stream requests</td>
</tr>
<tr>
<td><strong>Media Router</strong></td>
<td>TCP 554</td>
<td>Live and playback stream requests</td>
</tr>
<tr>
<td><strong>Redirector</strong></td>
<td>TCP 560</td>
<td>Live and playback stream requests</td>
</tr>
<tr>
<td></td>
<td>UDP 8000–12000</td>
<td>Live unicast audio and video streams</td>
</tr>
<tr>
<td></td>
<td>UDP 47806</td>
<td>Live multicast audio and video streams</td>
</tr>
<tr>
<td></td>
<td>TCP 555</td>
<td>Communication with Archiver</td>
</tr>
<tr>
<td><strong>RTSP Media Router</strong></td>
<td>TCP 654</td>
<td>Live and playback stream requests</td>
</tr>
<tr>
<td></td>
<td>UDP 51914</td>
<td>Live multicast audio and video streams</td>
</tr>
<tr>
<td><strong>Omnicast Federation</strong></td>
<td>UDP 1024-2048</td>
<td>Security Desk when viewing video from an Omnicast Federation in Security Center</td>
</tr>
<tr>
<td><strong>Client workstations</strong></td>
<td>UDP 6000–6500</td>
<td>Live unicast audio and video streams</td>
</tr>
<tr>
<td>(Security Desk and Config Tool)</td>
<td>UDP 47806</td>
<td>Live multicast video streams</td>
</tr>
<tr>
<td></td>
<td>UDP 47807</td>
<td>Live multicast audio streams</td>
</tr>
<tr>
<td></td>
<td>TCP 554–560</td>
<td>Live and playback audio and video requests</td>
</tr>
</tbody>
</table>

1 Additional Archiver roles created on the same server will use port numbers that are incremented by 5000. For example, the second Archiver role will use ports 20000-21000, the third one will use ports 25000-26000, and so on.

### Synergis-specific ports

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

---

1 Additional Archiver roles created on the same server will use port numbers that are incremented by 5000. For example, the second Archiver role will use ports 20000-21000, the third one will use ports 25000-26000, and so on.
Computer | Inbound | Outbound | Port usage
--- | --- | --- | ---
Access Manager | UDP/TCP 4070 | UDP/TCP 4070 | HID VertX/Edge controllers
 |  |  | HID Vertx/Edge EVO controllers
TCP 20 | TCP 21, 23 | HID VertX/Edge controllers
TCP 4050 |  | HID VertX/Edge controllers
 |  | HID Vertx/Edge EVO controllers
TCP 22 |  | HID Vertx/Edge EVO controllers
TCP 2000 | Default Synergis unit discovery port (this port can be modified in Config Tool)

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>Fixed Sharp unit discovery</td>
<td></td>
</tr>
<tr>
<td>TCP 8731</td>
<td>Fixed Sharp units and Patrollers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP 8832</td>
<td>Patroller hotfix requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP 8787</td>
<td>Pay-by-Plate</td>
<td></td>
<td></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 5.4.

3. Copy the .glic license file from the email to the BeNomad folder.
   
   BeNomad maps are enabled when you start Security Center.
Converting the main server to an expansion server

When a computer comes pre-installed with Security Center, the main server configuration is always used by default. You might need to convert a main server to an expansion server, because only one main server is allowed per system.

**Before you begin**

You must have another main server installed to connect to before disabling your current main server. For more information about installing Security Center on a main server, see the Security Center Installation and Upgrade Guide.

**What you should know**

You convert the main server to an expansion server by deactivating the Directory role using Server Admin, but you must log on to Server Admin from a web browser. The conversion cannot be done if you log on to Server Admin from Config Tool, because you must stay connected to the Directory.

**CAUTION:** This operation will restart the Genetec Server service, which means you’ll have to log on to Server Admin again to connect the new expansion server to the main server.

**To convert the main server to an expansion server:**

1. Log on to Server Admin on your computer using a web browser.
2. In the Server Admin page, click the Genetec Server tab.
3. Scroll to the bottom of the browser page and click Deactivate Directory.
4. Open a web browser, and enter “http://machine/Genetec” in the address bar, where machine is the DNS name or the IP address of your server.
5. Log on again to Server Admin.
   This time, the Directory tab should not appear.
6. Scroll to the Main server connection section, and configure the name and password of the main server it is supposed to connect to.
7. Click Apply.

**Related Topics**

Installing Security Center on the main server on page 13
Converting an expansion server to the main server

You can convert an expansion server into the main server, either to replace your existing main server or to start a brand new system.

What you should know

You can only convert an expansion server to a main server when you log on to Server Admin from a web browser. The conversion cannot be done if you log on to Server Admin from Config Tool, because you must stay connected to the Directory.

CAUTION: This operation restarts the Genetec Server service, which means you’ll have to log on to Server Admin again to activate the software license on the newly converted server.

To convert an expansion server to the main server:

1. Log on to Server Admin on your computer using a web browser.
2. In the Server Admin page, click the Genetec Server tab.
   The Genetec Server service restarts.
4. Open a web browser, and enter http://machine/Genetec in the address bar, where machine is the DNS name or the IP address of your server.
5. Log on again to Server Admin.
   The Directory tab should now be available.
6. Activate the software license on the new main server.
7. Click Apply.
8. If you are replacing an existing main server, configure the Database settings so that this server connects to your existing Directory database.

After you finish

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

Related Topics
Activating Security Center license using the web on page 22
Connecting expansion servers to the main server on page 37
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 5.4 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 5.4 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 5.4, 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 5.4
    - On 64-bit systems: C:\Program Files (x86)\Genetec Security Center 5.4
    - On all systems:
      - C:\ProgramData\Genetec Security Center
      - C:\ProgramData\Genetec Security Center 5.4
      - C:\ProgramData\Genetec Update Service
      - C:\ProgramData\AppData\Local\Genetec Security Center 5.4
      - C:\Users\<username>\AppData\Local\Genetec Inc
      - C:\Users\<username>\AppData\Local\Genetec Security Center 5.4
      - 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 5.4

This section includes the following topics:

- "Supported upgrades from earlier versions of Security Center" on page 54
- "Preparing to upgrade from an earlier release of Security Center 5.4" on page 55
- "Preparing to upgrade from Security Center 5.3 to 5.4" on page 56
- "Preparing to upgrade from Security Center 5.2 to 5.4" on page 57
- "Preparing to upgrade from Security Center 5.1 to 5.4" on page 58
- "Differences between Security Center 5.x and 5.4 partitions" on page 59
- "Upgrading the Public partition from 5.x to 5.4" on page 61
- "Backward compatibility requirements for Security Center" on page 62
- "Supported federations for Security Center 5.4 SR2" on page 66
- "Upgrading from an earlier release of Security Center 5.4" on page 67
- "Upgrading from Security Center 5.3 to 5.4" on page 68
- "Upgrading from Security Center 5.2 to 5.4" on page 69
- "Upgrading from Security Center 5.1 to 5.4" on page 70
- "Upgrading from Security Center 5.0 to 5.4" on page 71
- "Upgrading from Security Center 4.0 to 5.4" on page 72
- "Upgrading the main server" on page 73
- "Upgrading expansion servers" on page 74
- "Upgrading Security Center Client" on page 75
- "Back up databases" on page 76
- "Upgrading the Directory database" on page 77
- "Shrinking Security Center databases after an upgrade" on page 79
- "About the Genetec Update Service" on page 80
- "Logging on to the Genetec Update Service" on page 81
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 5.4 SR2.

- Security Center 5.1 GA/SR1/SR2/SR3
- Security Center 5.3 GA/SR1/SR2/SR3/SR4
- Security Center 5.4 GA

**NOTE:** The upgrade from the Security Center 5.0 version is a two-step procedure. You have to first upgrade to Security Center 5.3 and then upgrade to 5.4.
Preparing to upgrade from an earlier release of Security Center 5.4

If you need to upgrade from an earlier release of Security Center 5.4 to 5.4 SR2, you must prepare the following.

**What you should know**

To prepare to upgrade from an earlier release of Security Center 5.4 to 5.4 SR2:

- 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 5.4 SR2.
Preparing to upgrade from Security Center 5.3 to 5.4

If you need to upgrade your 5.3 system to 5.4, 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 remembered when 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 5.4:

1. If you are running Microsoft SQL Server 2005, install a more recent version of the database server. Security Center 5.4 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.

2. 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 5.4.

3. (AutoVu only) The MatchersSettings.xml file is overwritten during the upgrade. Back up the current MatchersSettings.xml file to another location on your system, so you can use it as a reference to reconfigure the overwritten file.

4. If you have HID EVO units in your system, the VertXConfig.gconfig file is not copied during the upgrade. Save a copy of the VertXConfig.gconfig file, if it exists in your Security Center 5.x program files folder, so you can copy it to the 5.4 folder after the software upgrade.

5. If you have an Active Directory role in your current system, make sure 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, then 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 5.4

If you need to upgrade your 5.2 system to 5.4, 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 remembered when 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 5.4:**

1. If you are running Microsoft SQL Server 2005, install a more recent version of the database server. Security Center 5.4 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.

2. 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 5.4.

3. (AutoVu only) The `MatchersSettings.xml` file is overwritten during the upgrade. Back up the current `MatchersSettings.xml` file to another location on your system, so you can use it as a reference to reconfigure the overwritten file.

4. If you have HID EVO units in your system, the `VertXConfig.gconfig` file is not copied during the upgrade. Save a copy of the `VertXConfig.gconfig` file, if it exists in your Security Center 5.x program files folder, so you can copy it to the 5.4 folder after the software upgrade.

5. If you have an Active Directory role in your current system, make sure 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, then 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 5.1 to 5.4

If you need to upgrade your 5.1 system to 5.4, 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 remembered when 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 5.1 to 5.4:**

1. If you are running Microsoft SQL Server 2005, install a more recent version of the database server. Security Center 5.4 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.

2. 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 5.4.

3. (AutoVu only) The MatchersSettings.xml file is overwritten during the upgrade. Back up the current MatchersSettings.xml file to another location on your system, so you can use it as a reference to reconfigure the overwritten file.

4. If you have HID EVO units in your system, the VertXConfig.gconfig file is not copied during the upgrade. Save a copy of the VertXConfig.gconfig file, if it exists in your Security Center 5.x program files folder, so you can copy it to the 5.4 folder after the software upgrade.

5. If you have an Active Directory role in your current system, make sure the Windows user configured to connect to the Windows Active Directory has read access to the accountExpires attribute.

**CAUTION:** If the Windows user does not have read access to the accountExpires attribute, then 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 Security Center 5.x and 5.4 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 or higher:

**NOTE:** For more information on creating and configuring partitions in Security Center 5.4, see the Security Center Administrator Guide.

<table>
<thead>
<tr>
<th>Security Center 5.0, 5.1, or 5.2</th>
<th>Security Center 5.3 or 5.4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Terminology</strong></td>
<td></td>
</tr>
<tr>
<td>• Accepted users</td>
<td>• Authorized users</td>
</tr>
<tr>
<td>• Partition manager</td>
<td>• Partition administrator</td>
</tr>
<tr>
<td><strong>Security configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Security task: Allows you to</td>
<td>User management task:</td>
</tr>
<tr>
<td>configure users, user groups,</td>
<td>configure users, user</td>
</tr>
<tr>
<td>and partitions in three</td>
<td>groups, and partitions</td>
</tr>
<tr>
<td>separate tabs.</td>
<td>within a single entity</td>
</tr>
<tr>
<td><strong>Partition configuration</strong></td>
<td></td>
</tr>
<tr>
<td>• Can only be created in the</td>
<td>• Can be created from any</td>
</tr>
<tr>
<td>Partitions tab of the Security</td>
<td>administration task where</td>
</tr>
<tr>
<td>task in Config Tool.</td>
<td>an entity hierarchy is</td>
</tr>
<tr>
<td>• Partitions are always shown</td>
<td>shown. Users can choose</td>
</tr>
<tr>
<td>in the Partitions tab of the</td>
<td>to show or hide</td>
</tr>
<tr>
<td>Security task in Config Tool.</td>
<td>partitions in any</td>
</tr>
<tr>
<td>• The content of a partition</td>
<td>administration tasks</td>
</tr>
<tr>
<td>can only be modified in the</td>
<td>by clicking Show</td>
</tr>
<tr>
<td>partition’s Properties tab.</td>
<td>partitions ( ) in the</td>
</tr>
<tr>
<td></td>
<td>Search box. Partitions</td>
</tr>
<tr>
<td></td>
<td>are completely hidden if</td>
</tr>
<tr>
<td></td>
<td>no user-created partitions</td>
</tr>
<tr>
<td></td>
<td>exist.</td>
</tr>
<tr>
<td><strong>Partition access rights</strong></td>
<td></td>
</tr>
<tr>
<td>configuration</td>
<td></td>
</tr>
<tr>
<td>• Users’ access rights for</td>
<td>• Users’ access rights for</td>
</tr>
<tr>
<td>partitions are configured in the</td>
<td>partitions are configured</td>
</tr>
<tr>
<td>Accepted users tab of each</td>
<td>in the Access rights tab</td>
</tr>
<tr>
<td>partition entity.</td>
<td>of each individual user</td>
</tr>
<tr>
<td>• Access rights are implicitly</td>
<td>and user group entity.</td>
</tr>
<tr>
<td>inherited from parent user</td>
<td>• Access rights are</td>
</tr>
<tr>
<td>groups. User group members have</td>
<td>explicitly inherited</td>
</tr>
<tr>
<td>access to the partition even</td>
<td>from parent user groups</td>
</tr>
<tr>
<td>though they are not shown in</td>
<td>and are clearly indicated</td>
</tr>
<tr>
<td>the Accepted users tab.</td>
<td>in the user’s Access</td>
</tr>
<tr>
<td>• Access rights granted for</td>
<td>rights tab.</td>
</tr>
<tr>
<td>a parent partition are also</td>
<td>• Access rights granted for</td>
</tr>
<tr>
<td>granted for the child partitions.</td>
<td>a parent partition are</td>
</tr>
<tr>
<td></td>
<td>granted by default for</td>
</tr>
<tr>
<td></td>
<td>the child partitions, but</td>
</tr>
<tr>
<td></td>
<td>can be denied on a case</td>
</tr>
<tr>
<td></td>
<td>by case basis.</td>
</tr>
</tbody>
</table>

Upgrading to Security Center 5.4
## Partition membership configuration

<table>
<thead>
<tr>
<th>Security Center 5.0, 5.1, or 5.2</th>
<th>Security Center 5.3 or 5.4</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>

---

### Public partition

- 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.
- 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 5.4, the **Public partition** is migrated, but the features of the **Public partition** in 5.4 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 5.4.
  - You can rename, modify and delete the **Public partition** in 5.4.

### 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 5.4

After upgrading a Security Center 5.0, 5.1, or 5.2 system that uses multiple partitions to 5.4, 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 5.4. This does not apply if you are upgrading from 5.3 to 5.4.

Before you begin

- Upgrade Security Center Server to 5.4.
- Upgrade Security Center Client to 5.4.

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 5.4, 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 5.4.
- You can rename, modify and delete the Public partition in 5.4.

To ensure that all users have the access rights they need after an upgrade from 5.x to 5.4:

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 5.4, 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 5.4 SR2 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 5.4 SR2, 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 5.4 SR2, you must upgrade all Directory servers to 5.4 SR2.

• **SQL Server:** Because Security Center 5.4 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 5.4 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>5.4 role</th>
<th>Backward compatible with 5.1 through 5.3</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>Auxilliary 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>Yes</td>
</tr>
<tr>
<td>Intrusion Manager</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Backward Compatibility with Security Center Tasks

The Security Center 5.4 tasks that are backward compatible with Security Desk 5.2 and 5.3 are summarized in the following table.

<table>
<thead>
<tr>
<th>Task Category</th>
<th>Task Type</th>
<th>Backward compatible with Security Desk 5.1 through 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Monitoring²</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><strong>Alarm Management</strong></td>
<td>Alarm monitoring</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Alarm report</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Investigation</strong></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 5.1 through 5.3</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 (Mutli-region)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Reads</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Reads (Mutli-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 5.1 through 5.3</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>

*Includes live video and playback video.*
Supported federations for Security Center 5.4 SR2

Security Center 5.4 SR2 can federate and be federated with other Security Center systems running different versions.

Security Center 5.4 can federate the following:

- Security Center 5.4, 5.3, and 5.2 systems.
- Omnicast 4.6, 4.7 and 4.8 systems.
- Stratocast 1.6 systems.

Security Center 5.4 can be federated by the following:

- Security Center 5.3 and 5.4 systems.

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

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

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

To have the latest release of Security Center 5.4, you can upgrade from an earlier release of 5.4 to SR2 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.

The InstallShield Wizard automatically detects an earlier version of Security Center and upgrades it to Security Center 5.4.

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 to release 5.4 SR2:

1. Install Security Center 5.4 SR2 on your main server.
2. Install Security Center 5.4 SR2 on your expansion servers, according to your priorities.
3. Install Security Center Client 5.4 SR2 on your client workstations, according to your priorities.

After you finish

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

**TIP:** Configure one unit with the required synchronization settings, then use the Copy configuration tool to set the same settings on multiple units.
Upgrading from Security Center 5.3 to 5.4

To have the latest version of Security Center, you can upgrade from your 5.3 system to 5.4 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 5.3 to 5.4:

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 5.2 to 5.4

To have the latest version of Security Center, you can upgrade from your 5.2 system to 5.4 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.
- 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 will be moved to the *root* partition after the upgrade to 5.4, and all partitions will be hidden. All users will have access to the *root* partition.

If partitions other than the *Public partition* were used in your old system, then all old partitions will be migrated to 5.4 with the same content and same accepted users (called *authorized users* in 5.4).

Moreover:

- All entities that were hidden in 5.x will be moved to the *root* partition in 5.4.
- Only the administrators will 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 5.4.

**To upgrade from Security Center 5.2 to 5.4:**

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 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 5.1 to 5.4

To have the latest version of Security Center, you can upgrade from your 5.1 system to 5.4 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.
- 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 will be moved to the root partition after the upgrade to 5.4, and all partitions will be hidden. All users will have access to the root partition.

If partitions other than the Public partition were used in your old system, then all old partitions will be migrated to 5.4 with the same content and same accepted users (called authorized users in 5.4).

Moreover:

- All entities that were hidden in 5.x will be moved to the root partition in 5.4.
- Only the administrators will 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 5.4.

To upgrade from Security Center 5.1 to 5.4:

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 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 5.0 to 5.4

Direct upgrades from Security Center 5.0 to 5.4 are not supported. First you need to upgrade your system to Security Center 5.3, and then to 5.4.

To upgrade from Security Center 5.0 to 5.4:
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 5.4.
3. Upgrade to Security Center 5.4.
Upgrading from Security Center 4.0 to 5.4

Direct upgrades from Security Center 4.0 to 5.4 are not supported. First you need to upgrade your system to Security Center 5.2, and then to 5.4.

To upgrade from Security Center 4.0 to 5.4:

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 5.4.
3. Upgrade to Security Center 5.4.
Upgrading the main server

The main server in your current Security Center system must be upgraded first. You’ll have to apply a new license and upgrade the Directory database.

**Before you begin**

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

**What you should know**

You need the 5.4 Config Tool to connect it to the 5.4 Directory. If Security Center Client were installed on the main server, upgrade it at the same time.

**NOTE:** Client upgrade from version 5.1 to Security Center 5.4 is not supported. Security Center 5.4 Client is installed side-by-side with previous Security Center Client versions, and then 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 will have to reboot after completing the upgrade.

**To upgrade the main server:**

- Install Security Center 5.4 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 5.4.

**After you finish**

Activate your new Security Center 5.4 license.

**Related Topics**

- Activating Security Center license using the web on page 22
- Activating Security Center license without Internet access on page 25
- Preparing to upgrade from Security Center 5.3 to 5.4 on page 56
- Preparing to upgrade from Security Center 5.2 to 5.4 on page 57
- Preparing to upgrade from Security Center 5.1 to 5.4 on page 58
- Backing up databases on page 76
Upgrading expansion servers

You can upgrade expansion servers by installing Genetec Server onto them and letting the InstallShield Wizard do the rest.

Before you begin

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

What you should know

If a reboot warning message appears during the upgrade, accept the message and continue with the upgrade procedure. You will have to reboot after completing the upgrade.

To upgrade an expansion server:

1. Install Security Center 5.4 on your expansion server.
   - Use the Expansion server installation type.
   - The InstallShield Wizard automatically detects an earlier version of Security Center and upgrades it to Security Center 5.4.
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 may need to upgrade the Directory database.

Related Topics

Back up databases on page 76
Upgrading Security Center Client

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

**What you should know**

Client upgrade from version 5.1 to Security Center 5.4 is not supported. Security Center 5.4 Client is installed side-by-side with previous Security Center Client versions, and then you can delete the older version.

**To upgrade from Security Center 5.1 to 5.4:**

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

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

**To upgrade from Security Center 5.2 or 5.3 to 5.4:**

1. **Install Security Center Client.**

   The InstallShield Wizard automatically detects an earlier version of Security Center and upgrades it to Security Center 5.4.
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 Directory tab of the Server Admin connected to the main server. 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 Directory database

After upgrading Security Center, you must also upgrade the Directory database.

To upgrade the Directory database:

1. Open Server Admin, and click Directory.

2. In the Database section, click Update database.

   After the upgrade is complete, the Directory status indicates Directory started, and the database status indicates Database connected.

3. Close the Web browser, and then log on to Config Tool.

4. Open the System task, and click Roles.

5. Select the Archiver role, and click Resources.

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

7 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've 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) and Transaction Log Truncation.

To shrink a database:

1. Follow the procedure 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 81.
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 83
- "Preparing to perform a silent installation" on page 84
- "Silent install command for Security Center" on page 85
- "Installer (MSI) options" on page 87
- "Sample Security Center Server installation commands" on page 92
- "Sample Security Center Client installation commands" on page 94
- "Uninstalling Security Center in silent mode" on page 95
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") 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 contains spaces. If not specified, the default is &lt;ProgramFiles&gt;\Genetec Security Center 5.4, where &lt;ProgramFiles&gt; is either %PROGRAMFILES% or %PROGRAMFILES(X86)%%, depending on the version of your 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 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>• Comp Packs,Comp Pack 4x[,Comp Pack 4x] (Omnicast compatibility packs, you must 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 with no user interaction.</td>
</tr>
</tbody>
</table>
### Setup option

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>/debuglog&lt;FilePath&gt;</strong></td>
<td>Enables the creation of the debug log file and specifies the file path.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> The folder path specified in <code>&lt;FilePath&gt;</code> must exist. The setup program will not create it.</td>
<td><strong>EXAMPLE:</strong> <code>/debuglog&quot;C:\DebugLog.log&quot;</code></td>
</tr>
<tr>
<td><strong>/log&lt;FolderPath&gt;</strong></td>
<td>Enables the creation of log files and specifies the folder path.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> The <code>&lt;FolderPath&gt;</code> must exist. The setup program will not create it.</td>
<td><strong>EXAMPLE:</strong> <code>/log&quot;C:\AllMyLogFiles&quot;</code></td>
</tr>
<tr>
<td><strong>/language:</strong></td>
<td>Sets the language used by the installation program. Immediately precedes the four-digit language code. No space is allowed.</td>
</tr>
<tr>
<td><strong>EXAMPLES</strong></td>
<td></td>
</tr>
<tr>
<td>• <code>/language:1033</code> for English (DEFAULT)</td>
<td></td>
</tr>
<tr>
<td>• <code>/language:3084</code> for French</td>
<td></td>
</tr>
<tr>
<td><strong>&lt;msi_options&gt;</strong></td>
<td>Sets the Security Center Installer (MSI) option list.</td>
</tr>
<tr>
<td>Each option in the list uses the following syntax:</td>
<td></td>
</tr>
<tr>
<td><code>&lt;option&gt;</code>=&lt;value_list&gt; where <code>&lt;option&gt;</code> is an option name, and <code>&lt;value_list&gt;</code> 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 (<code>\</code>).</td>
<td><strong>Example</strong>: <code>msi_options&quot;=option1=value1,option2=value2,option3=value3&quot;</code></td>
</tr>
</tbody>
</table>
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>
<tbody>
<tr>
<td>SERVER_TYPE</td>
<td>Specify whether to install a main or an expansion server. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Main: Install Genetec Server with Directory (DEFAULT)</td>
</tr>
<tr>
<td></td>
<td>• Expansion: Install Genetec Server without Directory</td>
</tr>
<tr>
<td>SQLSERVER_GROUP</td>
<td>Specify if a new or an existing SQL server is silently installed. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• NewServer (must be used with SQL_INSTANCE_NAME)</td>
</tr>
<tr>
<td></td>
<td>• ExistingServer (DEFAULT)</td>
</tr>
<tr>
<td>SQL_INSTANCE_NAME</td>
<td>Specify the new SQL Server instance's name. This option needs to be specified when SQLSERVER GROUP has a value of NewServer.</td>
</tr>
<tr>
<td>GLOBAL_SERVER</td>
<td>Specify the database server name for all roles installed by default. When omitted, the default value is (local) \ SQLEXPRESS. EXAMPLE: GLOBAL_SERVER=BLADE32\SQLServerEnterprise</td>
</tr>
<tr>
<td>DATABASE_SERVER</td>
<td>Same as GLOBAL_SERVER option. This parameter maintains backward compatibility with previous silent installation scripts.</td>
</tr>
<tr>
<td>DATABASE_INSTANCE</td>
<td>Used in conjunction with the BACKUP_DATABASE option. Specify the instance name of the Directory database, if different from the default.</td>
</tr>
<tr>
<td>UPGRADE_DATABASE</td>
<td>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</td>
</tr>
<tr>
<td>Installer (MSI) option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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.</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.</td>
</tr>
<tr>
<td>SERVICEUSERNAME</td>
<td>Specify the username to use in the services.</td>
</tr>
<tr>
<td>SERVICEPASSWORD</td>
<td>Specify the password to use in the services.</td>
</tr>
<tr>
<td></td>
<td>User and password need to be created first with the right credentials prior to using those properties. If not specified, the default is blank.</td>
</tr>
<tr>
<td>SERVERADMIN_PORT</td>
<td>Specify the HTTP port for the web-based Server Admin.</td>
</tr>
<tr>
<td></td>
<td>If not specified, the default is 5500.</td>
</tr>
<tr>
<td>SERVERADMIN_PASSWORD</td>
<td>Specify the password for the web-based Server Admin.</td>
</tr>
<tr>
<td></td>
<td>If not specified, the default is blank.</td>
</tr>
</tbody>
</table>
### Installer (MSI) option

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LANGUAGECHOSEN</strong> Language used by Security Center. The possible code values are:</td>
</tr>
<tr>
<td>• Arabic - 1025</td>
</tr>
<tr>
<td>• Chinese (Simplified) - 2052</td>
</tr>
<tr>
<td>• Chinese (Traditional) - 1028</td>
</tr>
<tr>
<td>• Czech - 1029</td>
</tr>
<tr>
<td>• Dutch - 1043</td>
</tr>
<tr>
<td>• English - 1033</td>
</tr>
<tr>
<td>• French - 3084</td>
</tr>
<tr>
<td>• German - 1031</td>
</tr>
<tr>
<td>• Hebrew - 1037</td>
</tr>
<tr>
<td>• Hungarian - 1038</td>
</tr>
<tr>
<td>• Italian - 1040</td>
</tr>
<tr>
<td>• Japanese - 1041</td>
</tr>
<tr>
<td>• Korean - 1042</td>
</tr>
<tr>
<td>• Norwegian - 1044</td>
</tr>
<tr>
<td>• Persian - 1065</td>
</tr>
<tr>
<td>• Polish - 1045</td>
</tr>
<tr>
<td>• Brasilian Portuguese - 2070</td>
</tr>
<tr>
<td>• Russian - 1049</td>
</tr>
<tr>
<td>• Spanish - 1034</td>
</tr>
<tr>
<td>• Swedish - 1053</td>
</tr>
<tr>
<td>• Thai - 1054</td>
</tr>
<tr>
<td>• Turkish - 1055</td>
</tr>
<tr>
<td>• Vietnamese - 1066</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WEBSERVER_PORT</strong> Specify the HTTP port for the web-based Server Admin.</td>
</tr>
<tr>
<td>If not specified, the default is 80.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CREATE_FIREWALL_RULES</strong> Add the installed Security Center applications to the Windows Firewall exceptions list. Possible values are 0 or 1.</td>
</tr>
<tr>
<td>• 0 = Do not create firewall rules</td>
</tr>
<tr>
<td>• 1 = Create firewall rules (DEFAULT)</td>
</tr>
</tbody>
</table>

**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 |
| MAINSERVER_PASSWORD    | Used for expansion server installation. Specify password for the main server.  
If not specified, the default is blank. |
| 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>
</table>
| **REBOOT**             | This option allows you to force or suppress a reboot after the Server installation has ended. Possible values are:  
- **F** - To force a reboot when your installation is complete.  
- **S** - To suppress any reboot except the one caused by the ForceReboot action.  
- **R** - To suppress any reboot caused by Windows Installer actions. (DEFAULT) |
| **SKIPSERVICESTART**   | 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.  
**EXAMPLE:** SKIPSERVICESTART=Y |
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:"C:" /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 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 97
- "Troubleshooting: Files remain blocked after unblocking them manually" on page 98
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 from 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 one after another, the hotfixes you've downloaded, 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
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) document.

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.