Security Center
Installation and Upgrade Guide
5.2 SR2

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

© 2013 Genetec Inc. All rights reserved.

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

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

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

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

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

"Genetec", "Omnicast", "Synergis", "Synergis Master Controller", "AutoVu", "Federation", "Stratocast", the Genetec stylized "G", and the Omnicast, Synergis, AutoVu and Stratocast logos are trademarks of Genetec Inc., either registered or pending registration in several jurisdictions.

"Security Center", "Security Center Mobile", "Plan Manager", "Stratocast" and the Security Center logo are trademarks of Genetec Inc.

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

All specifications are subject to change without notice.

Document information

Document title: Security Center Installation and Upgrade Guide 5.2 SR2
Document number: EN.500.002-V5.2.C2(1)
Document update date: May 8, 2013
You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.
About this guide

This guide explains how to install and upgrade Security Center components. It assumes you are familiar with the following concepts and systems:

- Microsoft Windows administration
- Installation, configuration, and use of Microsoft SQL Server 2008
- IP networking administration

For information about migrating from Omnicast 4.x to Security Center 5.2, see the Omnicast Migration Guide 5.2.

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.
# Contents

About this guide ........................................ iii
Notes and notices ..................................... iii

## Chapter 1: Installing Security Center 5.2

- Pre-installation checklist .......................... 2
- Install SQL Server on a separate drive .......... 4
- About the Security Center installation package 8
  - Where can I find the Security Center installation package 8
  - Installation modes ................................. 8
  - Installer languages ................................. 8
  - What’s in the installation package ............... 8
- Installation overview ............................... 10
- Install Security Center on the main server ...... 12
  - Activate your license ............................. 21
- Install an expansion server ....................... 26
  - Connect the expansion server to the main server 35
- Install Security Center Client ................... 37
- Ports used by Security Center .................... 40
- Install Omnicast compatibility packs ............ 42
- Installing plugins .................................. 43
  - Enable Point-of-Sale plugin in Security Center 43
- Install Microsoft hotfixes ........................ 44
- Convert a main server to an expansion server .... 45
- Uninstall Security Center components ........... 46
- Post-installation checklist ....................... 47

## Chapter 2: Upgrading to Security Center 5.2

- Before you upgrade ................................ 49
- Before you upgrade from 5.1 to 5.2 ............... 49
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before you upgrade from 5.0 to 5.2</td>
<td>49</td>
</tr>
<tr>
<td>Before you upgrade from 4.0 to 5.2</td>
<td>50</td>
</tr>
<tr>
<td>Upgrade overview</td>
<td>53</td>
</tr>
<tr>
<td>Upgrade overview from 5.1 to 5.2</td>
<td>53</td>
</tr>
<tr>
<td>Upgrade overview from 5.0 to 5.2</td>
<td>54</td>
</tr>
<tr>
<td>Upgrade overview from 4.0 to 5.2</td>
<td>54</td>
</tr>
<tr>
<td>Security Center backward compatibility</td>
<td>56</td>
</tr>
<tr>
<td>Security Center backward compatibility requirements</td>
<td>56</td>
</tr>
<tr>
<td>Backward compatibility between Security Center roles</td>
<td>56</td>
</tr>
<tr>
<td>Backward compatibility with Security Desk tasks</td>
<td>57</td>
</tr>
<tr>
<td>Upgrade the main server</td>
<td>60</td>
</tr>
<tr>
<td>Upgrade an expansion server</td>
<td>62</td>
</tr>
<tr>
<td>Upgrading Security Center Client</td>
<td>63</td>
</tr>
<tr>
<td>Upgrade Security Center Client 4.0 or 5.0 to 5.2 SR2</td>
<td>63</td>
</tr>
<tr>
<td>Upgrade Security Center Client 5.1 to 5.2 SR2</td>
<td>63</td>
</tr>
<tr>
<td>Reapply role settings after you upgrade from 4.0</td>
<td>64</td>
</tr>
<tr>
<td>Find out which roles need their settings reapplied</td>
<td>64</td>
</tr>
<tr>
<td>Reapply Access Manager settings</td>
<td>65</td>
</tr>
<tr>
<td>Reapply Active Directory settings</td>
<td>67</td>
</tr>
<tr>
<td>Reapply LPR Manager settings</td>
<td>67</td>
</tr>
<tr>
<td>Reapply Omnicast Federation settings</td>
<td>68</td>
</tr>
<tr>
<td>Reapply Security Center Federation settings</td>
<td>68</td>
</tr>
<tr>
<td>Upgrade zone entities</td>
<td>68</td>
</tr>
</tbody>
</table>

**Chapter 3: Installing a Service Release update**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install a Service Release update</td>
<td>70</td>
</tr>
<tr>
<td>Installing a Service Release update in silent mode</td>
<td>71</td>
</tr>
<tr>
<td>Uninstall a Service Release update in silent mode</td>
<td>71</td>
</tr>
<tr>
<td>Uninstalling a Service Release update</td>
<td>72</td>
</tr>
</tbody>
</table>

**Chapter 4: Automating Security Center installation**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About silent installation</td>
<td>74</td>
</tr>
<tr>
<td>Before a silent installation</td>
<td>75</td>
</tr>
<tr>
<td>Limitations.</td>
<td>75</td>
</tr>
</tbody>
</table>
Installing Security Center 5.2

This section explains how to install Security Center components. It also describes the Security Center installation package.

This section includes the following topics:

- "Pre-installation checklist" on page 2
- "Install SQL Server on a separate drive" on page 4
- "About the Security Center installation package" on page 8
- "Installation overview" on page 10
- "Install Security Center on the main server" on page 12
- "Install an expansion server" on page 26
- "Install Security Center Client" on page 37
- "Ports used by Security Center" on page 40
- "Install Omnicast compatibility packs" on page 42
- "Installing plugins" on page 43
- "Install Microsoft hotfixes" on page 44
- "Convert a main server to an expansion server" on page 45
- "Uninstall Security Center components" on page 46
- "Post-installation checklist" on page 47
Pre-installation checklist

Before you install or upgrade Security Center, check and do the following:

- Check the network connections between your servers, workstations, and units.
- Check the unicast and multicast network connections and settings.
- Check that the minimum hardware requirements (servers and workstations) and software requirements (Windows, web browser, and so on) are met.
  
- Download any additional software (plugins, add-ons).
- Disable the power saving feature on your servers.
- Check that your servers are not domain controllers.
- Check the order of the network interface cards (NICs).
  
  The NICs used by Security Center roles should be on top of the list.
- Have your system ID and password in hand.
  
  You need this information 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.
- Check that you have a valid upgrade or migration path.
  
  For more information, see the Security Center 5.2 SR2 Release Notes.
- If you are upgrading, see "Security Center backward compatibility" on page 56.
- You must be logged on as administrator of the local computer.
  
  You may need to be a Microsoft Windows Domain administrator to access databases and storage on the machines. You may need to coordinate with the IT administrator.
- Check that the service users have all necessary permissions.
  
  For the Directory role to run, the service user needs the following SQL permission if their login name is not SYSADMIN:

  GRANT VIEW SERVER STATE TO [login name].
- (For remote databases) Check that SQL Server is set up for remote database access.
- Back up your Directory and role-specific databases.
  
  For information, see the Security Center Administrator Guide for the current version of your system.
- Close Internet Explorer.
- Check that the latest video and network drivers (servers and workstations) are installed.
• (For Windows 7 only) Activate .NET Framework 3.5.1, as follows:
  a Choose Start > Control Panel > Programs and Features.
  b In the Programs and Features dialog box, choose Turn Windows features on or off.
  c In the Windows Features dialog box, select the Microsoft .NET Framework 3.5.1 option, and click OK.
Install 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.

1. Do one of the following:
   - If you are installing SQL Server Standard or Enterprise:
     - In Windows, navigate to the SQL installation package folder.
     - Double-click **Setup.exe**.
   - If you are installing SQL Server Express:
     - In Windows, navigate to the Security Center installation package folder.
     - Click **Full > SQLExpress**.
     - Double-click one of the following:
       - If you are on a 64-bit computer: **SQLEXRWTS_x64_ENU.exe**.
       - If you are on a 32-bit computer: **SQLEXRWTS_x86_ENU.exe**.

2. In the SQL Server Installation Center, 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. You can type a path, or browse for a folder.

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 [http://msdn.microsoft.com/en-us/library/ms189822.aspx](http://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 (@).

9 In the Instance root directory field, select where to install the SQL Server and all directory database files.
You can type a path, or browse for a folder.

10 Click Next.

11 In the Server Configuration page, select the account name for each SQL Server service, and click Next.
12 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.** System administrators can access the database engine using their Windows credentials, or the specific password you specify here.

13 In the **Error Reporting** page, specify if you would like to send any errors to Microsoft, and click Next.

The SQL Server is installed.

14 Click Close.

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

**After you are done:** Install Security Center on the main server, and use the new SQL Server as your database server. See "Install Security Center on the main server" on page 12.
About the Security Center installation package

This section includes the following topics:

• "Where can I find the Security Center installation package" on page 8
• "Installation modes" on page 8
• "Installer languages" on page 8
• "What’s in the installation package" on page 8

Where can I find the Security Center installation package

The Security Center installation package is available on DVD or for download from the GTAP Product Download page, at https://gtap.genetec.com.

NOTE You will need a username and password to log on to GTAP.

Installation modes

You can run the Security Center installer in two modes:

• Wizard mode. The Genetec Security Center InstallShield Wizard appears when you insert the Security Center DVD into your DVD drive, or when you double-click setup.exe found in the root folder of your installation package.

• Silent mode. The silent mode is used to run the installer in an automated way without user intervention. For more information, see "Automating Security Center installation" on page 73.

Installer languages

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

What’s in the installation package

In Security Center 5.2, the Client and Server InstallShield Wizards have been merged into one installer from which you can install all Security Center components. The Security Center 5.2 installation package includes the following:

• setup.exe. The Security Center InstallShield Wizard, from which you can install the following applications:
  • Genetec Server. The server component of Security Center. Genetec Server is the Windows service that must be installed on every server computer in your Security
Center system. Once installed on a computer, that computer becomes part of your system's pool of servers.

- **Config Tool.** The client application used to configure and administer your Security Center system.
- **Security Desk.** The task-based, unified user interface of Security Center.
- **Hotfixes\Microsoft.** Microsoft hotfixes that are needed in some rare situations. If the software detects that you need them, it will ask you to apply them manually.
- **Tools.** This folder includes the following additional applications and tools:
  - **Access\HID VertX.** Discovery tool. A tool that allows you to discover HID units connected to your network. Once discovered, the units can be added to your system.
  - **BoschSDK.** The Bosch Video SDK application, and online help.
  - **Clustering\NEC Cluster.** Scripts for NEC failover purposes, and technical documentation on how to configure Security Center with NEC Clustering.
  - **Clustering\Windows Cluster.** Technical documentation on how to configure Security Center with Windows Clustering.
  - **LPR\MapInfo.** MapInfo installation package.
  - **LPR\SecurityDesk.** Custom tasks for Security Desk.
  - **LPR\Sharp.** Plate Reader Server software.
  - **LPR\XMLTemplatesSamples\XMLExport.** XML Export sample template files.
  - **LPR\XMLTemplatesSamples\XMLImport.** XML Import sample template files.
  - **Open Source Libraries.** Information about the open source libraries used by Security Center applications.
  - **Video.** VideoFileAnalyser.exe used by Technical Support and Field engineers to analyze the content of video files (G64).
  - **VisiowaveCodec.** Interlogix Visiowave codec drivers setup.exe.
  - **WireShark.** Network monitoring freeware useful for gathering diagnosis information when contacting Genetec Technical Assistance.
- **Compatibility packs.** This folder includes the Omnicast compatibility packs you'll need to install if federating Omnicast to Security Center. It includes compatibility packs for Omnicast 4.6, 4.7, and 4.8. If you need the compatibility packs for earlier versions of Omnicast, please contact Genetec Technical Assistance.
- **Documentation.** This folder contains the PDF versions of Security Center documentation, and some documentation on supported third-party hardware. For a list of available documentation, see "Where to find product documentation" on page 86.
The following table summarizes the Security Center installation process:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Before you install and upgrade Security Center, read the Security Center Release Notes for any known issues and other information about the release.</td>
<td>Click here for the most recent version of this document. It is also available from the GTAP Documents page. You will need a username and password to log on to GTAP.</td>
</tr>
<tr>
<td>2</td>
<td>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:</td>
<td>Security Center 5.2 System Requirements document, available at: <a href="http://www.genetec.com/Lists/Reference%20Documents/Genetec%20-%20Security%20Center%20System%20Requirements.pdf">http://www.genetec.com/Lists/Reference%20Documents/Genetec%20-%20Security%20Center%20System%20Requirements.pdf</a></td>
</tr>
<tr>
<td></td>
<td>• Security Center Server (main or expansion server)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Security Center Client (Config Tool, Security Desk, or both)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SQL Server (dedicated database server)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Go through the pre-installation checklist.</td>
<td>&quot;Pre-installation checklist&quot; on page 2.</td>
</tr>
<tr>
<td>4</td>
<td>Depending on your deployment requirements, you can install SQL Server on a separate drive from the OS drive.</td>
<td>&quot;Install SQL Server on a separate drive&quot; on page 4.</td>
</tr>
<tr>
<td>5</td>
<td>Install Security Center components on the main server that will host the Directory role.</td>
<td>&quot;Install Security Center on the main server&quot; on page 12.</td>
</tr>
<tr>
<td>6</td>
<td>Activate your product license on the main server.</td>
<td>&quot;Activate your license&quot; on page 21.</td>
</tr>
<tr>
<td>7</td>
<td>Make sure that all ports used by Security Center are open and redirected for firewall and network address translation purposes.</td>
<td>&quot;Ports used by Security Center&quot; on page 40.</td>
</tr>
<tr>
<td>8</td>
<td>Install Security Center components on any expansion servers that will connect to the main server to add processing power to your Security Center system.</td>
<td>&quot;Install an expansion server&quot; on page 26.</td>
</tr>
<tr>
<td>9</td>
<td>Install Security Center Client (Config Tool, Security Desk, or both).</td>
<td>&quot;Install Security Center Client&quot; on page 37.</td>
</tr>
<tr>
<td>10</td>
<td>If Omnicast systems will be federated to Security Center, install their compatibility packs on every computer where Security Center components (Server or Client) are installed. You need a different compatibility pack for each version of Omnicast you federate.</td>
<td>&quot;Install Omnicast compatibility packs&quot; on page 42.</td>
</tr>
<tr>
<td>11</td>
<td>Install any Security Center plugins.</td>
<td>&quot;Installing plugins&quot; on page 43.</td>
</tr>
</tbody>
</table>
### Installation overview

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>If required, install the Microsoft hotfixes.</td>
<td>&quot;Install Microsoft hotfixes&quot; on page 44.</td>
</tr>
<tr>
<td>13</td>
<td>Go through the post-installation checklist.</td>
<td>&quot;Post-installation checklist&quot; on page 47.</td>
</tr>
<tr>
<td>14</td>
<td>Configure your system for:</td>
<td>For Omnicast or Synergis deployment, see the Security Center Administrator Guide. For AutoVu deployment, see the AutoVu Handbook.</td>
</tr>
<tr>
<td></td>
<td>• Video surveillance/management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Access control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• License Plate Recognition</td>
<td></td>
</tr>
</tbody>
</table>

**IMPORTANT** If you need to install the Security Center Server on a computer after you have installed Security Center Client, always use the original Security Center installation DVD (or a downloaded copy of it). Using the Change option from Programs and Features (Add/Remove Programs on Windows XP) will not install the SQL Express component you need.
Install 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.

The main server installation procedure installs the following:

- The Genetec Server service with the Directory role.
  
  When installing Genetec Server, the Directory database (optionally SQL Express 2008 R2), the web-based <Admin Tool>, and the Watchdog service are also installed.

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

Before you begin: Read "Pre-installation checklist" on page 2.

1 Insert and display the Security Center DVD, or double-click setup.exe in the root folder of the Security Center installation package.

   The Security Center Installation startup screen appears.

2 In the lower-right corner of the dialog box, select the installation language (English or French).

3 Click Server installation.

4 If you are prompted to install any missing prerequisites, click Install. A reboot might be required.

5 In the InstallShield Wizard Welcome page, click Next.

6 In the License Agreement page, select I accept the terms in the license agreement and click Next.

7 In the Custom Setup page, select the Security Center applications to install. You can choose from the following:
- **Server.** Installs the Genetec Server service, the Directory database, the web-based Server Admin, and the Watchdog service.

- **(Optional) Client.** Installs the Security Center Client applications: Config Tool, the Security Desk, or both.

**NOTE** From this page, you can also do the following:

- Click the application name to view a *Feature Description* and its space requirements.
- Click the icon next to the application to change how the feature is installed.
- Click Help to view the custom setup tips.
- Click Space to view the disk space requirement summary.

8 In 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 “Documentation languages” in 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 5.2 program group.

9 In the *Destination folder* page, change the folder if necessary, and click Next.
10 In the *Installation Type* page, select the Main server option, and click Next.

**NOTE** If you are installing an expansion server, see "Install an expansion server" on page 26.
11 In the *Database Server* page, select one of the following options:

- **Install a new database server.** Installs Microsoft SQL Server 2008 R2 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 [http://msdn.microsoft.com/en-us/library/ms189822.aspx](http://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 (@).

- **Use an existing database server.** Select an existing Microsoft SQL Server instance to install the database on.

  **Best practice:** Replace *(local)* with your machine name. This is necessary if you are configuring the Directory for load balancing. For more information, see the *Security Center Administrator Guide*.

12 Click Next.
13 In the Services logon parameters page, select one of the following options:

- **Use default username 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.

14 Click Next.
15 In 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 <Admin Tool> (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, you’ll need to call Genetec Technical Support to reset it. See "Technical support" on page 87.

16 Click Next.
17 In the *Firewall Rules* page, select the *Allow Genetec Security Center 5.2 to create necessary firewall rules for its applications* option.

Select this option to ensure that the internal Windows Firewall security rules are configured correctly.

**NOTE** You’ll also need to configure the Security Center ports on your company’s Firewall after the installation. See "Ports used by Security Center" on page 40.
18 In the WinPcap Installation page, select the Install WinPcap 4.1.2 option. 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 4.1.2 Installation Wizard opens.

![WinPcap Installation Wizard](image)

a In the WinPcap Installation Wizard, follow the installation instructions.
b In 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.

19 In the Ready to Install the Program page, click Install.
20 When the *Installation Wizard Completed* page appears, select one the options that apply:

- **Launch the web-based Server Admin.** Opens the Server Admin in a browser for additional configuration. Always leave this option selected.
- **Connect to GTAP for the latest service pack now.** If you have access to Internet from your computer, select this option to download the latest service pack. Once connected to GTAP, click **System Management > Product Download**.
- **Show the Windows Installer log.**

21 Opens the Window Installer log in Notepad.

22 Click Finish.

23 If you selected the *Launch the web-based Server Admin* option in Step 20, the Server Admin browser window appears.

24 In the Server Admin, activate your product license. See "Activate your license" on page 21.

Security Center is now installed on the main server.

**After you are done:** If Omnicast systems will be federated, install the required Omnicast compatibility packs now (see "Install Omnicast compatibility packs" on page 42). Proceed to install Security Center on the expansion servers (see "Install an expansion server" on page 26).
Activate your license

You must activate your Security Center license on the main server using Server Admin. You can activate your license one of two ways:

- If you have Internet access: See "Web activation" on page 21. (Recommended)
- If you do not have Internet access: See "Manual license activation" on page 23.

Before you begin: To activate your license, you’ll need the following:

- The System ID and password found in the Security Center License Information document. Genetec Technical Support sends you this document when you purchase the product.
- The Server password to log on to Server Admin. The password is specified in Step 15 during the main server installation.

Web activation

1. Open the Server Admin web page.
2. Do one of the following:
   - In the address bar of your Web browser, type http://computer:port/Genetec, where computer is the DNS name or the IP address of your server, and port is the Web server port specified during Security Center Server installation (see Step 15). You may omit the Web server port if you are using the default value (80).
   - If connecting to Server Admin from the local host, double-click Genetec Server Admin ( ) in the Genetec Security Center 5.2 program folder.
3. Enter the server password that you set in Step 15 of the main server installation, and click Log on.
4 In the License dialog box that appears, click Modify license (📝).
   The License management dialog box appears.

5 Click Web activation.
6 In the Web activation dialog box, enter your System ID and Password as specified in the Security Center License Information document.
7 Click Activate.
   The details of your license appear in the License dialog box.

![License dialog box]

8 Click Save to close the License dialog box.

9 Close the browser window.

After you are done: Reboot your server.

NOTE Many more settings can be configured in the Server Admin. For more information, see “Server – Server Admin” in the Security Center Administrator Guide.

Manual license activation

If you do not have Internet access, you can activate your license manually.

1 Open the Server Admin web page.

2 Do one of the following:
   - In the address bar of your Web browser, type http://<computer>:<port>/Genetec, where <computer> is the DNS name or the IP address of your server, and <port> is the Web server port specified during Security Center Server installation (see Step 15). You may omit the Web server port if you are using the default value (80).
   - If connecting to Server Admin from the local host, double-click Genetec Server Admin ( ) in the Genetec Security Center 5.2 program folder in Windows.
3 Enter the server password that you set in Step 15 of the main server installation, and click Log on.

4 In the License dialog box that appears, click Modify license (✍).

5 In the License management dialog box, click Validation key, and choose to save or copy the validation key.

The validation key is a number sequence (in hexadecimal text format) generated by the Server Admin. It is used to obtain the license key that unlocks your Security Center software. The default name for the file is Validation.vk.

6 From another computer with Internet access, log on to GTAP at https://gtap.genetec.com.
7 In the GTAP login page, enter the System ID and the Password specified in the Security Center License Information document, and click Login.

8 Click Activate your license, and navigate to and open the Validation.vk file, and click Submit.

The message Your license has successfully been activated appears.

9 Click Click here to download your license key, and save the license key to a file.

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

10 Return to the Security Center main server.

11 In the Directory tab of the Server Admin web page, click License information.

12 In the License dialog box, click Modify license (Edit).

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

14 In the Manual activation dialog box, do one of the following:
   - Paste your license information from the License.lic file (open with a text editor).
   - Browse for the License.lic file, and click Open.

15 Click Activate.

NOTE Many more settings can be configured in the Server Admin. For more information, see “Server – Server Admin” in the Security Center Administrator Guide.
Install an expansion server

This section explains how to install an expansion server. An expansion server adds processing power to your Security Center system. You can add expansion servers to your Security Center system at any time by connecting them to the main server.

The expansion server installation procedure installs the following:

- The Genetec Server service without the Directory role.
  When installing Genetec Server, the Directory database (optionally SQL Express 2008 R2), the web-based <Admin Tool>, and the Watchdog service are also installed.

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

**IMPORTANT** You cannot install an expansion server until the main server is up and running. For more information, see "Install Security Center on the main server" on page 12.

**Before you begin:** Read "Pre-installation checklist" on page 2.

1 Insert and display the Security Center DVD, or double-click setup.exe in the root folder of the Security Center installation package.
   The Security Center Installation startup screen appears.

2 In the lower-right corner of the dialog box, select the installation language (English or French).

3 Click Server installation.

4 If you are prompted to install any missing prerequisites, click Install. A reboot might be required.

5 In the InstallShield Wizard Welcome page, click Next.

6 In the License Agreement page, select I accept the terms in the license agreement and click Next.
7 In the Custom Setup page, select the Security Center applications to install. You can choose from the following:

- **Server.** Installs the Genetec Server service, the Directory database, the web-based Server Admin, and the Watchdog service.
- **(Optional) Client.** Installs the Security Center Client applications: Config Tool, the Security Desk, or both.

**NOTE** From this page, you can also do the following:

- Click the application name to view a Feature Description and its space requirements.
- Click the icon next to the application to change how the feature is installed.
- Click Help to view the custom setup tips.
- Click Space to view the disk space requirement summary.

8 In 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 “Documentation languages” in 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 5.2 program group.

9 In the Destination folder page, change the folder if necessary, and click Next.
10 In the *Installation Type* page, select the Expansion server option, and click Next.
11 In the Database Server page, select one of the following options:

- **Install a new database server.** Installs Microsoft SQL Server 2008 R2 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 [http://msdn.microsoft.com/en-us/library/ms189822.aspx](http://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 (@).

- **Use an existing database server.** Select an existing Microsoft SQL Server instance to install the database on.

  **Best practice:** Replace (local) with your machine name. This is necessary if you are configuring the Directory for load balancing. For more information, see the Security Center Administrator Guide.

12 Click Next.
13 In the Services logon parameters page, select one of the following options:

- **Use default username 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.

14 Click Next.
15 In 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 <Admin Tool> (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, you’ll need to call Genetec Technical Support to reset it. See "Technical support" on page 87.

16 Click Next.
17 In 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.

18 In the *Firewall Rules* page, select the *Allow Genetec Security Center 5.2 to create necessary firewall rules for its applications* option.
Select this option to ensure that the internal Windows Firewall security rules are configured correctly.

**NOTE** You’ll also need to configure the Security Center ports on your company’s Firewall after the installation. See “Ports used by Security Center” on page 40.

19 In the *WinPcap Installation* page, select the *Install WinPcap 4.1.2* option. This option allows you to capture diagnostic data for units and other services in Security Center. The *WinPcap 4.1.2 Installation Wizard* opens.

![WinPcap Installation Wizard](image)

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

b) In 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.

20 In the *Ready to Install the Program* page, click *Install*. 
21 When the *Installation Wizard Completed* page appears, select one the options that apply:

- **Launch the web-based Server Admin.** Opens the Server Admin in a browser for additional configuration. Always leave this option selected.
- **Connect to GTAP for the latest service pack now.** If you have access to Internet from your computer, select this option to download the latest service pack. Once connected to GTAP, click System Management > Product Download.
- **Show the Windows Installer log.**

22 Click Finish.

23 The expansion server is installed.

**After you are done:** If Omnicast systems will be federated, install the required Omnicast compatibility packs now (see "Install Omnicast compatibility packs" on page 42). Proceed to connect the expansion server to the main server.
**Connect the expansion server to the main server**

This step is only applicable if you need to modify the information that was entered in **Step 17** of the expansion server setup wizard.

1. Do one of the following:
   - If you selected the *Launch the web-based Server Admin* option in **Step** of the expansion server installation procedure, the Server Admin browser window appears automatically. Continue with **Step 3**.
   - If you did not select the *Launch the web-based Server Admin* option, open the Server Admin Web page in **Step 2**.

2. Do one of the following:
   - In the address bar of your Web browser, type `http://<computer>:<port>/Genetec`, where `<computer>` is the DNS name or the IP address of your server, and `<port>` is the Web server port specified during Security Center Server installation (see **Step 15**).
     You may omit the Web server port if you are using the default value (80).
   - If connecting to Server Admin from the local host, double-click *Genetec Server Admin* ( ) in the *Genetec Security Center 5.2* program folder in Windows.

3. Enter the server password that you set in **Step 15**, and click *Log on*.

4. 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 is specified in Step during the main server installation.

5 Click **Apply** to save your changes.

Now your expansion server is connected to the main server.

**NOTE** Many more settings can be configured in the Server Admin. For more information, see “Server – Server Admin” in the *Security Center Administrator Guide.*
Install Security Center Client

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

1. Insert and display the Security Center DVD, or double-click `setup.exe` in the root folder of the Security Center installation package.

   The Security Center Installation startup screen appears.

   ![Security Center Installation Startup Screen](image)

2. In the lower-right corner of the dialog box, select the installation language (English or French).

3. Click Client installation.

4. If you are prompted to install any missing prerequisites, click Install. A reboot might be required.

5. In the InstallShield Wizard Welcome page, click Next.

6. In the License Agreement page, select I accept the terms in the license agreement and click Next.

7. In the Custom Setup page, select Security Center 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.

![Genetec Security Center 5.2 Installer](image)

**NOTE** From this page, you can also do the following:

- Click the application name to view a *Feature Description* and its space requirements.
- Click the icon next to the application to change how the feature is installed.
- Click Help to view the custom setup tips.
- Click Space to view the disk space requirement summary.

8 In 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 “Supported documentation languages” in 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 5.2 program group.

9 In the *Destination folder* page, change the folder if necessary, and click Next.

10 In the *Firewall Rules* page, select the *Allow Genetec Security Center 5.2 to create necessary firewall rules for its applications* option.

Select this option to ensure that the internal Windows Firewall security rules are configured correctly.

**NOTE** You’ll also need to configure the Security Center ports on your company’s Firewall after the installation. See “*Ports used by Security Center*” on page 40.

11 In the *Ready to Install the Program* page, click Install.
12 Click Finish.

After you are done: Install any required compatibility packs and hotfixes, and configure the Security Center ports on your company’s Firewall. See "Install Omnicast compatibility packs" on page 42, "Install Microsoft hotfixes" on page 44, and "Ports used by Security Center" on page 40.
During the Security Center installation, you were given the option of allowing Security Center to create firewall rules for its applications. If you selected this option, all Security Center applications were added as exceptions to the internal Windows firewall. However, you still need to ensure that all ports used by Security Center are open and redirected for firewall and network address translation purposes.

The following table describes the default ports used by Security Center applications. The ones you configure for your installation may be different.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Inbound</th>
<th>Outbound</th>
<th>Port usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>All servers</td>
<td>TCP 4502</td>
<td>TCP 4502</td>
<td>Communication between servers</td>
</tr>
<tr>
<td></td>
<td>HTTP 80</td>
<td></td>
<td>Connection via Server Admin</td>
</tr>
<tr>
<td>Main server</td>
<td>TCP 5500</td>
<td></td>
<td>Directory connection requests</td>
</tr>
<tr>
<td>All expansion servers</td>
<td></td>
<td>TCP 5500</td>
<td>Directory connection requests</td>
</tr>
<tr>
<td>Omnicast Federation</td>
<td>UDP 1024-2048</td>
<td></td>
<td>Security Desk when viewing video from an Omnicast Federation in Security Center</td>
</tr>
<tr>
<td>Archiver</td>
<td>TCP 555</td>
<td></td>
<td>Live and playback stream requests</td>
</tr>
<tr>
<td></td>
<td>UDP 15000–16000</td>
<td>UDP 15000–16000</td>
<td>Live unicast streams (audio &amp; video)</td>
</tr>
<tr>
<td></td>
<td>TCP &amp; UDP</td>
<td></td>
<td>Vendor specific ports for events and unit discovery</td>
</tr>
<tr>
<td></td>
<td>UDP 47806</td>
<td>UDP 47806</td>
<td>Live multicast video streams</td>
</tr>
<tr>
<td></td>
<td>UDP 47807</td>
<td>UDP 47807</td>
<td>Live multicast audio streams</td>
</tr>
<tr>
<td></td>
<td>TCP 554 or HTTP 80</td>
<td></td>
<td>Typical port used to request video from a unit</td>
</tr>
<tr>
<td>Media Router</td>
<td>TCP 554</td>
<td></td>
<td>Live and playback stream requests</td>
</tr>
<tr>
<td>Redirector</td>
<td>TCP 560</td>
<td></td>
<td>Live and playback stream requests</td>
</tr>
<tr>
<td></td>
<td>UDP 8000–12000</td>
<td></td>
<td>Live audio &amp; video unicast streams</td>
</tr>
<tr>
<td></td>
<td>UDP 47806</td>
<td></td>
<td>Live audio &amp; video multicast streams</td>
</tr>
<tr>
<td></td>
<td>TCP 555</td>
<td></td>
<td>Communication with Archiver</td>
</tr>
</tbody>
</table>
## Ports used by Security Center

<table>
<thead>
<tr>
<th>Computer</th>
<th>Inbound</th>
<th>Outbound</th>
<th>Port usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Manager</td>
<td>UDP/TCP 4070</td>
<td>UDP/TCP 4070</td>
<td>HID VertX controllers</td>
</tr>
<tr>
<td>TCP 20</td>
<td>TCP 21, 23</td>
<td>HID VertX controllers</td>
<td></td>
</tr>
<tr>
<td>TCP 4050</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LPR Manager</td>
<td>UDP 5000</td>
<td>Fixed Sharp unit discovery</td>
<td></td>
</tr>
<tr>
<td>TCP 8731</td>
<td></td>
<td>Fixed Sharp units and Patrollers</td>
<td></td>
</tr>
<tr>
<td>TCP 8832</td>
<td></td>
<td>Patroller hotfix requests</td>
<td></td>
</tr>
<tr>
<td>Intrusion Manager</td>
<td>TCP 3001</td>
<td>TCP 3001</td>
<td>Bosch intrusion panels</td>
</tr>
<tr>
<td>Security Desk &amp; Config Tool</td>
<td>TCP 5500</td>
<td>Directory connection requests</td>
<td></td>
</tr>
<tr>
<td>UDP 6000–6500</td>
<td></td>
<td>Live audio &amp; video unicast streams</td>
<td></td>
</tr>
<tr>
<td>UDP 47806</td>
<td></td>
<td>Live multicast video streams</td>
<td></td>
</tr>
<tr>
<td>TCP 554–560</td>
<td></td>
<td>Live and playback audio/video requests</td>
<td></td>
</tr>
</tbody>
</table>
Install Omnicast compatibility packs

The Omnicast compatibility pack is a software component that lets you view video from federated Omnicast systems in Security Center.

**IMPORTANT** Before you begin please note the following important notes:

- Security Center components (Server or Client) must be installed first.
- When installing both Omnicast and Security Center on the same computer, install Omnicast before installing the compatibility packs.
- Close all Security Center applications (Config Tool and Security Desk) and stop all Genetec services before installing the compatibility packs.
- You need to install a different Omnicast compatibility pack for each Omnicast version you will federate to your Security Center.
- If upgrading from an earlier version of Security Center, previously installed compatibility packs must be uninstalled and replaced with the ones provided on the Security Center 5.2 installation package.

1. Insert and display the Security Center DVD, or open the Security Center installation package.

To install an Omnicast compatibility pack:

1. In the *CompatibilityPacks* folder, open the folder for the required Omnicast version.
2. Double-click *setup.exe*, and follow the Installation Wizard instructions.
3. When the installation is complete, click *Finish*.
4. Repeat Step 1 to Step 3 for all Omnicast versions you need.
5. If you stopped Genetec services prior to this installation, restart them now.

**NOTE** The Omnicast compatibility packs are also available for download from the GTAP *Product Download* page, at [https://gtap.genetec.com](https://gtap.genetec.com). You will need a username and password to log on to GTAP.
Installing plugins

Plugins are installed separately from Security Center. Before installing a plugin, you must have a valid certificate for that plugin in your license. The procedures for installing plugins are found in the individual Plugin User Guides. For more information about using plugins in Security Center, contact your Genetec Sales Representative.

Enable Point-of-Sale plugin in Security Center

To view POS reports in Security Desk, do the following after installing the Security Center Client:

1. Open the SecurityDesk.plugins.xml file in \Program Files\Genetec Security Center 5.2.  

   EXAMPLE  <Assembly Name="Genetec.Synergis.Reporting.PointOfSale.dll"  
   Enabled="true" />

After you are done: Perform this procedure on each computer hosting a Security Center Client.
Install Microsoft hotfixes

After installing Security Center, you may receive the following notification when you log on to Config Tool or Security Desk: “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”. If you receive this message, you must install the microsoft hotfix on your computer.

1 Close Config Tool and Security Desk.
2 Insert and display the Security Center DVD, or open the Security Center installation package.
3 If you are using a 64-bit system, do the following:
   a Open the Hotfixes/Microsoft/KB2468871 (first) folder.
   b Double-click NDP40-KB2468871-v2-IA64.exe.
   c Click Run, follow the Installation Wizard instructions, and click Finish.
   d Double-click NDP40-KB2468871-v2-x64.exe.
   e Click Run, follow the Installation Wizard instructions, and click Finish.
   f Open the Hotfixes/Microsoft/KB2494124 folder.
   g Double-click NDP40-KB294124-x64.exe.
   h Click Run, follow the Installation Wizard instructions, and click Finish.
4 If you are using a 32-bit system, do the following:
   a Open the Hotfixes/Microsoft/KB2468871 (first) folder.
   b Double-click NDP40-KB2468871-v2-x86.exe.
   c Click Run, follow the Installation Wizard instructions, and click Finish.
   d Open the Hotfixes/Microsoft/KB2494124 folder.
   e Double-click NDP40-KB294124-x86.exe.
   f Click Run, follow the Installation Wizard instructions, and click Finish.
5 Restart your computer.
Convert a 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 since only one main server is allowed per system.

Before you begin: Make sure you have another main server to connect to before you decommission your current main server. For more information, see "Install Security Center on the main server" on page 12.

1. Log on to Server Admin on your computer using a Web browser (Internet Explorer).
2. In the Server Admin page, click the Genetec Server tab.
3. Scroll to the end of the browser page and click Deactivate Directory.
   This operation will restart Genetec Server.
4. Log on again to Server Admin.
   This time, the Directory tab will not appear.
5. Scroll to the section labelled Main server connection, and configure the name and password of the main server it is supposed to connect to.
6. Click Apply to save your changes.
Uninstall Security Center components

Security Center components are uninstalled from Windows Control Panel.

**CAUTION** If you are uninstalling a Security Center 5.1 Client and a Security Center 5.2 Server is installed on the same computer, the server component is also uninstalled. You will need to reinstall the Security Center Server.

To uninstall a component from Windows XP:
1. Click Start > Control Panel > Add or Remove programs.
2. In the window that appears, select the component name and click Remove.

To uninstall a component from Windows 7 or Windows 2008:
1. Click Start > Control Panel > Programs and Features.
2. In the window that appears, right-click the component name and select Uninstall.
Post-installation checklist

After you install or upgrade Security Center, check and do the following:

- Server Admin/main server
  - Directory is started
  - Database is connected (update if required)
  - Network interface card (NIC) order, and the NIC used by Server Admin
- Server Admin/expansion server
  - Connected to the main server
  - Network interface card (NIC) order, and the NIC used by Server Admin
- All clients applications are able to log on
- All roles must be running
  - Any yellow warning?
  - Database is connected (update if required)
  - NIC used by the role (switch to *Advanced* view)
- Archiver
  - Check disks groups, must have at least 0.2% of free space
  - Multiple Archivers on one server? Separate the databases and storage
- Access Manager
  - All required extensions have been added
- LPR Manager
  - Root folder set to the correct folder
- Network view
  - Tree structure and routes are configured
  - All servers are showing up in the tree structure
Upgrading to Security Center 5.2

This section explains how to upgrade an earlier version of Security Center (such as version 5.1) to version 5.2.

This section includes the following topics:

- "Before you upgrade" on page 49
- "Upgrade overview" on page 53
- "Upgrade the main server" on page 60
- "Upgrade an expansion server" on page 62
- "Upgrading Security Center Client" on page 63
- "Reapply role settings after you upgrade from 4.0" on page 64
Before you upgrade

This section describes the things you need to know and do before upgrading to Security Center 5.2.

This section includes the following topics:

- "Before you upgrade from 5.1 to 5.2" on page 49
- "Before you upgrade from 5.0 to 5.2" on page 49
- "Before you upgrade from 4.0 to 5.2" on page 50

Before you upgrade from 5.1 to 5.2

Before you upgrade your system from Security Center 5.1 to 5.2, read and do the following:

- If you have a 5.1 client and 5.1 server installed and want to upgrade the server to 5.2, you must uninstall the 5.1 server before installing the 5.2 server upgrade.
  
  **NOTE** You will not lose your previous configuration settings.

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

  **IMPORTANT** Be sure to enter the same values as used in your previous installation when InstallShield Wizard prompts you for these parameters.

- (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 re-configure the overwritten file.

- If you have HID EVO units in your system, the `VertXConfig.gconfig` file is not copied during the upgrade. After upgrading, you must copy the `VertXConfig.gconfig` file, if it exists, from your Security Center 5.1 program files folder to the 5.2 folder.

Before you upgrade from 5.0 to 5.2

Before you upgrade your system from Security Center 5.0 to 5.2, read the following:

- Security Center main server must be upgraded first.
- Config Tool, Media Router, and LPR Manager must be upgraded to 5.2.
  
  **NOTE** Upgrading a role to version 5.2 means upgrading the server hosting the role.

- New features introduced in 5.2 are only available if the server has been upgraded.
- When multiple servers are assigned to the same role, they must all be upgraded at the same time.
- New roles introduced in 5.2 cannot be hosted on 5.0 servers. They are:
Auxiliary Archiver
Directory Manager
Health Monitor
Global Cardholder Synchronizer

- If you are upgrading an AutoVu LPR system, you must also upgrade the Sharp cameras. For more information about upgrading AutoVu systems, see “Upgrading AutoVu” in the AutoVu Handbook. Click here for the most recent version of this document.

- After the upgrade, some users may get errors (Account disabled or locked down) when logging on to Security Center. As the administrator, you will need to reset their passwords. If the administrator’s password is affected, you will need to reset it through the Web Console. Not all users will be affected by this security upgrade.

- If you have HID EVO units in your system, the VertXConfig.gconfig file is not copied during the upgrade. After upgrading, you must copy the VertXConfig.gconfig file, if it exists, from your Security Center 5.0 program files folder to the 5.2 folder.

### Before you upgrade from 4.0 to 5.2

Before you upgrade your system from Security Center 4.0 to 5.2, read the following:

- The Installation Wizard does not migrate the server and database settings of the services and external systems it upgrades. Therefore, before you upgrade, write down the following information so you can reapply them after the upgrade.

  - **Synergis Access Manager service.** Write down its server name, its data server and database name, and its device extensions (for SST extensions, write down the discovery ports).
**TIP** You’ll find the database and device extension settings in Server Admin, under the Synergis Access Manager node.

```
You'll find the database and device extension settings in Server Admin, under the Synergis Access Manager node.
```

- **External system.** Write down the name and type of external system and the server name of the Integration Service hosting it.

  **TIP** You’ll find that information in the Config Tool’s Network view.

- In most cases, SQL Server 2005 is installed. But Security Center AutoVu requires SQL Server 2008, so you’ll need to either upgrade SQL Server 2005 to SQL Server 2008, or install a separate SQL Server 2008.

- If you are upgrading an AutoVu LPR system, you must also upgrade the Sharp cameras. For more information about upgrading AutoVu systems, see “Upgrading AutoVu” in the AutoVu Handbook. Click [here](#) for the most recent version of this document.

- **Zone entities in earlier versions of Security Center are converted to either hardware zones (_REAL_P) or virtual zones (VIRTUAL) in Security Center 5.2.** A hardware zone is a zone based on the inputs of a single access control unit, and it is controlled by the Access Manager role. A virtual zone is a zone based on the inputs of more than one unit, and is controlled by the Zone Manager role (introduced in Security Center 5.0).

  If you have virtual zones in your system after the upgrade, you’ll have to attach them manually to the Zone Manager role. See "Upgrade zone entities" on page 68.
• The services and external systems from earlier versions of Security Center are converted to the following roles in Security Center 5.2:

<table>
<thead>
<tr>
<th>Security Center 4.0 Service/External System</th>
<th>Is converted to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration Service (service)</td>
<td>Genetec Server (service)</td>
</tr>
<tr>
<td>Directory (service)</td>
<td>Directory (role)</td>
</tr>
<tr>
<td>Synergis Access Manager (service)</td>
<td>Access Manager (role)</td>
</tr>
<tr>
<td>AutoVu LPR Manager (external system)</td>
<td>LPR Manager (role)</td>
</tr>
<tr>
<td>Active Directory (external system)</td>
<td>Active Directory (role)</td>
</tr>
<tr>
<td>Omnicast federation (external system)</td>
<td>Omnicast Federation (role)</td>
</tr>
<tr>
<td>Security Center federation (external system)</td>
<td>Security Center Federation (role)</td>
</tr>
</tbody>
</table>
Upgrade overview

This section summarizes the upgrade process to 5.2.

This section includes the following topics:

- "Upgrade overview from 5.1 to 5.2" on page 53
- "Upgrade overview from 5.0 to 5.2" on page 54
- "Upgrade overview from 4.0 to 5.2" on page 54

Upgrade overview from 5.1 to 5.2

The following table summarizes the upgrade process from 5.1 to 5.2. For supported upgrade paths, see the Security Center Release Notes.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Read the things you need to know and do before you upgrade.</td>
<td>&quot;Before you upgrade from 5.1 to 5.2&quot; on page 49.</td>
</tr>
<tr>
<td>2</td>
<td>Read about backward compatibility.</td>
<td>&quot;Security Center backward compatibility&quot; on page 56</td>
</tr>
<tr>
<td>3</td>
<td>If Omnicast systems were federated to your previous Security Center system, you must uninstall the previously installed compatibility packs and replace them with the ones provided on the Security Center 5.2 installation package.</td>
<td>&quot;Install Omnicast compatibility packs&quot; on page 42.</td>
</tr>
<tr>
<td>4</td>
<td>Upgrade the main server.</td>
<td>&quot;Upgrade the main server&quot; on page 60.</td>
</tr>
<tr>
<td>5</td>
<td>Upgrade Config Tool.</td>
<td>&quot;Upgrading Security Center Client&quot; on page 63.</td>
</tr>
<tr>
<td>6</td>
<td>If you had a Directory failover configuration in your previous installation, upgrade all secondary Directory servers using the expansion server upgrade procedure. Be sure to write down and apply the same settings as used for your previous installation: passwords, database, ports, general properties, and so on.</td>
<td>&quot;Upgrade an expansion server&quot; on page 62.</td>
</tr>
<tr>
<td>7</td>
<td>Upgrade the other expansion servers and client workstations in your system according to your priorities and schedule. Be sure to write down and apply the same settings as used for your previous installation: passwords, database, ports, general properties, and so on.</td>
<td>&quot;Upgrade an expansion server&quot; on page 62.</td>
</tr>
</tbody>
</table>
Upgrade overview from 5.0 to 5.2

The following table summarizes the upgrade process from 5.0 to 5.2. For supported upgrade paths, see the Security Center Release Notes.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Read the things you need to know and do before you upgrade.</td>
<td>&quot;Before you upgrade from 5.0 to 5.2&quot; on page 49.</td>
</tr>
<tr>
<td>2</td>
<td>If Omnicast systems were federated to your previous Security Center system, you must uninstall the previously installed compatibility packs and replace them with the ones provided on the Security Center 5.2 installation package.</td>
<td>&quot;Install Omnicast compatibility packs&quot; on page 42.</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade the main server.</td>
<td>&quot;Upgrade the main server&quot; on page 60.</td>
</tr>
<tr>
<td>4</td>
<td>Upgrade Config Tool.</td>
<td>&quot;Upgrading Security Center Client&quot; on page 63.</td>
</tr>
<tr>
<td>5</td>
<td>Upgrade the Media Router role and the LPR Manager role by upgrading the servers hosting those roles.</td>
<td>&quot;Upgrade an expansion server&quot; on page 62.</td>
</tr>
</tbody>
</table>
| 6     | During this phase, you can roll out the upgrades to the other expansion servers and clients in your system according to your priorities and schedule. For a list of Security Center 5.0 roles and features that are backward compatible with 5.2, see the Security Center Release Notes. | • "Upgrade an expansion server" on page 62.  
   • "Upgrading Security Center Client" on page 63. |

Upgrade overview from 4.0 to 5.2

The following table summarizes the upgrade process from 4.0 to 5.2. For supported upgrade paths, see the Security Center Release Notes.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Read the things you need to know and do before you upgrade and write down all settings that you'll need to reapply after the upgrade.</td>
<td>&quot;Before you upgrade from 4.0 to 5.2&quot; on page 50.</td>
</tr>
<tr>
<td>2</td>
<td>If Omnicast systems were federated to your previous Security Center system, you must uninstall the previously installed compatibility packs and replace them with the ones provided on the Security Center 5.2 installation package.</td>
<td>&quot;Install Omnicast compatibility packs&quot; on page 42.</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade the Directory server in your previous system to be the main server.</td>
<td>&quot;Upgrade the main server&quot; on page 60.</td>
</tr>
</tbody>
</table>
### Upgrade overview

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Upgrade all other servers in your previous system as expansion servers.</td>
<td>&quot;Upgrade an expansion server&quot; on page 62.</td>
</tr>
<tr>
<td>5</td>
<td>If you upgraded from version 4.0, enable all inactive roles.</td>
<td>&quot;Reapply role settings after you upgrade from 4.0&quot; on page 64.</td>
</tr>
<tr>
<td>6</td>
<td>Upgrade all Security Center client applications.</td>
<td>&quot;Upgrading Security Center Client&quot; on page 63.</td>
</tr>
</tbody>
</table>
Security Center backward compatibility

Security Center 5.2 SR2 is backward compatible with many Security Center 5.1 components, allowing the system administrator to upgrade the system in stages.

This section includes the following topics:

- "Security Center backward compatibility requirements" on page 56
- "Backward compatibility between Security Center roles" on page 56
- "Backward compatibility with Security Desk tasks" on page 57

Security Center backward compatibility requirements

The requirements for Security Center backward compatibility are as follows:

- **Upgrading to latest version.** If upgrading to the latest version (for example, from 5.1 to 5.2), then you must always upgrade the main server hosting the Directory role and Config Tool.
- **Using new features.** A Security Center server must be upgraded in order to use the new features introduced in version 5.2 SR2.
- **Role is assigned to multiple servers.** If a role is assigned to multiple servers, such as in a failover configuration, all its servers must be running the same version of Security Center.

Backward compatibility between Security Center roles

Each new release of Security Center 5.2 includes new role features that may or may not be compatible with earlier versions. The backward compatibility with Security Center roles is summarized in the following table.

<table>
<thead>
<tr>
<th>Role type</th>
<th>Backward compatible to 5.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Router</td>
<td>No</td>
</tr>
<tr>
<td>Access Manager</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>IMPORTANT</strong></td>
<td>Security Center 5.2 SR2 is not backward compatible with Access Manager running on Security Center 5.1SR3_SP6 expansion server.</td>
</tr>
<tr>
<td>Archiver</td>
<td>Yes</td>
</tr>
<tr>
<td>Auxiliary Archiver</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Yes</td>
</tr>
<tr>
<td>Intrusion Manager</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Backward compatibility with Security Desk tasks

Security Center 5.2 SR2 backward compatibility with Security Desk 5.1 tasks is summarized in the following table.

<table>
<thead>
<tr>
<th>Task category</th>
<th>Task type</th>
<th>Backward compatibility to Security Desk 5.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Monitoring\textsuperscript{a}</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>No</td>
</tr>
<tr>
<td></td>
<td>Inventory management</td>
<td>No</td>
</tr>
<tr>
<td>Investigation</td>
<td>Incidents</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Zone activities</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Transactions</td>
<td>No</td>
</tr>
</tbody>
</table>

\textsuperscript{a} Monitoring includes both Monitoring and Operation Monitoring.
<table>
<thead>
<tr>
<th>Task category</th>
<th>Task type</th>
<th>Backward compatibility to Security Desk 5.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigation /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>Elevator activities</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Visit details</td>
<td>Yes</td>
</tr>
<tr>
<td>Investigation /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 /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 /LPR</td>
<td>Hits</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Reads</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Route playback</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Inventory report</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Daily usage per Patroller</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Logons per Patroller</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Reads/hits per day</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Reads/hits per zone</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Zone occupancy</td>
<td>No</td>
</tr>
<tr>
<td>Investigation /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>Task category</td>
<td>Task type</td>
<td>Backward compatibility to Security Desk 5.1</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------</td>
<td>---------------------------------------------</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>Maintenance /Access control</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 control unit configuration</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>IO configuration</td>
<td>Yes</td>
</tr>
<tr>
<td>Maintenance /Video</td>
<td>Archiver events</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Archiver storage details</td>
<td>Yes</td>
</tr>
<tr>
<td>Alarm management</td>
<td>Alarm monitoring</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Alarm report</td>
<td>Yes</td>
</tr>
</tbody>
</table>

a. Includes live video and playback.
Upgrade the main server

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

Before you begin:

- Read "Before you upgrade" on page 49.
- Back up all your previous system’s databases. For information about how to backup your databases, see the Security Center Administrator Guide of your previous system.

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

1. Install Genetec Server on the previous main server. Use the Main server installation type. See "Install Security Center on the main server" on page 12.
   The Installation Wizard automatically detects an earlier version of Security Center, and upgrades it to Security Center 5.2.

2. In the Server Admin, click Directory.

3. 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.
4 Close the Web browser.
5 Log on to Config Tool.
6 Open the System task and click Roles.
7 Select the Archiver role, and click Resources.
8 In the Actions section, click Database update ( ).

After the upgrade is complete, the Database status indicates Connected.
9 Repeat Step 7 to Step 8 for every role that requires a database update.
The roles on your system vary depending on your license options.
Upgrade an expansion server

Before you begin:

- If you are migrating from Omnicast 4.x, see the Omnicast Migration Guide 5.2.
- Back up all your previous system’s databases. For information on how to backup your databases, see the Security Center Administrator Guide of your previous system.

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

- Install Genetec Server on the expansion server you are upgrading. Use the Expansion server installation type. See "Install an expansion server" on page 26.
  
  The Installation Wizard automatically detects an earlier version of Security Center, and upgrades it to Security Center 5.2.

After you are done: Repeat this procedure on all expansion servers in your system.

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 database. For more information, see the Security Center Administrator Guide.
Upgrading Security Center Client

This section includes the following topics:

- "Upgrade Security Center Client 4.0 or 5.0 to 5.2 SR2" on page 63
- "Upgrade Security Center Client 5.1 to 5.2 SR2" on page 63

Upgrade Security Center Client 4.0 or 5.0 to 5.2 SR2

Client upgrades from versions 4.0 or 5.0 to Security Center 5.2 SR2 are not supported. Security Center 5.2 Client is installed side-by-side with previous Security Center Client versions, and then you can delete the older version.

1 Install Security Center Client (see "Install Security Center Client" on page 37).

   NOTE The user workspace configuration is not preserved. In previous versions 4.0 and 5.0, the user workspace was saved as a workstation configuration. In 5.2, the user workspace is saved as part of the user profile in the Directory.

2 Uninstall the older version of Security Center Client (see "Uninstall Security Center components" on page 46).

Upgrade Security Center Client 5.1 to 5.2 SR2

Client upgrades from version 5.1 to Security Center 5.2 SR2 are supported.

- Install Security Center Client (see "Install Security Center Client" on page 37).

   The Installation Wizard automatically detects an earlier version of Security Center Client, and upgrades it to Security Center 5.2.
Reapply role settings after you upgrade from 4.0

When you upgrade from 4.0 to 5.2, the server and database settings are not moved to the latest version. After you upgrade, you need to manually reassign the servers to their respective roles, and in some cases, upgrade their databases.

This section includes the following topics:
- "Find out which roles need their settings reapplied" on page 64
- "Reapply Access Manager settings" on page 65
- "Reapply Active Directory settings" on page 67
- "Reapply LPR Manager settings" on page 67
- "Reapply Omnicast Federation settings" on page 68
- "Reapply Security Center Federation settings" on page 68
- "Upgrade zone entities" on page 68

Find out which roles need their settings reapplied

Before you begin: You need the latest Config Tool version to configure the roles. For more information, see "Upgrading Security Center Client" on page 63.

1. Log on to your upgraded system using Config Tool.
2. Open the System task and click Roles.
   All roles upgraded from the previous system are shown in red (inactive).
3. If you have an inactive Access Manager, see "Reapply Access Manager settings" on page 65.
4. If you have an inactive Active Directory, see "Reapply Active Directory settings" on page 67.
5. If you have an inactive LPR Manager, see "Reapply LPR Manager settings" on page 67.
6. If you have an inactive Omnicast Federation, do one of the following:
   - If you are not migrating the federated Omnicast system, see "Reapply Omnicast Federation settings" on page 68.
   - If you are upgrading the federated Omnicast system to an independent Security Center 5.2 system, see "Scenario #3: Migrate a federated Omnicast system to a federated Security Center system", in the Omnicast Migration Guide 5.2.
   - If you are merging the federated Omnicast system to the Security Center system you just upgraded, do one of the following:
     - If your Omnicast Directory is located on the same computer as your Security Center Directory, see "Scenario #4: Migrate and merge a federated Omnicast system to its federation host on the same server", in the Omnicast Migration Guide 5.2.
Reapply role settings after you upgrade from 4.0

- If your Omnicast Directory is located on a different computer than your Security Center Directory, see "Scenario #5: Migrate and merge a federated Omnicast system to its federation host on a different server", in the Omnicast Migration Guide 5.2.

7  If you had an inactive Security Center Federation, see "Reapply Security Center Federation settings" on page 68.

In the entity tree, all roles appear in black (active).

After you are done: Backup all databases of your new system. For more information, see “Backup your role database” in the Security Center Administrator Guide.

Reapply Access Manager settings

Because your settings are not preserved by the installation program, you need to reapply them to the Access Manager role after the upgrade.

1  In Config Tool, open the System task, click Roles and select the Access Manager role.

2  Click Extensions and click ( ) to add the hardware extensions that this Access Manager used to control.

3  Click Apply to save your changes.

4  Click Resources.
5 In the Servers section, click ( ).

6 Select the server that was previously hosting this Access Manager, and click Add.

7 Enter the values for Database server and Database previously used by this Access Manager.
8  Click Apply to save your changes.
    In the entity tree, the role appears in black (active).

9  (Optional) If you used to have zone entities working in online mode in your previous
    system, follow "Upgrade zone entities" on page 68.

After you are done: Backup the Access Manager database. For more information, see “Backup
your role database” in the Security Center Administrator Guide.

Reapply Active Directory settings

Because your settings are not preserved by the installation program, you need to reapply them
to the Active Directory role after the upgrade.

1  In Config Tool, open the System task, click Roles and select the Active Directory role.
2  Click Resources.
3  Click ( ), select the server that was previously hosting this Active Directory, and click
   Add.
4  Click Apply to save your changes.
   In the entity tree, the role appears in black (active).

Reapply LPR Manager settings

Because your settings are not preserved by the installation program, you need to reapply them
to the LPR Manager role after the upgrade.

1  In Config Tool, open the System task, click Roles and select the LPR Manager role.
2  Click Resources.
3  In the Servers section, click ( ).
4  Select the server that was previously hosting this LPR Manager, and click Add.
5  In the Actions section, click Database update ( ).
6  Click Apply to save your changes.
7  Click Options.
8  On the General settings page, verify that the Root folder is properly set.
    If you used a network drive in the previous version, you will have to reset the path to the
    root folder.
9  Click Apply to save your changes.
   In the entity tree, the role appears in black (active).

After you are done: Backup the LPR Manager database. For more information, see “Backup
your role database” in the Security Center Administrator Guide.
Reapply Omnicast Federation settings

Because your settings are not preserved by the installation program, you need to reapply them to the Omnicast Federation role after the upgrade.

1. In Config Tool, open the System task, click Roles, and select the Omnicast Federation role.
2. Click Resources.
3. In the Servers section, click ( ) and select the server that was previously hosting this Omnicast Federation and click Add.
4. Click Apply to save your changes.

In the entity tree, the role appears in black (active).

Reapply Security Center Federation settings

Because your settings are not preserved by the installation program, you need to reapply them to the Security Center Federation role after the upgrade.

1. In Config Tool, open the System task, click Roles, and select the Security Center Federation role.
2. Click Resources.
3. In the Servers section, click ( ) and select the server that was previously hosting this Security Center Federation and click Add.
4. Click Apply to save your changes.

Upgrade zone entities

Zone entities based on inputs from more than one unit are converted to virtual zones ( ) in Security Center 5.2. If you see virtual zones in the Logical view after the upgrade, you’ll have to manually associate them with the Zone Manager role. For more information, see “Managing zones” in the Security Center Administrator Guide.

1. In Config Tool, open the Logical view task, and select a virtual zone entity.
2. Click Properties.
3. From the Zone Manager drop-down list, assign a Zone Manager role to the virtual zone.
4. Click Apply to save your changes.
5. Click Arming and change the zone arming properties if necessary.
6. Click Apply to save your changes.
Installing a Service Release update

A Security Center Service Release update package lets you update your existing Security Center version to the latest product release. For example, 5.2 GA to 5.2 SR2. You can install a Service Release update package only on computers where the same full version of Security Center has been installed. For example, you cannot install a 5.2 Service Release update on a machine that has 5.1 installed. Update packages do not include prerequisites, compatibility packs, tools, SQL Express, or the complete documentation set. Installation packages are available on GTAP.

This section includes the following topics:

- "Install a Service Release update" on page 70.
- "Installing a Service Release update in silent mode" on page 71.
- "Uninstalling a Service Release update" on page 72
Install a Service Release update

Before you begin:

- Make sure the full version of Security Center is installed (for example, 5.2 x).
- Download the service release update package from GTAP.

**NOTE** You will need a username and password to log on to GTAP.

To install the Service release update:

1. Close all Security Center applications (Config Tool and Security Desk) and stop all Genetec services (Genetec Server, and so on).
2. Inside the service release `.exe` file, double-click the `setup.exe` and follow the Install Wizard instructions.
3. When the installation is complete, click Finish.
Installing a Service Release update in silent mode

The service release update can be installed without any prompts or visual feedback using a command line.

Before you begin:

- Make sure the full version of Security Center is installed (for example, 5.2 x).
- Download the service release update package from GTAP.

**NOTE** You will need a username and password to log on to GTAP.

To install the Genetec server in silent mode:

Use the command prompt to run the following command:

```
Setup.exe /L1033 /s /v"/qn INSTALLDIR=c:\GENETEC_PATH ADDLOCAL=Directory"
```

To install the Genetec client in silent mode:

Use the command prompt to run the following command:

```
Setup.exe /L1033 /s /v"/qn INSTALLDIR=c:\GENETEC_PATH
ADDLOCAL=ConfigTool,SecurityDesk"
```

For more information about silent install commands, see "Automating Security Center installation" on page 73.

Uninstall a Service Release update in silent mode

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

- Run the following command from the Full folder of the Security Center installation package:
  `setup.exe /s /v"/qn /x`

To uninstall Security Center Client components (if the Server is also installed):

- Run the following command from the Full folder of the Security Center installation package:
  `setup.exe /s /v"/qn REMOVE=Client"`

To uninstall Security Center Server components (if the Server is also installed):

- Run the following command from the Full folder of the Security Center installation package:
  `setup.exe /s /v"/qn REMOVE=Server"`
Uninstalling a Service Release update

Security Center Service releases are uninstalled from Windows Control Panel.

To uninstall a component from Windows XP:
1. Click Start > Control Panel > Add or Remove programs.
2. Select the Service Release and click Remove.

To uninstall a component from Windows 7 or Windows 2008:
1. Click Start > Control Panel > Programs and Features.
2. Select the Service Release and click Uninstall.
Automating Security Center installation

This section explains how to automate the process of installing Security Center.

This section includes the following topics:

- "About silent installation" on page 74
- "Before a silent installation" on page 75
- "Installing Security Center in silent mode" on page 76
About silent installation

A silent installation is an automated way of installing software without user intervention. The silent installation is run from the command line using the 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
Before a silent installation

This section describes the things you must know and do before you perform a silent installation. This section includes the following topics:

- "Limitations" on page 75
- "Preinstallation tasks" on page 75

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 the installation to activate the license. For more information, see "Install Security Center on the main server" on page 12.

- 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 or by mapping a network drive to the path of `setup.exe`.

- You cannot install WinPcap (utility for capturing diagnostic data) in silent mode.

Preinstallation tasks

Perform the following tasks before performing a silent installation:

- Make sure you have all the software prerequisites installed before you launch a silent install. 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 running the silent installer. For more information, see "Pre-installation checklist" on page 2.

- Security Center Server must connect to a database server. If there is no database server, you can install Microsoft® SQL Server 2008 R2 Express Edition on your server computer, which is available on the Security Center DVD in the folder `\Full\SQLExpress`. For more information, see "Install SQL Server on a separate drive" on page 4.

- 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.
Installing Security Center in silent mode

This section includes the following topics:

- "Silent install command" on page 76
- "Installer options" on page 77
- "Sample server installation commands" on page 80
- "Sample client installation commands" on page 80
- "Uninstall Security Center in silent mode" on page 81

Silent install command

The syntax for calling Security Center in silent mode is:

```
Setup.exe /L<language> /s /v"/qn <option_list>"n
```

The following table lists the setup program options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/L&lt;language&gt;</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></td>
<td>• /L1033 for English (default)</td>
</tr>
<tr>
<td></td>
<td>• /L3084 for French</td>
</tr>
<tr>
<td>/s</td>
<td>Sets the setup.exe program to run in silent mode with no user interaction.</td>
</tr>
<tr>
<td>/v&quot;</td>
<td>Makes sure that the options within the quotation marks are sent directly to the msieexec.exe executable.</td>
</tr>
<tr>
<td>/qn</td>
<td>Runs the install in silent mode.</td>
</tr>
<tr>
<td>&lt;option_list&gt;</td>
<td>Sets the installer option list. Each option in the list uses the following syntax:</td>
</tr>
<tr>
<td></td>
<td>&lt;option&gt;=&lt;value_list&gt;</td>
</tr>
<tr>
<td></td>
<td>where &lt;option&gt; is an option name, and &lt;value_list&gt; is a list of comma-separated values.</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>between a pair of double quotes preceded by a backslash (*). The individual options and their values are described in &quot;Installer options&quot; on page 77.</td>
</tr>
</tbody>
</table>
## Installer options

The following table lists the installer options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INSTALLDIR</strong></td>
<td>Specify the path where the software will be installed.</td>
</tr>
<tr>
<td></td>
<td><strong>INSTALLDIR=C:\MyChoiceOfFolder</strong></td>
</tr>
<tr>
<td></td>
<td><strong>INSTALLDIR=&quot;D:\Program Files\Security Center&quot;</strong></td>
</tr>
<tr>
<td></td>
<td>Note that in the second example, (&quot;&quot;) is required because the value contains spaces. If do you not specify a path, it will be installed at <strong>C:\Program Files\Genetec Security Center 5.2</strong>.</td>
</tr>
<tr>
<td><strong>ADDCALL</strong></td>
<td>Specify the features to be installed.</td>
</tr>
<tr>
<td></td>
<td>The Server features are:</td>
</tr>
<tr>
<td></td>
<td>• Server (Genetec Server with Directory)</td>
</tr>
<tr>
<td></td>
<td>• Directory (also Genetec Server with Directory)</td>
</tr>
<tr>
<td></td>
<td>• SimpleServer (Genetec Server without Directory)</td>
</tr>
<tr>
<td></td>
<td>The Client features are:</td>
</tr>
<tr>
<td></td>
<td>• Client (installs Config Tool and Security Desk)</td>
</tr>
<tr>
<td></td>
<td>• SecurityDesk (only Security Desk)</td>
</tr>
<tr>
<td></td>
<td>• ConfigTool (only Config Tool)</td>
</tr>
<tr>
<td><strong>GLOBAL_SERVER</strong></td>
<td>Specify the database server name for the Directory. When omitted, the default value is <strong>(local)\SQLExpress</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE</strong> <strong>GLOBAL_SERVER=BLADE32\SQLServerEnterprise</strong></td>
</tr>
<tr>
<td><strong>DATABASE_SERVER</strong></td>
<td>Same as <strong>GLOBAL_SERVER</strong> option. This parameter maintains backward compatibility with previous silent installation scripts.</td>
</tr>
<tr>
<td><strong>DATABASE_INSTANCE</strong></td>
<td>Used in conjunction with the <strong>BACKUP_DATABASE</strong> option. Specify the database instance name for the Directory if different from the default.</td>
</tr>
<tr>
<td><strong>UPGRADE_DATABASE</strong></td>
<td>Specify that the SQL server database for the Directory is automatically upgraded. If the database does not exist, this property is ignored. Possible values are Y or N. When this option is omitted, the default value is N.</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE</strong> <strong>UPGRADE_DATABASE=Y</strong></td>
</tr>
<tr>
<td><strong>BACKUP_DATABASE</strong></td>
<td>Specify that the SQL server database for the Directory 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 property is not set, the default value is N. When set to Y, the <strong>BACKUP_DATABASE_PATH</strong> property must be set to a valid folder.</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE</strong> <strong>BACKUP_DATABASE=Y</strong></td>
</tr>
<tr>
<td><strong>BACKUP_DATABASE_PATH</strong></td>
<td>Used in conjunction with the <strong>BACKUP_DATABASE</strong> 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></td>
<td><strong>EXAMPLE</strong> <strong>UPGRADE_DATABASE_PATH=C:\Backups</strong></td>
</tr>
</tbody>
</table>
### Installing Security Center in silent mode

**SERVICEUSERNAME**
Specify the username to use in the services.
**EXAMPLE**
```
SERVICEUSERNAME=\admin
```

**SERVICEPASSWORD**
Specify the password to use in the services.
**EXAMPLE**
```
SERVICEPASSWORD=anypassword
```
User and password need to be created first with the right credentials prior to using those properties.

**SERVERADMIN_PORT**
Specify the HTTP port for the web-based Server Admin.
**EXAMPLE**
```
SERVERADMIN_PORT=8080
```

**SERVERADMIN_PASSWORD**
Specify the password for the web-based Server Admin.

**LANGUAGECHOSEN**
Language used by Security Center. The possible code values are:
- Arabic - 1025
- Chinese (Simplified) - 2052
- Chinese (Traditional) - 1028
- Czech - 1029
- Dutch - 1043
- English - 1033
- French - 3084
- German - 1031
- Hebrew - 1037
- Hungarian - 1038
- Italian - 1040
- Japanese - 1041
- Korean - 1042
- Norwegian - 1044
- Persian - 1065
- Polish - 1045
- Brasilian Portuguese - 2070
- Spanish - 1034
- Thai - 1054
- Turkish - 1055
**EXAMPLE**
```
LANGUAGECHOSEN=1033
```
If the code is invalid, English will be used. If this option is omitted, the installation language (specified with the `/L` option) will be used.

**WEBSERVER_PORT**
Specify the HTTP port for the web-based Server Admin.
### Option Descriptions

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CREATE_FIREWALL_RULES</td>
<td>Add the installed Security Center applications to the Windows Firewall exceptions list. Possible values are 0 or 1. When omitted, the default value is 1.</td>
</tr>
<tr>
<td></td>
<td>• 0 = Do not create Firewall rules</td>
</tr>
<tr>
<td></td>
<td>• 1 = Create Firewall rules</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE</strong> CREATE_FIREWALL_RULES=1</td>
</tr>
<tr>
<td>MAINSERVER_ENDPOINT</td>
<td>Used for expansion server installation. Specify the name or IP address of the main server.</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE</strong> MAINSERVER_ENDPOINT=MYMAINSERVER</td>
</tr>
<tr>
<td>MAINSERVER_PASSWORD</td>
<td>Used for expansion server installation. Specify password for the main server.</td>
</tr>
<tr>
<td>REBOOT</td>
<td>This option allows you to force or suppress a reboot after the Server installation has ended. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• F - To force a reboot when your installation is complete.</td>
</tr>
<tr>
<td></td>
<td>• S - To suppress any reboot except the one caused by the ForceReboot action.</td>
</tr>
<tr>
<td></td>
<td>• R - To suppress any reboot caused by Windows Installer actions.</td>
</tr>
<tr>
<td>SKIPSERVICESTART</td>
<td>This option allows you to avoid starting the Security Center services immediately after the installation (default behavior), if for example, you need to install hotfixes right after the full installation. When you use this option, don't forget to start the Security Center services (NET START GenetecServer and NET START GenetecWatchdog) after the hotfix installation.</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE</strong> SKIPSERVICESTART=Y</td>
</tr>
</tbody>
</table>
Sample server installation commands

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

```
Setup.exe /L1033 /s /v"/qn ADDLOCAL=Directory 
INSTALLDIR=C:\NewServer SERVICEUSERNAME=\.toto 
SERVICEPASSWORD=password DATABASE_SERVER=(local)\Genetec 
DATABASE_INSTANCE=DirectorySecurityCenter REBOOT=S"
```

**EXAMPLE** This is the standard installation of the Genetec Server with Directory in English without any questions. Only the installation path is different.

```
Setup.exe /L1033 /s /v"/qn INSTALLDIR=c:\GENETEC_PATH ADDLOCAL=Directory"
```

**EXAMPLE** This is equivalent to a Standard Installation in French, in silent mode without any questions.

```
Setup.exe /L3084 /s /v"/qn"
```

**EXAMPLE** This is equivalent to a Complete Installation in English, in silent mode without any questions. The default database server name, (local)\SQLExpress, is used for the Directory.

```
Setup.exe /L1033 /s /v"/qn ADDLOCAL=ALL"
```

**EXAMPLE** This is equivalent to a Complete Installation in English, in silent mode without any questions. This setup will create a log file located in c: drive.

```
Setup.exe /L1033 /s /v"/qn ADDLOCAL=ALL /L*v C:\Server.log"
```

**EXAMPLE** This is equivalent to a Complete Installation in English, in silent mode without any questions. Security Center applications will use Arabic.

```
Setup.exe /L1033 /s /v"/qn ADDLOCAL=ALL LANGUAGECHOSEN=1025"
```

Sample client installation commands

**EXAMPLE** The Security Desk will be installed in English, in silent mode without any questions.

```
Setup.exe /L1033 /s /v"/qn INSTALLDIR=c:\GENETEC_PATH ADDLOCAL=SecurityDesk"
```

**EXAMPLE** The Config Tool and the Security Desk will be installed in French, in silent mode without any questions.

```
Setup.exe /L3084 /s /v"/qn INSTALLDIR=c:\GENETEC_PATH 
ADDLOCAL=ConfigTool,SecurityDesk"
```

**EXAMPLE** The Config Tool and the Security Desk will be installed in English, in silent mode without any questions.
Installing Security Center in silent mode

Setup.exe /L1033 /s /v"/qn INSTALLDIR=c:\GENETEC_PATH ADDLOCAL=ConfigTool,SecurityDesk"

**EXAMPLE** This is equivalent to a Typical Installation in French, in silent mode without any questions.

Setup.exe /L3084 /s /v"/qn"

**EXAMPLE** Complete Installation in English, in silent mode without any questions.

Setup.exe /L1033 /s /v"/qn ADDLOCAL=ALL"

**EXAMPLE** Complete Installation in English, in silent mode without any questions. Security Center applications will use Arabic.

Setup.exe /L1033 /s /v"/qn ADDLOCAL=ALL LANGUAGECHOSEN=1025"

Uninstall Security Center in silent mode

**To uninstall Security Center (Client and Server components) in silent mode:**
- Run the following command from the *Full* folder of the Security Center installation package:

  ```
  setup.exe /s /v"/qn /x
  ```

**To uninstall Security Center Client components (if the Server is also installed):**
- Run the following command from the *Full* folder of the Security Center installation package:

  ```
  setup.exe /s /v"/qn REMOVE=Client"
  ```

**To uninstall Security Center Server components (if the Server is also installed):**
- Run the following command from the *Full* folder of the Security Center installation package:

  ```
  setup.exe /s /v"/qn REMOVE=Server"
  ```
Index

A
about
installation package, 8
silent mode, 74
this guide, iii
Access Manager, reapply settings after upgrade, 65
activating
license, 21
Active Directory, reapply settings after upgrade, 67

B
Bosch SDK, tools, 9

C
contacting technical support, 87
converting main server to expansion server, 45

D
demo license, acquiring, 87
differences between Security Center versions, 52
Discovery tool, locating, 9
document information, ii
documentation. See production documentation

E
enabling
inactive roles, 64
Point-ofSale plugin, 43
expansion server
about, 26
converting from main server, 45
installing, 26
upgrading, 62

F
files
SETUP.EXE, 8
VALIDATION.VK, 23
VIDEFILEANALYSER.EXE, 9
firewalls, configuring ports, 40

G
Genetec Server, installing in silent mode, 80

H
hotfix KB2494124, installing, 44

I
inactive roles, reactivate after upgrade, 64
installation package
about, 8
contents, 8
locating, 8
installing
See also installing options
expansion server, 26
Genetec Server in silent mode, 80
hotfix KB2494124, 44
main server, 12
Omnicast compatibility packs, 42
plugins, 43
Security Center
expansion server, 26
main server, 12
overview, 10
postrequisites, 47
prerequisites, 2
silent mode, 76
Security Center Client, 37
silent mode, 80
Service Release update, 70
silent mode, 71
silent mode, 76
WinPcap, 19, 33
installing options
languages, 8
modes
silent mode, 8
wizard mode, 8

L
languages, installing options, 8
license
activating, 21
manual activation, 23
web activation, 21
license key, about, 23
licensing, 87
limitations
silent mode, 75
locating
installation package, 8
LPR Manager, reapply settings after upgrade, 67

M
main server
about, 12
converting to expansion server, 45
installing, 12
upgrading, 60
manual license activation, 23
MapInfo, tools, 9
modes, installation options, 8

N
NEC Cluster
document location, 9
tools, 9

O
Omnicast compatibility pack, installing, 42
Omnicast Federation, reapply settings after upgrade, 68
opening
ports on company firewalls, 40
Server Admin, 21, 23
overviews
installing, 10
upgrading, 53

P
plugins, installing, 43
Point-of-Sale plugin, enabling, 43
Portable Archive Player
document location, 9
tools, 9
ports, configuring for firewalls, 40
post-installation checklist, 47
postrequisites
installing Security Center, 47
pre-installation checklist, 2
preinstallation tasks
silent mode, 75
prerequisites
installing Security Center, 2
silent mode, 75
upgrading, 49
product documentation, about, 86

R
reactivate roles
Access Manager, 65
Active Directory, 67
LPR Manager, 67
Omnicast Federation, 68
Security Center Federation, 68
reassigning servers to roles, 64

S
Security Center
installing
overview, 10
uninstalling components
from Windows 7, 46
from Windows XP, 46
silent mode, 81
upgrading, 53
overview, 53
prerequisites, 49
version differences, 52
Security Center Client
enabling Point-of-Sale plugin, 43
installing, 37
silent mode, 80
upgrading, 63
Security Center Federation, reapply settings after upgrade, 68
Security Desk custom tasks, tools, 9
Server Admin
creating password, 17, 31
opening, 21, 23
server password, creating, 17, 31
server, reassigning to roles, 64
Service Release update
installing, 70
installing in silent mode, 71
uninstalling, 72
SETUP.EXE, file, 8
silent install command, using, 76
silent mode
about, 8, 74
installing, 76
Genetec Server, 80
install command, 76
options, 77
preinstallation tasks, 75
Security Center Client, 80
limitations, 75
prerequisites, 75
uninstalling Security Center, 81
uninstalling Service Release update, 71

t
technical support, contacting, 87

tools
Bosch SDK, 9
Discovery tool, 9
MapInfo, 9
NEC Cluster, 9
Portable Archive Player, 9
Security Desk custom tasks, 9
VIDEOFILEANALYSER.EXE, 9
Visiowave Codec, 9
Windows Cluster, 9
Wireshark, 9
XML templates, 9

U
uninstalling
Security Center components, 46
Security Center in silent mode, 81
Service Release update, 72
Service Release update in silent mode, 71
upgrading
expansion server, 62
main server, 60
overview, 53
prerequisites, 49
reapply role settings, 64
Security Center, 53
Security Center Client, 63
zone entities, 68
V
validation key, about, 23
VALIDATION.VK, file, 23
VIDEOFILEANALYSER.EXE, file location, 9
Visiowave codec, tools, 9

W
web license activation, using, 21
Windows Cluster
document location, 9
tools, 9
WinPcap, installing, 19, 33
Wireshark, tools, 9
wizard mode, about, 8

X
XML templates, tools, 9

Z
zone entity, enabling after upgrade, 68
Where to find product documentation

You can find our product documentation in the following locations:

- **Installation package.** The documentation is available in the *Documentation* folder of the installation package. Some of the documents also have a direct download link to the latest version of the document.

- **Genetec Technical Assistance Portal (GTAP).** The latest version of the documentation is available from the GTAP *Documents* page. Note, you’ll need a username and password to log on to GTAP.

- **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 Assistance Portal (GTAP), where you can find information and search for answers to your product questions.

- **Genetec Technical Assistance Portal (GTAP).** GTAP is a support website that provides in-depth support information, such as FAQs, knowledge base articles, user guides, supported device lists, training videos, product tools, and much more.
  
  Prior to contacting GTAC or opening a support case, it is important to look at this website for potential fixes, workarounds, or known issues. You can log in to GTAP or sign up at https://gtap.genetec.com.

- **Genetec Technical Assistance Center (GTAC).** If you cannot find your answers on GTAP, you can open a support case online at https://gtap.genetec.com. For GTAC’s contact information in your region see the Contact page at https://gtap.genetec.com.
  
  **NOTE** Before contacting GTAC, please have your System ID (available from the About button in your client application) and your SMA contract number (if applicable) ready.

- **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).

Additional resources

If you require additional resources other than the Genetec Technical Assistance Center, the following is available to you:

- **GTAP 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/Services.