Security Center 5.0 GA Installation and Upgrade Guide

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

© 2011 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.

Trademarks

"Genetec", "Omnicast", "Synergis", "AutoVu", "Federation", the Genetec stylized "G" and the Omnicast, Synergis and AutoVu logos are trademarks of Genetec Inc., either registered or pending registration in several jurisdictions.
"Security Center", "Security Center Mobile", "Plan Manager", 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.
## Contents

**Preface**
- What's in this guide ............................................. v
- Who should read this guide .................................... v
- Where to find more information ................................. v
  - About Security Center documentation ....................... vi
  - About AutoVu Patroller documentation ...................... vi
  - About AutoVu Sharp documentation ............................ vii
  - Additional information ....................................... vii
- How to provide feedback ........................................ vii
- Contacting Genetec Technical Assistance ..................... ix

**Chapter 1: Before you install**

- Read the Release Notes ......................................... 2
- About Security Center 5.0 architecture ........................ 3
- System requirements ............................................. 4
  - Server hardware requirements ............................... 4
  - Client hardware requirements ................................ 5
  - Client and Server software requirements ................... 5
- Supported upgrades, migrations, federations and interoperability ............................................ 7
  - Upgrade paths ................................................ 7
  - Migration paths .............................................. 7
  - Supported Federations ........................................ 8
  - Omnicast interoperability .................................... 8
- Preinstallation tasks ............................................ 9
  - Administrator privileges ..................................... 9
  - Internet access required to extract license ................ 9
  - Turn off power saving features .............................. 9
  - Back up system databases .................................... 9
  - Before you install Genetec Server on Windows 7 .......... 10
  - Before you install Security Desk on Windows Server 2008 10
Chapter 2: Installing Security Center 5.0

About the Security Center installation package
Availability
About the installation package
Installation modes
Installer languages
Installation workflow
Install Omnicast compatibility packages
Installing Security Center Server
Installing the main server
What is the main server
Install the main server
Activate license
Manual license activation
Installing an expansion server
What is an expansion server
Install an expansion server
Connect to the main server
Converting a main server to an expansion server
Upgrading the main server
What is the main server
Before upgrading the main server
Upgrade the main server
Upgrading an expansion server
What is an expansion server
Upgrade an expansion server
Uninstalling Security Center Server
Installing Security Center Client
Install Security Center Client
Enable Point-of-Sale plugin
Upgrade Security Center Client
Uninstall Security Center Client
## Installing Synergis Web Client
- Install Synergis Web Client
- Upgrade Synergis Web Client
- Uninstall Synergis Web Client

### Chapter 3: Installing Security Center in Silent Mode

**Before you begin**
- About Silent Mode
- Limitations
- Software prerequisites
- Preinstallation tasks

**Installing Security Center in Silent Mode**
- Silent install command
- Installer options
- Sample Genetec Server installation commands
- Sample client installation commands
- Install Security Center in Silent Mode
- Uninstall Security Center in Silent Mode

### Chapter 4: Migrating from Omnicast 4.x

**About the Migration tool**

**Migrating Omnicast to Security Center 5.0**
- Straight migration from Omnicast to Security Center
- Migrate and merge Omnicast to its federation host
- Migrate Omnicast and its federation host separately
- Using the Migration tool
- Running the Migration tool in silent mode

**Directory migration**

**Archiver migration**
- What is included in the Archiver migration
- What is not included in the Archiver migration

**Known migration limitations**

### Chapter 5: Migrating from AutoVu 4.3 and earlier
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Differences between Security Center and AutoVu 4.3</td>
<td>58</td>
</tr>
<tr>
<td>AutoVu migrating process</td>
<td>59</td>
</tr>
<tr>
<td>Setting up the LPR Manager role</td>
<td>60</td>
</tr>
<tr>
<td>Changing the location of the LPR Manager database</td>
<td>63</td>
</tr>
</tbody>
</table>
Preface

This section includes the following topics:

- "What's in this guide" on page v
- "Who should read this guide" on page v
- "Where to find more information" on page v
- "How to provide feedback" on page vii
- "Contacting Genetec Technical Assistance" on page ix

What's in this guide

This guide describes the prerequisites for installing Security Center 5.0 and the procedures for installing, uninstalling, upgrading, and migrating to Security Center.

This guide includes the following sections:

- Chapter 1 – Before you install
- Chapter 2 – Installing Security Center 5.0
- Chapter 3 – Installing Security Center in Silent Mode
- Chapter 4 – Migrating from Omnicast 4.x
- Chapter 5 – Migrating from AutoVu 4.3 and earlier

Who should read this guide

This guide is written for those responsible for installing Security Center. It assumes you are familiar with the following concepts and systems:

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

Where to find more information

Security Center includes documentation to help you get started, as well as provide detailed information about the product features. The latest version of the documentation is available from the Genetec Technical Assistance Portal (GTAP).
NOTE You’ll need a username and password to log on to GTAP.

About Security Center documentation

The documentation for Security Center is available on the Security Center DVD in the Documentation folder. Security Center includes the following documentation:

- **Security Center Release Notes.** Describes the release in detail, including new features, fixed issues, and known issues.
- **Security Center Installation and Upgrade Guide.** Describes the prerequisites for installing Security Center and provides instructions for installing and upgrading Security Center on your system.
- **Security Center Administrator Guide.** Provides all the instructions and conceptual information you’ll need to set up, configure, and administer your Security Center system. This guide is also from the Config Tool online Help.
- **Genetec Security Desk User Guide.** Provides the instructions and conceptual information you need to get started with Security Desk to monitor and generate reports for AutoVu LPR, Omnicast video surveillance, Synergis access control systems. This guide is also from the Security Desk online Help.
- **Security Center Synergis Web Client Quick Reference.** Describes how to use the Security Center Web Client to configure and generate reports for Synergis access control entities.
- **Creating a Security Center Map.** Describes how to create interactive graphical representation of doors, cameras, alarms, and areas on floor plans.

About AutoVu Patroller documentation

The documentation for AutoVu Patroller is available on the Patroller DVD in the Documentation folder.

Patroller includes the following documentation:

- **Patroller Release Notes.** Describes the Patroller release in detail and provide late-breaking or other information that supplements the main documentation. The latest version of the Release Notes is available at: [http://downloads.genetec.com/Security-Center/5.0/GA/AutoVu/EN.AutoVu Patroller Release Notes 5.0 GA.pdf](http://downloads.genetec.com/Security-Center/5.0/GA/AutoVu/EN.AutoVu Patroller Release Notes 5.0 GA.pdf).
- **Patroller Administrator Guide.** Describes how to install, configure, and troubleshoot AutoVu Patroller software.
- **Patroller User Guides.** Quick reference guides to using Patroller, AutoVu's mobile LPR solution. There is a separate user guide for each Patroller installation type (Law Enforcement, City Parking Enforcement, University Parking Enforcement, and Mobile License Plate Inventory).
• **AutoVu MLPI Handheld User Guide.** Instructions on how to install, configure, and use the license plate reading unit.

• **AutoVu Plate Reader Server Administration Guide.** Explains how to install, configure and upgrade the Sharp Plate Reader Server software.

• **AutoVu Connecting the Sharp Camera.** Explains how to power up and connect your Sharp. A printed version is provided in the Sharp box.

• **AutoVu Connecting the SharpX Camera.** Explains how to power up and connect your SharpX. A printed version is provided in the SharpX box.

**About AutoVu Sharp documentation**

The documentation for AutoVu Sharp is available on the Patroller DVD in the **Sharp** folder. Sharp includes the following documentation:

• **AutoVu Hardware Installation Guide.** Describes how to install and configure the hardware components in AutoVu fixed and mobile installations.

• **AutoVu Plate Reader Server Administration Guide.** Explains how to install, configure and upgrade the Sharp Plate Reader Server software.

**Additional information**

In addition to the product documentation, you can use the following resources to find out more about Security Center:


• Genetec’s Technical Assistance Portal (GTAP). Provides in-depth support information, including FAQs, knowledge base articles, product forums, as well as product assistance tools for our full suite of IP security solutions. Go to [http://gtap.genetec.com/](http://gtap.genetec.com/).

• Genetec Solutions 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. Go to [http://www.genetec.com/English/Support/Training](http://www.genetec.com/English/Support/Training).

**How to provide feedback**

Comments, corrections, and suggestions on Genetec documentation can be sent to documentation@genetec.com.
You can also let us know the improvements or related information you would like to see in the guide, by filling out our documentation feedback form at: https://spreadsheets.google.com/viewform?formkey=dDB6X2NYeUFPdWJGNVVnIva2xPUXc6MQ.
For more information or support, you can contact Genetec’s Technical Assistance Center (GTAC) in the following ways:

- Genetec’s Technical Assistance Portal (GTAP): For in-depth product technical information and assistance, customers can log in to the portal at [http://gtap.genetec.com](http://gtap.genetec.com).
- Email: support@genetec.com
- Telephone: 1-514-856-7100. Toll Free (USA & Canada): 1-866-338-2988, from Monday to Friday, 8:00 AM to 8:00 PM (Eastern time, GMT -5h).
  
  Europe: +800 01818200 (Please visit [gtap.genetec.com](http://gtap.genetec.com) for a list of covered territories.)

No matter how you contact us, you’ll need to have all relevant product information available, including System ID and product version. This information is available from the Help menu.
Before you install

This section describes the things you should know and do before you install or upgrade Security Center.

This section includes the following topics:

• Read the Release Notes on page 2
• About Security Center 5.0 architecture on page 3
• System requirements on page 4
• Supported upgrades, migrations, federations and interoperability on page 7
• Preinstallation tasks on page 9
About Security Center 5.0 architecture

The Security Center architecture has changed in version 5.0. In previous releases the installation included three services: the Directory, the Integration Service, and the Access Manager. In Security Center 5.0, there is only one type of service—the Genetec Server.

Genetec Server is the Windows service you must install on every server computer you want included in your Security Center’s pool of servers. Every server is a generic computing resource capable of taking on any role (set of functions) you assign to it. You can increase your Security Center system’s computing power at any time by adding more servers to the pool.

A role is a software module that performs a specific function (or job) within Security Center. You create and configure roles using the Config Tool. You can assign one or more roles to a single server, or a role to multiple servers to provide load balancing and failover.

The Directory role identifies your Security Center system. There can be only one instance of this role in your entire system, and the server hosting the Directory role must be set up first. This is your main server. All other servers you add to your Security Center system are called expansion servers, and must connect to the main server.
System requirements

This section describes the Security Center hardware and software requirements. This section includes the following topics:

- Server hardware requirements on page 4
- Client hardware requirements on page 5
- Client and Server software requirements on page 5

Server hardware requirements

The server hardware requirements depend on the product solutions included in your Security Center (AutoVu, Omnicast, Synergis, or a combination thereof). To determine which hardware configuration best suits your needs, contact the Genetec Sales Engineering team at salesengineering@genetec.com.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Server hardware requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Intel® Core 2 Duo 3.0 GHz or better</td>
</tr>
<tr>
<td></td>
<td>• 2 GB of RAM or more</td>
</tr>
<tr>
<td></td>
<td>• 80 GB hard drive for OS and Security Center applications</td>
</tr>
<tr>
<td></td>
<td>• Standard SVGA video card</td>
</tr>
<tr>
<td></td>
<td>• 1024 x 768 or higher screen resolution</td>
</tr>
<tr>
<td></td>
<td>• 100/1000 Ethernet Network Interface Card</td>
</tr>
<tr>
<td></td>
<td>• DVD ROM drive</td>
</tr>
<tr>
<td>Medium</td>
<td>Dual Core Intel® Xeon® 2.66 GHz or better</td>
</tr>
<tr>
<td></td>
<td>• 2 GB of RAM or more</td>
</tr>
<tr>
<td></td>
<td>• 80 GB hard drive for OS and Security Center applications</td>
</tr>
<tr>
<td></td>
<td>• Standard SVGA video card</td>
</tr>
<tr>
<td></td>
<td>• 1024 x 768 or higher screen resolution</td>
</tr>
<tr>
<td></td>
<td>• 100/1000 Ethernet Network Interface Card</td>
</tr>
<tr>
<td></td>
<td>• DVD ROM Drive</td>
</tr>
<tr>
<td>High(^a)</td>
<td>Quad Core Intel® Xeon® 2.0 GHz or better</td>
</tr>
<tr>
<td></td>
<td>• 4 GB of RAM or more</td>
</tr>
<tr>
<td></td>
<td>• 80 GB hard drive for OS and Security Center applications</td>
</tr>
<tr>
<td></td>
<td>• Standard SVGA video card</td>
</tr>
<tr>
<td></td>
<td>• 1024 x 768 or higher screen resolution</td>
</tr>
<tr>
<td></td>
<td>• 100/1000 Ethernet Network Interface Card</td>
</tr>
<tr>
<td></td>
<td>• DVD ROM Drive</td>
</tr>
</tbody>
</table>

\(^a\) Omnicast Archivers may record up to 300 cameras depending on the server’s configuration and the recording quality settings.
Client hardware requirements

The Security Center client requirements are the same for all product solutions.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Client Hardware requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Intel® Pentium® Dual-Core 2.5 GHz or better</td>
</tr>
<tr>
<td></td>
<td>• 2 GB of RAM or more</td>
</tr>
</tbody>
</table>
|               | • 80 GB hard drive for OS and Security Center applications
|               | • 128 MB PCI-Express x16 dual-head video adapter |
|               | • 1024 x 768 or higher screen resolution |
|               | • 10/100/1000 Ethernet Network Interface Card |
|               | • 16x DVD+/- RW Drive b |
| Medium        | Intel® Core®2 Duo 3.0 GHz or better |
|               | • 2 GB of RAM or more |
|               | • 80 GB hard drive for OS and Security Center applications
|               | • 256 MB PCI-Express x16 dual-head video adapter |
|               | • 1280 x 1024 or higher screen resolution |
|               | • 100/1000 Ethernet Network Interface Card |
|               | • 16x DVD+/- RW Drive b |
| High          | Intel® Core®2 Duo 3.0 GHz or better |
|               | • 4 GB of RAM or more |
|               | • 80 GB hard drive for OS and Security Center applications
|               | • 512 MB PCI-Express x16 dual-head video adapter |
|               | • 1600 x 1200 or higher screen resolution |
|               | • 100/1000 Ethernet Network Interface Card |
|               | • 16x DVD+/- RW Drive b |

a. After the installation, you must have at least 1 GB of free disk space to run Security Desk.
b. A DVD+/- RW drive is recommended in order to export archived video sequences.

Client and Server software requirements

Security Center client and server components share the same software requirements.

<table>
<thead>
<tr>
<th>Category</th>
<th>Required/Supported software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System a</td>
<td>• Microsoft® Windows 7 Professional and Ultimate 32-bit/64-bit</td>
</tr>
<tr>
<td></td>
<td>• Microsoft® Windows XP Pro SP3 32-bit/64-bit</td>
</tr>
<tr>
<td></td>
<td>• Microsoft® Windows Vista SP1 Business and Ultimate 32-bit/64-bit</td>
</tr>
<tr>
<td></td>
<td>• Microsoft® Windows Server® 2003 Standard Edition SP1/SP2/R2 32-bit/64-bit</td>
</tr>
<tr>
<td></td>
<td>• Microsoft® Windows Server® 2003 Enterprise Edition SP1/SP2/R2 32-bit/64-bit</td>
</tr>
<tr>
<td></td>
<td>• Microsoft® Windows Server® 2008 Standard Edition SP2/R2 32-bit/64-bit</td>
</tr>
<tr>
<td></td>
<td>• Microsoft® Windows Server® 2008 Enterprise Edition SP2/R2 32-bit/64-bit</td>
</tr>
</tbody>
</table>
Before you install | System requirements

<table>
<thead>
<tr>
<th>Category</th>
<th>Required/Supported software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Engine</td>
<td>• SQL Server 2005 Express/Standard/Enterprise SP2/SP3&lt;sup&gt;b&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• SQL Server 2008 R2 Express/Standard/Enterprise (required for AutoVu&lt;sup&gt;c&lt;/sup&gt;)</td>
</tr>
<tr>
<td>IIS&lt;sup&gt;d&lt;/sup&gt;</td>
<td>• Internet Information Service (IIS) 5.1 or later</td>
</tr>
<tr>
<td></td>
<td>• ASP.NET</td>
</tr>
<tr>
<td>Browsers&lt;sup&gt;d&lt;/sup&gt;</td>
<td>• Microsoft Internet Explorer 7 or 8, 32-bit</td>
</tr>
<tr>
<td>Virtualization</td>
<td>• VMWare ESX 4.0</td>
</tr>
</tbody>
</table>

a. Installation of the Security Center and Synergis/AutoVu is not supported on a Windows 2003/2008 Server running a Domain Controller.

b. SQL Server 2005 is not supported for AutoVu.

c. If Security Center manages more than five Patrollers, or if you intend to keep your LPR data over 30 days, it is recommended to use SQL Server 2008 Standard Edition instead of the Express Edition.

d. For Synergis Web Client and Web Server Admin.
Supported upgrades, migrations, federations and interoperability

This section includes the following topics:

- "Upgrade paths" on page 7
- "Migration paths" on page 7
- "Supported Federations" on page 8
- "Omnicast interoperability" on page 8

Upgrade paths

Security Center 5.0 GA supports the following upgrade paths:

- Security Center 3.0 (GA and SR1) to Security Center 5.0
- Security Center 4.0 (GA and SR1) to Security Center 5.0
- Security Center GA LA to Security Center GA 5.0

**NOTE** You cannot upgrade from Syngeris 2.1 to Security Center 5.0. You must first upgrade from Synergis 2.1 to Security Center 4.0, then upgrade to Security Center 5.0. For more information, see "Upgrading from Synergis 2.1" in the Security Center 4.0 SR1 Installation and Upgrade Guide, available at: http://downloads.genetec.com/SecurityCenter/4.0/SR1/EN.Security%20Center%20Installation%20and%20Upgrade%20Guide%204.0%20SR1.pdf

Migration paths

Security Center GA 5.0 supports the following migration paths:

- Omnicast (4.5, 4.6, and 4.7) to Security Center 5.0, using the Migration Tool.
  For more information, see "Migrating from Omnicast 4.x" in the Security Center Installation and Upgrade Guide.
- AutoVu 4.x to Security Center 5.0.
  For more information, see "Migrating from AutoVu 4.3 and earlier" in the Security Center Installation and Upgrade Guide.
Supported Federations

The Federation™ is a virtual system formed by joining multiple remote independent Genetec IP security systems together. The purpose of the Federation is to allow the users on your local system (the Federation host) to access the entities belonging to remote independent systems as if they were on your local system.

The Security Center GA 5.0 supports the following federations:

- Security Center 4.0 (GA and SR1) systems
- Omnicast 4.2, 4.5, 4.6, and 4.7 systems

Omnicast interoperability

**IMPORTANT** The Security Center 5.0 Archiver role and the Omnicast 4.x Archiver service cannot run on the same server.

Security Center 5.0 can coexist on the same server with the following versions of Omnicast (as long as the Archiver role is not running on that server):

- Omnicast 4.2, 4.5, 4.6, and 4.7

**NOTE** It is not recommended to host Security Center and Omnicast on the same machine if the latter supports more than 30 cameras.
Before you install | Preinstallation tasks

This section describes the things you’ll need to do before you install or upgrade Security Center.

This section includes the following topics:

- Administrator privileges on page 9
- Internet access required to extract license on page 9
- Turn off power saving features on page 9
- Back up system databases on page 9
- Before you install Genetec Server on Windows 7 on page 10
- Before you install Security Desk on Windows Server 2008 on page 10
- Add a user to manage the SQL 2008 R2 database on page 10

Administrator privileges

You need administrator privileges to install and upgrade Security Center and its prerequisites.

Internet access required to extract license

You’ll need to connect to the Genetec website in order to submit your validation key and to extract your license. This applies to the main server (machine hosting the Directory role) installation only.

If the main server does not have Internet access, you can save the validation key to a file, and then apply for the license from another machine that has Internet access.

Turn off power saving features

Turn off hibernation on computers hosting Genetec Server or any database used by Genetec Server.

Back up system databases

Before you upgrade, it is best practice to back up all your system databases. For information on how to back up your system databases, see the Security Center Administrator Guide corresponding to the system you are upgrading from.
Before you install Genetec Server on Windows 7

Make sure that Microsoft .NET Framework 3.5 SP1 is activated on Windows 7.

1. Choose Start > Control Panel > Programs and Features.
2. In the Programs and Features dialog box, choose Turn Windows features on or off.
3. Select Features > Add Features.
4. In the Windows Features dialog box, select the Microsoft .NET Framework 3.5.1 option, and click OK.

Before you install Security Desk on Windows Server 2008

If you will be using the Security Desk video export features on Windows Server 2008, then you must install the Desktop Experience feature before you install Security Desk.

1. Click Start > Administrative Tools > Server Manager.
2. In the Features Summary section, click Add features.
3. Select Desktop Experience and click Next.
4. In the Ready to Install page, click Install.

Add a user to manage the SQL 2008 R2 database

When installing Security Center Server with SQL Server 2008 R2, you must manually add a user to manage the database.

**NOTE** If you are upgrading a SQL database from an earlier version to the 2008 R2 version, you can skip this procedure since the necessary user is already present.

1. Open Microsoft SQL Server Management Studio and connect to the server hosting Security Center.
2. In the Security folder, right-click Logins, and select New Login.
3. In the Login name field, enter the Windows logon user name that is used to start your Security Center services.
   For example, if you are using the default user name Local System for your Security Center services, you would enter <server name>\Local System.
5. Under Select a page, click Server Roles and select sysadmin, and Click OK.
   The new user will appear in the Logins folder.
6. Close the Microsoft SQL Server Management Studio and restart all SQL and Security Center services.
Installing Security Center 5.0

This section explains how you can install and upgrade Security Center components. It also describes the Security Center installation package.

This section includes the following topics:

- "About the Security Center installation package" on page 12
- "Installation workflow" on page 14
- "Install Omnicast compatibility packages" on page 15
- "Installing Security Center Server" on page 16
- "Installing Security Center Client" on page 28
- "Installing Synergis Web Client" on page 30
About the Security Center installation package

This section includes the following topics:

- "Availability" on page 12
- "About the installation package" on page 12
- "Installation modes" on page 13
- "Installer languages" on page 13

Availability

The Security Center installation package is available on DVD or for download. Contact Genetec Technical Assistance for a link to the download.

About the installation package

The Security Center 5.0 installation package includes the following:

- **Client installation.** The client component of Security Center includes Config Tool and Security Desk applications. Click to begin the installation process.
  - **Config Tool.** The client application used to configure and administer your Security Center system.
  - **Security Desk.** The client application used to control and monitor multiple security and safety applications.
- **Server installation.** The server component of Security Center. Genetec Server is the Windows service that must be installed on every server computer on your Security Center system. Once installed on a computer, that computer becomes part of your system’s pool of servers. Click to begin the installation process.
- **Synergis Web Client installation.** The web-based application used to perform most of the Synergis reporting tasks and entity configuration from Internet Explorer, without the need to install Security Desk or Config Tool on the local workstation. Click to begin the installation process.
- **Tools.** This folder includes the following additional applications and tools:
  - \Access\HID VertX. Discovery tool
  - \LPR\MapInfo. MapInfo installation package.
  - \LPR\Security Desk. LPR-related custom tasks for Security Desk.
  - \LPR\Sharp. Plate Reader Server software.
  - \LPR\XMLTemplatesSamples\XMLExport. XMLExport sample template files
  - \LPR\XMLTemplatesSamples\XMLImport. XMLImport sample template files
- **Compatibility packs.** This folder includes the Omnicast compatibility packs you’ll need to install if federating Omnicast to Security Center. It includes compatibility pack
Installing Security Center 5.0 | About the Security Center installation package

for Omnicast 4.5, 4.6, and 4.7. 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.
- View Installation and Upgrade Guide. Click to open the Security Center Installation and Upgrade Guide.

**Installation modes**

You can run the Security Center Installer in two modes:

- **Wizard mode.** The Genetec Security Center Installation splash screen appears when you insert the Security Center DVD into your DVD drive:

  ![Genetec Security Center Installation](image)

- **Silent mode.** See "Installing Security Center in Silent Mode" on page 31.

**Installer languages**

The Security Center installer is available in English and French. You can select the language in the Installation Wizard.
Installation workflow

Install Security Center components in the following order:

1. Read "Before you install" on page 1. This section describes the things you should know and do before you install or upgrade Security Center.

2. If Omnicast will be federated to Security Center, then "Install Omnicast compatibility packages" on page 15.

3. Do one of the following:
   - If installing Security Center for the first time, follow "Installing Security Center Server" on page 16, and then "Installing Security Center Client" on page 28.
   - If upgrading from Security Center 3.0 or 4.0, follow "Upgrade the main server" on page 25, and then "Upgrade Security Center Client" on page 29.
   - If upgrading from Omnicast 4.x, see "Migrating from Omnicast 4.x" on page 41.
   - If you want to install components in silent mode, see "Installing Security Center in Silent Mode" on page 31.
Install Omnicast compatibility packages

The Omnicast compatibility pack is a software component that lets you view video from federated Omnicast systems in Security Center. Omnicast compatibility packs must be installed before installing any of the Security Center applications.

**IMPORTANT** When installing both Omnicast and Security Center on the same computer, install Omnicast before installing the compatibility packs.

**Before you begin:** 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 5.0 installation package.

You’ll need to install a different Omnicast compatibility pack for each Omnicast version you will federate to your Security Center. The Omnicast compatibility pack must be installed on each computer hosting Security Center applications, both server and client.

1. Insert the Security Center installation DVD in your computer’s DVD drive.
   - If the Installation Wizard does not appear, double-click setup.exe in the product’s root folder.
2. Click Compatibility packs.
3. In the CompatibilityPacks folder, open the folder for the required Omnicast version.
4. Double-click setup.exe and follow the Installation Wizard instructions.
Installing Security Center Server

This section includes the following topics:

- "Installing the main server" on page 16
- "Installing an expansion server" on page 21
- "Converting a main server to an expansion server" on page 23
- "Upgrading the main server" on page 24
- "Upgrading an expansion server" on page 26
- "Uninstalling Security Center Server" on page 27

Installing the main server

This section explains how to install the main server.

This section includes the following topics:

- "What is the main server" on page 16
- "Install the main server" on page 16
- "Activate license" on page 18

What is the main server

The main server is the only server on your Security Center system that hosts the Directory role. All other servers on your system are used to expand its processing capability. Hence, they are called expansion servers. All expansion servers must connect to the main server in order to be part of the same system.

Install the main server

The main server must be the first server you install in your system. This procedures installs the Genetec Server service, the Directory role, the web-based Server Admin, and the Genetec Watchdog service, on the server.

Before you begin: You need administrative privileges on the computer to install this component.

1 Insert and display the Security Center DVD.
   If the Installation Wizard does not appear, double-click setup.exe in the product’s root folder.

2 In the Genetec Security Center Installation splash page, click Server installation.
   If the Wizard prompts you to install any missing prerequisites, click Install. A reboot might be required.
If upgrading, the Wizard detects the previous versions and asks you to confirm the upgrade. Click Yes.

3 In Welcome page, click Next.

4 In the License agreement page, click I accept the terms in the license agreement and click Next.

5 In the Language selection page, select the language and click Next.

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

7 In the Installation type page, select Main server and click Next.

8 In the Database Server page, do one of the following, and click Next.
   - **Install a new database server.** Installs Microsoft SQL Server 2008 R2 Express Edition. You must choose a database server name. The default is SQLEXPRESS.
   - **Use an existing database server.** Select an existing Microsoft SQL Server instance on which you want to install the database.

**NOTE** The database server name must meet the following rules:
- Not case sensitive.
- 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/ms143507.aspx](http://msdn.microsoft.com/en-us/library/ms143507.aspx).
- Cannot be longer than 16 characters.
- 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 (_).
- Not allowed: Embedded spaces of other special characters, backslash (\), comma (,), colon (:), semi-colon (;), single quotation mark (’), ampersand (&), number sign (#), and at sign (@).

9 In the Services logon parameters page, do one of the following, and click Next.
   - **Use default username and password.** Use the default username (Local System) to run the Genetec Server services. This option works in most cases.
   - **Specify the username and password for all services.** Enter a valid domain username and password.
     **IMPORTANT** If Genetec Server is to host an Active Directory role, the user must be a member of the Administrators group, have Log on as service user right, and Read access to the Active Directory you want it to connect to.

10 In the Server parameters page, do one of the following, and click Next.
   - **Web server port.** The HTTP port that is used for the web-based Server Admin. If you change the default, then Server Admin address will need to include the port number.

- Server port. The TCP port through which the Genetec Servers in your system communicate.
- Server password/ Confirm password. Leave blank (the default) or type and confirm a new password to open the Server Admin.

**IMPORTANT** If you lose the server password, you’ll need to call Genetec Technical Assistance to reset it.

11 In the Ready to Install page, click **Install**.

12 When the Installation Wizard Completed page appears, choose from the following options, and click Finish.
   - **Launch the web-based Server Admin.** Open the Server Admin in a browser for additional configuration. You should always leave this option selected.
   - **Show the Windows Installer log.** Open the Window Installer log in Notepad after you click Finish.

13 In the browser window that appears, enter the server password that you set in Step 10, and click **Log on**.

14 In the Genetec Security Center Server Admin page, activate your product license. For more information, see **Activate license** on page 18.

**After you are done:** Many more settings can be configured through Server Admin. For more information, see “Entity configuration – Server – Server Admin” in the Security Center Administrator Guide.

**Activate license**

You must activate your Security Center license on the main server (installed with Genetec Server with Directory). You activate your license in Server Admin.

**Before you begin:**

- You need the System ID and password found in the Security Center License Information document. Genetec Technical Assistance sends you this document when you purchase the product.
- You’ll also need the Server password to open the Server Admin. The password is specified during Security Center Server installation.
- If you do not have Internet access, you can save the validation key to file, and then email the key along with your System ID and password to support@genetec.com.

**To activate your license:**

1 Log on to the Main server with Server Admin.
   
   To open Server Admin, do one of the following:
- In the address bar of a Web browser, type http://machine:port/Genetec, where *machine* is the DNS name or the IP address, and *port* is the Web server port specified in Step 10, and then enter the Server password.
  You may omit the Web server port if you are using the default value (80).

- If connecting to the Server Admin from a local host, then click the Server Admin icon in the Security Center program folder.

  The Server Admin page appears in your browser.

2. In the Directory tab of the Server Admin, click License information.

3. In the License dialog box, click Modify license.

4. 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 Server Admin. It is used to obtain the license key that unlocks your Security Center software. The default name for that file is Validation.vk.

5. Activate the Security Center license in one of the following ways:

   - **Web activation (Recommended)**. Activate Security Center through the internet.
     i. In the Web activation dialog box, enter your System ID and Password specified in the Security Center License Information document.
     ii. Click Activate.

   - **Manual activation**. Activate Security Center manually using license file.
     For more information, see Manual license activation on page 20.
Installing Security Center 5.0 | Installing Security Center Server

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

![License dialog box](image)

6. Click OK to close the License dialog box, and close your Web browser (Server Admin).
7. Restart the Genetec Server service or restart the server.

Manual license activation

1. Log on to GTAP at [http://gtap.genetec.com](http://gtap.genetec.com). In the Username field type the System ID (as Username) and the Password specified in the Security Center License Information document, and click Log in.
2. 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.
3. 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.
5. In the License dialog box, click Modify license.
6. In the License management dialog box, click Manual Activation.
7. 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).
Installing an expansion server

This section explains how to install an expansion server.

This section includes the following topics:

- "What is an expansion server" on page 21
- "Install an expansion server" on page 21
- "Connect to the main server" on page 22

What is an expansion server

An expansion server is any server on your Security Center system that does not host the Directory role. The purpose of expansion servers is to add to the processing power of your Security Center system. You may have as many expansion servers on your system as necessary.

Install an expansion server

Expansion servers must be installed after the main server. You can add expansion servers at any time during the life span of your system. This procedures installs the Genetec Server service, the web-based Server Admin, and the Genetec Watchdog service, on the server.

Before you begin: You need administrative privileges on the computer to install this component.

1. Insert and display the Security Center DVD. If the Installation Wizard does not appear, double-click setup.exe in the product’s root folder.

2. In the Genetec Security Center Installation splash page, click Server installation. If the Wizard prompts you to install any missing prerequisites, click Install. A reboot might be required.

3. If upgrading, the Wizard detects the previous versions and asks you to confirm the upgrade. Click Yes.

4. In Welcome page, click Next.

5. In the License agreement page, click I accept the terms in the license agreement and click Next.

6. In the Language selection page, select the language and click Next.

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

8. In the Installation type page, select Expansion server, and click Next.

9. In the Services logon parameters page, do one of the following, and click Next.

   - Browse for the License.lic file, and click Open.
   - Click Activate.
Installing Security Center 5.0 | Installing Security Center Server

- **Use default username and password.** Use the default username (Local System) to run the Genetec Server services. This option works in most cases.
- **Specify the username and password for all services.** Enter a valid domain username and password. If Genetec Server is to host an Active Directory role, the user must be a member of the Administrators group, have Log on as service user right, and Read access to the Active Directory you want it to connect to.

9 In the Server parameters page, do one of the following, and click Next.
- **Web server port.** The HTTP port that is used for the web-based Server Admin. If you change the default, then Server Admin address will need to include the port number in the URL. For example, "http://machine:port/Genetec" instead of "http://machine/Genetec".
- **Server port.** The TCP port through which the Genetec Servers in your system communicate.
- **Server password/ Confirm password.** Leave blank (the default) or type and confirm a new password to open the Server Admin.
  
  **IMPORTANT** If you lose the server password, you’ll need to call Genetec Technical Assistance to reset it.

10 In the Ready to Install page, click Install.

11 When the Installation Wizard Completed page appears, choose from the following options, and click Finish.
- **Launch the web-based Server Admin.** Open the Server Admin in a browser for additional configuration. You should always select this option.
- **Show the Windows Installer log.** Open the Windows Installer log in Notepad after you click Finish.

12 In the browser window that appears, enter the **server password** that you set in Step 10, and click Log on.

13 In the Genetec Security Center Server Admin page, connect it to the main server. For more information, see **Connect to the main server** on page 22.

**After you are done:** Many more settings can be configured through Server Admin. For more information, see “Entity configuration – Server – Server Admin” in the Security Center Administrator Guide.

**Connect to the main server**

You must connect your expansion server to your main server for it to be part of your Security Center system.

**Before you begin:**
- You’ll need the DNS name or IP address of your main server.
• You’ll also need the Server passwords of both servers (main and additional servers).

You connect an expansion server to the main server using Server Admin.

1 Log on to the new server you added with Server Admin if you have not yet done so. To open Server Admin, do one of the following:
   • In the address bar of a Web browser, type `http://machine/Genetec`, where `machine` is the DNS name or the IP address, and then enter the Server password.
   • If connecting to the Server Admin from a local host, then click the Server Admin icon in the Security Center program folder.

The Server Admin page appears in your browser.

2 Under Main server connection, enter the main server’s DNS name (or IP address) and its server password.

3 Click Apply to save your changes.

Converting a main server to an expansion server

This procedure is often necessary when you are adding a machine pre-installed with Security Center to your system. Whenever a machine comes pre-installed with Security Center, the Main server configuration is always used by default.

Before you begin: Make sure you have a new main server to connect to before you decommission your current main server.

1 Log on to Server Admin on the main server using a Web browser (Internet Explorer).
2 In the Server Admin page, select 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 should 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.
Upgrading the main server

This section explains how to upgrade a main server. This section includes the following topics:

- "What is the main server” on page 24
- "Before upgrading the main server” on page 24
- "Upgrade the main server” on page 25

What is the main server

The main server is the only server on a Security Center 5.0 system that hosts the Directory role. It is equivalent to the server hosting the Directory service in previous Security Center versions. All other servers on your system are used to expand its processing capability. Hence, they are called expansion servers. All expansion servers must connect to the main server in order to be part of the same system.

Before upgrading the main server

Before starting the upgrade process, you should note the following:

- The services and external systems from earlier versions of Security Center are converted into the following roles in Security Center 5.0:

Table 2-1: Security Center 5.0 role conversion chart

<table>
<thead>
<tr>
<th>Security Center 3.0/4.0 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>

- In most cases, SQL Server 2005 will be 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. Technical documentation provided on the DVD will mention this limitation.
- The upgrade process does not migrate the server and database settings of the services and external systems listed in Table 2-1. After the upgrade, you’ll need to manually
assign a server to each role and upgrade the database (when applicable). For more information, see Upgrade the main server on page 25.

Upgrade the main server

Upgrading your Directory server to a Security Center 5.0 main server involves upgrading the Directory database, and all services into roles. Since the roles are hosted on expansion servers, all expansion servers must be upgraded before you can complete your upgrade.

Before you begin: Read "Before upgrading the main server" on page 24 and 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 when upgrading from Security Center 4.x to 5.x, accept the message and continue with the upgrade procedure. A reboot will be required after the upgrade is completed.

1 Install Genetec Server on the main Directory server you are upgrading, using the Main server installation type.

   Apply your new Security Center 5.0 license, but do not close the web-based Server Admin. For more information, see Installing the main server on page 16.

2 From the Directory tab in the Server Admin page, under the Database–Actions group, click Upgrade database to upgrade the Directory database.

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

3 Close the Web browser (Server Admin).

4 Restart the Genetec Server service or restart the server.

   The main server is now fully functional.

5 (Optional) If your system is distributed over multiple servers, upgrade all of them as expansion servers before continuing, or else, you can repeat the role configuration steps after all servers on your system are upgraded.

   For more information, see Upgrading an expansion server on page 26.

6 Upgrade the Config Tool in order to complete the rest of the upgrade.

   For more information, see Upgrade Security Center Client on page 29.

7 Logon with Config Tool and select the Role view from the Home page.

8 (Optional) If you have an Active Directory role in your browser, do the following:

   a Select the Active Directory role, then select its Resources tab.

   b In the Servers section, click and select the server for hosting this role.

   c Click Apply to save your changes.

9 (Optional) If you have an Access Manager role in your browser, do the following:

   a Select the Access Manager role, then select its Resources tab.
b) In the Servers section, click \( \text{\(\text{\textsuperscript{\textregistered}}\)} \) and select the server for hosting this role.
c) In the Database section, click Upgrade database.
d) Click Apply to save your changes.

10 (Optional) If you have an LPR Manager role in your browser, do the following:
a) Select the LPR Manager role, then select its Resources tab.
b) In the Servers section, click \( \text{\(\text{\textsuperscript{\textregistered}}\)} \) and select the server for hosting this role.
c) In the Database section, click Upgrade database.
d) Click Apply to save your changes.

11 (Optional) If you have an Omnicast Federation role in your browser, do one of the following:

- If you are not migrating the federated Omnicast system, select the Resources tab of this role, and select the server for hosting this role.
- If you are upgrading the federated Omnicast system to an independent Security Center 5.0 system, see "Migrate Omnicast and its federation host separately" on page 45
- If you are merging the federated Omnicast system to the Security Center system you just upgraded, see "Migrate and merge Omnicast to its federation host" on page 44.

12 (Optional) If you have a Security Center Federation role in your browser, do the following:
a) Select the Security Center Federation role, then select its Resources tab.
b) In the Servers section, click \( \text{\(\text{\textsuperscript{\textregistered}}\)} \) and select the server for hosting this role.
c) Click Apply to save your changes.

After you are done: Backup all databases of your new system. For more information, see “Managing databases – Database backup and restore” in Security Center 5.0 Administrator Guide.

### Upgrading an expansion server

This section explains how to upgrade an expansion server.

This section includes the following topics:

- "What is an expansion server" on page 26
- "Upgrade an expansion server" on page 27

### What is an expansion server

An expansion server is any server on your Security Center system that does not host the Directory role. The purpose of expansion servers is to add to the processing power of your Security Center system.
Upgrade an expansion server

Before you begin: Read "Before upgrading the main server" on page 24 and 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 when upgrading from Security Center 4.x to 5.x, accept the message and continue with the upgrade procedure. A reboot will be required after the upgrade is completed.

• Install Genetec Server on the server you are upgrading, using the Expansion server installation type.
  
  For more information, see Installing an expansion server on page 21.

After you are done: Repeat the same process on all expansion servers on your system. Then, you will need to log on to the main server with Config Tool and verify in the Network view that all your expansion servers are active (shown in black). Assign the expansion servers to the roles, either as primary or as secondary servers, based on your needs.

Uninstalling Security Center Server

Use the Windows Add or Remove Programs tool (renamed Programs and Features in Windows 7) to uninstall Genetec Server.

1. On the computer hosting Genetec Server, click Start > Control Panel > Add or Remove programs.
2. Click Genetec Security Center 5.0 Server, and then click Remove.
Installing Security Center Client

This section includes the following topics:

- "Install Security Center Client" on page 28
- "Enable Point-of-Sale plugin" on page 29
- "Upgrade Security Center Client" on page 29
- "Uninstall Security Center Client" on page 29

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.

NOTE If the Installation Wizard prompts you to install any missing prerequisites, click Install. A reboot might be required.

1 Insert and display the Security Center DVD. If the Installation Wizard does not appear, double-click setup.exe in the product’s root folder.

2 In the Genetec Security Center Installation splash page, click Client installation.

3 In Welcome page, click Next.

4 In the License agreement page, click I accept the terms in the license agreement and click Next.

5 In the Language selection page, select the language and click Next.

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

7 In the Custom setup page, choose to install Config Tool and Security Desk, and click Next.

Both client applications are installed by default.

TIP From this page, you can also do the following:

- Click the application name to view a feature description and it’s space requirements.
- Click the Arrow button next to the application to change how a feature is installed.
- Click Help to view the custom setup tips.
- Click Space to view the disk space requirement summary.

8 In the Ready to Install page, click Install.

9 When the InstallShield Wizard Completed page appears, choose from the following options, and click Finish.
Enable Point-of-Sale plugin

In order to view POS reports in Security Desk, do the following after installing the Security Center Client:

1. Open the `SecurityDesk.plugins.xml` file in `C:\Program Files\Genetec Security Center 5.0`.

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

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

Upgrade Security Center Client

Security Center Client upgrades are only supported for minor version upgrade, such as from LA to GA. Upgrades from a previous major version, such as 3.0 and 4.0, are not supported.

In those cases, Security Center 5.0 Client is installed side-by-side with previous Security Center Client versions. To install Security Center Client, see "Install Security Center Client" on page 28.

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

Uninstall Security Center Client

Use the Windows Add or Remove Programs tool (renamed Programs and Features in Windows 7) to uninstall Security Center Client.

1. On the computer hosting Genetec Security Center Client, click **Start** > **Control Panel** > **Add or Remove programs**.
2. Click Genetec Security Center Client, and then click Remove.
Installing Synergis Web Client

This section includes the following topics:

- "Install Synergis Web Client" on page 30
- "Upgrade Synergis Web Client" on page 30
- "Uninstall Synergis Web Client" on page 30

Install Synergis Web Client

If the Installation Wizard prompts you to install any missing prerequisites, click Install. A reboot might be required.

1. Insert and display the Security Center DVD. If the Installation Wizard does not appear, double-click setup.exe in the product’s root folder.
2. In the Genetec Security Center Installation splash page, click Synergis Web Client installation.
3. In Welcome page, click Next.
4. In the License agreement page, click I accept the terms in the license agreement and click Next.
5. In the Directory page, specify the Security Center directory the Synergis Web Client will connect to. You type the computer name or IP address.
6. In the Ready to Install page, click Install.
7. When the InstallShield Wizard Completed page appears, choose from the following options, and click Finish.

Upgrade Synergis Web Client


Uninstall Synergis Web Client

Use the Windows Add or Remove Programs tool (renamed Programs and Features in Windows 7) to uninstall Synergis Web Client.

1. On the computer hosting Genetec Server, click Start > Control Panel > Add or Remove programs.
2. Click Synergis Web Client, and then click Remove.
Installing Security Center in Silent Mode

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

This section includes the following topics:

- Before you begin on page 32
- Installing Security Center in Silent Mode on page 35
Before you begin

This section describes the things you should know and do before you perform a silent installation.

This section includes the following topics:

- About Silent Mode on page 32
- Limitations on page 32
- Software prerequisites on page 32
- Preinstallation tasks on page 34

About Silent Mode

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

Limitations

Before performing a silent installation, you should note the following limitations:

- 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 Activate license on page 18.
- A command line is limited to a maximum of 850 characters.
  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.

Software prerequisites

During a silent installation the installer will verify and install the software prerequisites on your system, but this may cause your system to restart. Therefore, it is best practice to manually install the software prerequisites before running the silent installer.
The following table lists the software prerequisites. If they are not installed, the installation packages (.msi or .exe) are available on the Security Center DVD in the folder `\Client\ISSetupPrerequisites` or `\Server\ISSetupPrerequisites`.

**Table 3-2: Security Center software prerequisites**

<table>
<thead>
<tr>
<th>Computer</th>
<th>Prerequisite software</th>
</tr>
</thead>
</table>
| 32-bit and 64 bit operating systems | - Microsoft® .NET Framework 3.5 SP1 (dotNetFx35.exe)  
- Microsoft® .NET Framework 4.0 (dotNetFx40_x86_x64.exe)  
- Microsoft® Report Viewer 2008 (ReportViewer.exe)  
- Microsoft® CCR and DSS Runtime 2008 R2  
- Microsoft® CCR and DSS Runtime 2008 R3  
- Microsoft® Silverlight 4 (Silverlight.exe)  
- DirectX End-User Runtimes (DXSETUP.exe) – Only for client apps.  
- Visual C++ 2005 SP1 Redistributable (vcredist_x86.exe)  
- Visual C++ 2008 SP1 Redistributable (vcredist_x86.exe)  
- Visual C++ 2010 SP1 Redistributable(x86) (vcredist_x86.exe) |
| 32-bit operating systems  | - Microsoft® SQL Server 2008 Native Client (sqlncli.msi)  
- Microsoft® SQL Server 2008 Management Object Collection (SharedManagementObjects.msi)  
- Microsoft® SQL Server CLR Types (SQLSysClrTypes.msi)  
- MSXML 6.0 SP1 (msxml6_x86.msi)  
- One of the following depending on your operating system:  
  - Windows Installer 4.5 for Windows Server 2003 SP1 and later (x86)  
  - Windows Installer 4.5 for Windows Server 2008 (x86)  
  - Windows Installer 4.5 for Windows Vista (x86)  
  - Windows Installer 4.5 for Windows XP SP2 and later (x86) |
| 64-bit operating systems  | - Microsoft® SQL Server 2008 Native Client (x64) (sqlncli.msi)  
- Microsoft® SQL Server 2008 Management Object Collection (x64) (SharedManagementObjects.msi)  
- Microsoft® SQL Server CLR Types (x64) (SQLSysClrTypes.msi)  
- MSXML 6.0 SP1 (x64) (msxml6_x86.msi)  
- One of the following depending on your operating system:  
  - Windows Installer 4.5 for Windows Server 2003 and XP (x64)  
  - Windows Installer 4.5 for Windows Server 2008 (x64)  
  - Windows Installer 4.5 for Windows Vista (x64) |
Preinstallation tasks

Perform the following tasks before performing a silent installation:

- Security Center Server requires a database server to connect to. If there are none, 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 \Server\SQLExpress.
- 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 right.
Installing Security Center in Silent Mode

This section includes the following topics:

- Silent install command on page 35
- Installer options on page 36
- Sample Genetec Server installation commands on page 38
- Sample client installation commands on page 39
- Install Security Center in Silent Mode on page 39
- Uninstall Security Center in Silent Mode on page 39

Silent install command

Security Center's Client and Server packages each have its own setup.exe program. The syntax for calling this program in silent mode is the same for both:

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

Table 3-3 lists the setup.exe options.

### Table 3-3: Setup.exe 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. The language is a four-digit code that must immediately follow the /L command option. 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 executable to run in silent mode.</td>
</tr>
<tr>
<td>/v&quot;/qn &lt;option_list&gt;&quot;</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; where &lt;option&gt; is an option name, and &lt;value_list&gt; is a list 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 between a pair of double quotes preceded by a backslash (&quot;). The individual options and their values are described in &quot;Installer options&quot; on page 36.</td>
</tr>
</tbody>
</table>
## Installer options

Table 3-4 lists the installer options.

### Table 3-4: Installer options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR</td>
<td>Specify the path where the software should be installed. Example: <code>INSTALLDIR=C:\MyChoiceOfFolder</code>&lt;br&gt;Example: <code>INSTALLDIR=&quot;D:\Program Files\Security Center&quot;</code> If omitted, the default is <code>C:\Program Files\Genetec Security Center 5.0</code>. Note that in the second example, (<code>\</code>) are required because the value contains spaces.</td>
</tr>
<tr>
<td>ADDLOCAL</td>
<td>Specify the features to install. The Server features are:&lt;br&gt;• <code>ServerFiles,Directory</code> (Genetec Server with Directory)&lt;br&gt;• <code>ServerFiles,SimpleServer</code> (Genetec Server without Directory)&lt;br&gt;The Client features are:&lt;br&gt;• <code>ClientFiles,SecurityDesk</code> (only Security Desk)&lt;br&gt;• <code>ClientFiles,ConfigTool</code> (only Config Tool)&lt;br&gt;• <code>ALL</code> (all the above)</td>
</tr>
<tr>
<td>GLOBAL_SERVER</td>
<td>Specify the database server name for the Directory. When omitted, the default value is <code>(local)\SQLExpress</code>. Example: <code>GLOBAL_SERVER=BLADE32\SQLServerEnterprise</code></td>
</tr>
<tr>
<td>DATABASE_SERVER</td>
<td>Same as <code>GLOBAL_SERVER</code> option. This parameter keeps backward compatibility with previous silent installation scripts.</td>
</tr>
<tr>
<td>UPGRADE_DATABASE</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. Example: <code>UPGRADE_DATABASE=Y</code></td>
</tr>
<tr>
<td>BACKUP_DATABASE</td>
<td>Specify that the SQL server database for the Directory should 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, a default value is N. When set to Y, the <code>BACKUP_DATABASE_PATH</code> property must be set to a valid folder. Example: <code>BACKUP_DATABASE=Y</code></td>
</tr>
<tr>
<td>DATABASE_INSTANCE</td>
<td>Used in conjunction with the <code>BACKUP_DATABASE</code> option. Specify the database instance name for the Directory if different from the default.</td>
</tr>
<tr>
<td>BACKUP_DATABASE_PATH</td>
<td>Used in conjunction with the <code>BACKUP_DATABASE</code> option. Specify the folder where the database backup must be saved. If the path does not exist, it will be created. Example: <code>UPGRADE_DATABASE_PATH=C:\Backups</code></td>
</tr>
</tbody>
</table>
**Table 3-4: Installer options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVICEUSERNAME</td>
<td>Specify the username to use in the services. <strong>Example:</strong> SERVICEUSERNAME=.\admin</td>
</tr>
<tr>
<td>SERVICEPASSWORD</td>
<td>Specify the password to use in the services. <strong>Example:</strong> SERVICEPASSWORD=anypassword</td>
</tr>
<tr>
<td>SERVERADMIN_PORT</td>
<td>Specify the HTTP port for the Web-based Server Admin. <strong>Example:</strong> SERVERADMIN_PORT=8080</td>
</tr>
<tr>
<td>SERVERADMIN_PASSWORD</td>
<td>Specify the password for the Web-based Server Admin.</td>
</tr>
</tbody>
</table>
| ALLUSERS=1      | Add this command to install the shortcuts for all users. This parameter specifies whether to perform a per-machine or per-user installation on Windows NT-based target systems.
  - If this property is set to 2, the configuration data for the installation is stored in the All Users profile if the user has administrative privileges, or otherwise to the current user’s profile.
  - If set to 1, configuration data is written to the All Users profile if the user has administrative privileges, and if not the installation will display an error message and then exit. |
| LANGUAGECHosen  | Language used by Security Center. The parameter is a two-letter language code. The possible values are:
  - ar - Arabe
  - de - German
  - en - English
  - es - Spanish
  - fa - Persian
  - fr - French
  - nl - Dutch
  - it - Italian
  - ja - Japanese
  - ko - Korean
  - pt - Brasillian Portuguese
  - zh - Simplified Chinese
  **Example:** LANGUAGECHosen=fr
  If the code is invalid, English will be used. If this option is omitted, the installation langue (specified with the /L option) will be used. |
| WEBSERVER_PORT  | Specify the HTTP port for the web-based Server Admin.                                                                                                                                                   |
Table 3-4: Installer options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REBOOT</td>
<td>This option allows you to force or suppress a reboot after the Server installation completes. 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>
</tbody>
</table>

Sample Genetec Server installation commands

Run the setup.exe program located on the Security Center installation DVD in the Server folder.

**EXAMPLE**  The Genetec Server with Directory will be installed 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 in English.

```
Setup.exe /L1033 /s /v"/qn ADDLOCAL=ServerFiles,Directory
INSTALLDIR=C:\NewServer SERVICEUSERNAME=.\toto
SERVICEPASSWORD=password DATABASE_SERVER=(local)\Genetec
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=Server-Files,Directory"
```

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

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

**EXAMPLE**  This is equivalent to a Complete Installation in silent mode without any questions in English.

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

**EXAMPLE**  This is equivalent to a Complete Installation in silent mode without any questions in English. 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 silent mode without any questions in English. Security Center will use language 1025 (Arabic).

```
Setup.exe /L1033 /s /v"/qn ADDLOCAL=ALL LANGUAGECHOSEN=ar"
```
Sample client installation commands

Run the setup.exe program located on the Security Center installation DVD in the Client folder.

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

```
Setup.exe /L1033 /s /v"/qn INSTALLDIR=c:\GENETEC\PATH ADDLOCAL=ClientFiles,SecurityDesk"
```

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

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

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

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

**EXAMPLE** Complete installation in silent mode without any questions in English.

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

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

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

Install Security Center in Silent Mode

- Do one of the following:
  - Run the setup.exe program located on the Security Center installation DVD in the Client folder.
  - Run the setup.exe program located on the Security Center installation DVD in the Server folder.

Uninstall Security Center in Silent Mode

To uninstall Security Center in Silent Mode, the command is the same for both Client and Server components.

- Run the following command from either the Client or Server folder of the Security Center installation DVD:

  ```
  setup.exe /s /v"/qn" /x
  ```
Migrating from Omnicast 4.x

This section explains how to migrate Omnicast versions 4.x data to Security Center, whether Omnicast is a stand-alone or federated system.

This section includes the following topics:

- "About the Migration tool" on page 42
- "Migrating Omnicast to Security Center 5.0" on page 43
- "Directory migration" on page 48
- "Archiver migration" on page 53
- "Known migration limitations" on page 55
About the Migration tool

Security Center comes with a Migration tool to help you migrate your current Omnicast data to Security Center 5.0.

The Migration tool is always installed as part of Security Center 5.0.

**IMPORTANT** Both Security Center 5.0 Server and Client must be installed on the machine where you plan to run the Migration Tool.

The Migration tool must be executed on every machine where Omnicast components are installed.
Migrating Omnicast to Security Center 5.0

This section explains the most common Omnicast migration scenarios. This section includes the following topics:

- "Straight migration from Omnicast to Security Center" on page 43
- "Migrate and merge Omnicast to its federation host" on page 44
- "Migrate Omnicast and its federation host separately" on page 45
- "Using the Migration tool" on page 46

Before you begin: If you are using a Windows 7 or Windows 2008 system, make sure you have full administrative rights on the computer before using the Migration tool.

Straight migration from Omnicast to Security Center

This procedure describes how to migrate an Omnicast system straight into Security Center without a federation.

1. On the computer where Omnicast Directory is installed, install Security Center 5.0 Server and Client.
   For the Server installation, use the Main server installation type. For more information, see Installing the main server on page 16.
2. Log on to Security Center 5.0 with Config Tool and select the Role view.
3. Delete the Archiver role that was created by default on the main server.
4. Close all Omnicast and Security Center client applications.
5. Use the Migration tool to move the data from Omnicast to Security Center.
   For more information, see Using the Migration tool on page 46.

After the migration, the Omnicast 4.x system is turned off, its data are migrated to the Security Center 5.0 system, and its video units are controlled by the new Archiver role.
Migrate and merge Omnicast to its federation host

This procedure describes how to migrate an Omnicast system that is federated by a previous version of Security Center. The federation exist for the sole purpose of integrating Omnicast to Security Center. There is no requirement to keep two independent systems.

1. First upgrade Security Center 4.0 to version 5.0 on the main server. For more information, see Upgrade the main server on page 25.
2. Upgrade or install Security Center 5.0 Client on the main server. For more information, see Upgrade Security Center Client on page 29.
3. Log on with Config Tool to the main server.
4. Select the Network view, and verify that the expansion server entity is created.
5. Select the Role view, and delete the Archiver role that was created by default on the main server.
6. Run the Migration tool on the main server.

**IMPORTANT** Make sure you select the Omnicast Federation role that corresponds to the Omnicast system you are migrating. For more information, see Using the Migration tool on page 46.
7 Install Security Center 5.0 Server and Client on the Omnicast 4.x Archiver server. Security Center 5.0 Server must use the Expansion server installation. For more information, see “Install an expansion server” on page 21 and “Install Security Center Client” on page 28.

8 Run the Migration tool on the expansion server.
For more information, see Using the Migration tool on page 46.

Where there were two separate systems, Security Center 4.0 and Omnicast 4.x, now there is a single Security Center 5.0 system, running on two servers (main and expansion server).

**Migrate Omnicast and its federation host separately**

This procedure describes how to migrate a federated Omnicast system that must remain independent of its federation host (Security Center 4.0). After the migration, both systems are upgraded to Security Center 5.0, but remain as separate independent systems.

1 First migrate the Omnicast system to Security Center 5.0 by following the procedure described in “Straight migration from Omnicast to Security Center” on page 43. The stand-alone Omnicast 4.x system becomes a stand-alone Security Center 5.0 system with an Archiver role.

2 Then upgrade the federation host from Security Center 4.0 to Security Center 5.0.
For more information, see Upgrade the main server on page 25.

After the upgrade, the Omnicast federation external system becomes an Omnicast Federation role.

3 Log on to the upgraded federation host with Config Tool and select the Role view.
4 Select the Omnicast Federation role and upgrade it to Security Center.
   a Select the Omnicast Federation role that corresponds to the Omnicast system you just upgraded.
      It should appear in red (inactive) because the Omnicast services have been disabled by the Migration tool.
   b Select its Properties tab.
   c From the Version drop-down list, select Upgrade to Security Center.
   d In the warning message that appears, click Continue.
      The Identity tab is selected, and the entity type shows Security Center Federation.
   e (Optional) Change the entity name and description if necessary, and click Apply.
   f Select the Properties tab.
   g Enter the main server name, the username, and the password, and click Apply.
      After a short while, the Connection status should show Connected.

Where there were two different types of system (Security Center and Omnicast), there is now one type, Security Center 5.0. The two systems remain separate. The federation host continue to be the federation host.

Using the Migration tool

Before you begin: A Security Center 5.0 system must first be created to receive the data (entity configurations, events, etc.) migrated from the Omnicast 4.x system.

IMPORTANT If Omnicast is deployed on several machines, the Omnicast Directory server must always be migrated first.

1 Run the MigrationTool.exe located in the C:\Program Files\Genetec Security Center 5.0 folder, or wherever you installed Security Center 5.0.
   This opens the Migration tool Wizard.
2 Click the Browse button, and select where to save the migration reports, and then click Next. For more information about migration reports, see Step 9.
3 In the License agreement page, click I accept the terms in the license agreement and click Next.
4 In the Service selection page, select the services you want to migrate, and click Next.
   The possible choices are:
   • Directory
   • Archiver
- Metadata Engine
  Only the services installed on your Omnicast server are listed.

5 In the Omnicast information page, specify the Omnicast databases you want to migrate.
  If the information checks out, a green confirmation message appears. Click Next.

6 In the Security Center information page, enter the logon and database information of your target system.
  If the information checks out, a green confirmation message appears. Click Next.

7 (Optional) In the Omnicast Federation page, select the Omnicast Federation role that corresponds to the server you are migrating, and click Next.

8 Verify that the information is correct in the Creation summary page, then click Migrate.

   The Migration Progress window appears.
   The Migration tool will automatically stop and disable all Omnicast services.

9 When the migration is complete, click Close.

   If you selected the Open the Migration report folder option, the report folder will automatically open so you can see the logs that indicate what was migrated (or any errors that occurred). The names of the log files are as follows:
   - MigratedEntities.csv. Lists all entities that were migrated.
   - NotMigratedEntities.csv. Lists any entities that were not migrated and the reason why.
   - OtherErrors.csv. Lists any errors that prevented the migration process.

10 Verify your new Security Center system. If you are satisfied, you can uninstall Omnicast. If not, you can re-enable and start the Omnicast services. The Omnicast system will work just like before the migration. No old Omnicast data were lost or corrupted during the migration.

Running the Migration tool in silent mode

IMPORTANT When running the Migration tool in silent mode, never use localhost to specify a server. Always use the DNS name or IP address of the machine.
Directory migration

When migrating the Directory service, the following entities/items are included:

<table>
<thead>
<tr>
<th>Item</th>
<th>What's migrated</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Camera</strong></td>
<td>A camera is migrated to Security Center with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Logical ID</td>
</tr>
<tr>
<td></td>
<td>• Site membership (see <strong>Sites</strong>)</td>
</tr>
<tr>
<td></td>
<td>• Video quality/stream usage</td>
</tr>
<tr>
<td></td>
<td>• Recording settings</td>
</tr>
<tr>
<td></td>
<td>• Motion detection (and motion mask) settings</td>
</tr>
<tr>
<td></td>
<td>• Video attributes</td>
</tr>
<tr>
<td></td>
<td>• Network settings</td>
</tr>
<tr>
<td></td>
<td>• Time zone settings</td>
</tr>
<tr>
<td></td>
<td>• Camera specific settings</td>
</tr>
<tr>
<td><strong>PTZ motors</strong></td>
<td>A PTZ motor is migrated to Security Center and is merged with the camera</td>
</tr>
<tr>
<td></td>
<td>it is associated with. The following properties are migrated:</td>
</tr>
<tr>
<td></td>
<td>• PTZ protocol</td>
</tr>
<tr>
<td></td>
<td>• PTZ number</td>
</tr>
<tr>
<td></td>
<td>• Serial device</td>
</tr>
<tr>
<td><strong>Camera sequence</strong></td>
<td>A camera sequence is migrated with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Camera list, with dwell time and PTZ commands</td>
</tr>
<tr>
<td><strong>NOTE</strong></td>
<td>In Security Center 5.0, camera sequences can only be run by the local Security Desk. There is no Virtual Matrix that runs camera sequences on a server. Therefore, every time you view a camera sequence in Security Desk, it always starts from the beginning of the camera list.</td>
</tr>
<tr>
<td><strong>Sites</strong></td>
<td>A site is migrated to Security Center as two separate entities: an <em>area</em> and a <em>partition</em>, with the following transformations:</td>
</tr>
<tr>
<td></td>
<td>• An area and a partition are created for each site.</td>
</tr>
<tr>
<td></td>
<td>• The site hierarchy is reproduced in the Logical view as an area hierarchy.</td>
</tr>
<tr>
<td></td>
<td>• The site hierarchy is reproduced as a partition hierarchy under a new <em>root</em> partition.</td>
</tr>
<tr>
<td></td>
<td>• The site member entity list is copied to the area member entity list.</td>
</tr>
<tr>
<td></td>
<td>• The site member entity list is copied into the partition member entity list.</td>
</tr>
<tr>
<td></td>
<td>• The site accepted user list is copied into the partition accepted user list.</td>
</tr>
<tr>
<td>Item</td>
<td>What's migrated</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Units</td>
<td>A unit is migrated to Security Center as a <em>video unit</em> with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Network settings</td>
</tr>
<tr>
<td></td>
<td>• Username/password</td>
</tr>
<tr>
<td>Digital Input and</td>
<td>A input and output entities are migrated to Security Center as peripherals of the <em>video unit</em> they belong to. The following properties are migrated:</td>
</tr>
<tr>
<td>Output relays</td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td>Serial ports</td>
<td>A serial port is migrated to Security Center as a peripheral of the <em>video unit</em> it belongs to. The following properties are migrated:</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Serial communication settings</td>
</tr>
<tr>
<td></td>
<td>• Line driver</td>
</tr>
<tr>
<td>Speakers</td>
<td>A speaker is migrated to Security Center as a peripheral of the <em>video unit</em> it belongs to. The following properties are migrated:</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Network settings</td>
</tr>
<tr>
<td></td>
<td>• Volume gain</td>
</tr>
<tr>
<td></td>
<td>• Camera it is linked to</td>
</tr>
<tr>
<td>Microphones</td>
<td>A microphone is migrated to Security Center as a peripheral of the <em>video unit</em> it belongs to. The following properties are migrated:</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Network settings</td>
</tr>
<tr>
<td></td>
<td>• Sensitivity</td>
</tr>
<tr>
<td></td>
<td>• Input type</td>
</tr>
<tr>
<td></td>
<td>• Camera it is linked to</td>
</tr>
</tbody>
</table>
### What’s migrated

<table>
<thead>
<tr>
<th>Item</th>
<th>Details</th>
</tr>
</thead>
</table>
| **Users**       | A user is migrated with the following properties:  
• Name  
• Description  
• User group membership  
• Email  
• User status (enabled/disabled)  
• Password  
• Password expiration  
• Number of workstations the user can log on from  
• Logon schedules  
• Supervised logon settings  
• Privileges  
  If an Omnicast user had the same name as a Security Center user, the two will be merged, and the privileges granted to the Omnicast user will be granted to the Security Center user.  
  **CAUTION**  The Migration tool will try to migrate as many privileges as possible, however it is a best practice to verify the privileges after the migration.  
• List of viewer layouts (see **Viewer layouts**)  
• PTZ priority (called User level in Security Center)  
• Archive viewing limitation |
| **User groups** | A user group is migrated with the following properties:  
• Name  
• Description  
• Member list  
• Supervised logon settings  
• Privileges  
  If an Omnicast user group had the same name as a Security Center user group, the two will be merged, and the privileges granted to the Omnicast user group will be granted to the Security Center user group.  
  **CAUTION**  The Migration tool will try to migrate as many privileges as possible, however it is a best practice to verify the privileges after the migration.  
• PTZ priority (called User level in Security Center)  
• Archive viewing limitation |
| **Viewer layouts** | A viewer layout is migrated to Security Center as a **Public Monitoring task** with the following properties:  
• Name  
• Description  
• Tile pattern  
• Tile content (displayed entity) |
### Alarm entities

An alarm entity is migrated with the following properties:

- Name
- Description
- Logical ID
- Schedule
- Priority
- Dwell time
- Reactivation threshold
- Alarm recording duration
- Protect recorded video for
- Procedure (URL)
- Automatic acknowledgement after (seconds)
- Recipient list
- Broadcast option
- For sequential broadcasts, the *Time out* period is copied to every recipient.
- Displayed entity (cameras and camera sequences) list
- Camera list

The display option of the first camera in the list is applied to all cameras in Security Center. If the display option is *Still frames*, the closest playback options will be used. Duplicate cameras are removed and listed in the error log.

### Active alarm instances

Active alarm instances are migrated with the following properties:

- GUID
- Creation time
- Source entity and event
- Propagation level
- When the recipient notification is sequential, the last recipient that has been notified in the list is remembered.
- Dynamic alarm context data

### Acknowledged alarm instances

Acknowledged alarm instances are migrated with the following properties:

- GUID
- Creation time
- Source entity and event
- Acknowledgement time
- Acknowledgement type
- *Custom acknowledgements* are converted to *Default acknowledgements*.
- Acknowledged by

### Generic schedules

A generic schedule is migrated to Security Center as a *schedule* entity with the following properties:

- Name
- Description
- All recurrence settings with time coverage options
Migrating from Omnicast 4.x | Directory migration

<table>
<thead>
<tr>
<th>Item</th>
<th>What’s migrated</th>
</tr>
</thead>
</table>
| Archiving schedules| There are no archiving schedule entities in Security Center 5.0. Instead, each camera has the choice to use its own recording settings or follow the default settings of the Archiver role. The migration is performed as follows:  
- For each archiving schedule in Omnicast, the generic schedule and archiving mode is copied to each attached camera.  
- For each Archiver in Omnicast, only the default archiving schedules are copied to the corresponding Archiver role. |
Archiver migration

The following section lists how Archiver scenarios from Omnicast 4.x are migrated to Security Center 5.0:

<table>
<thead>
<tr>
<th>Omnicast scenario</th>
<th>Migration solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Archiver with no standby</td>
<td>• All video events and files are migrated to the Archiver role.</td>
</tr>
</tbody>
</table>
| An Archiver with standby/redundant Archiver| • All video events and files are migrated to a single Archiver role.  
• The Archiver role will be assigned the same servers used to host the primary and standby Omnicast Archiver services.  
• The primary Archiver must be migrated first. The first migrated Archiver will dictate the common settings of the Archiver role.  
• If all cameras have the same redundant setting, the setting is copied to the role. Otherwise, the cameras will keep their individual settings. |
| Multiple Archivers with one standby Archiver| • All video events and files are migrated to the Archiver roles.  
• For every subset of cameras that share the same primary and standby Omnicast Archivers, a Security Center Archiver role will be created, assigned to the same servers originally hosting the primary and standby Archivers services. |
| One primary Archiver with multiple standby Archivers| • Only the video events and files from the primary Archiver and the first standby Archiver are migrated to the Archiver role.                                                                                           |

What is included in the Archiver migration

The following items are migrated from the Archiver to Security Center:

• All storage configuration (disk configurations, disk groups, camera assignment to each disk group and camera retention periods) are all copied to the Archiver role properties.
• Watermarking settings and extension configurations are copied to the Archiver role properties.
• All archived video is preserved by the migration, including video recorded by a secondary Archiver during a failover event.
• Ghost cameras are migrated as offline cameras that are not attached to any unit.
  • If after the migration the video unit for the camera is created, then the offline camera is automatically attached to the video unit and comes online.
  • Recorded video for ghost cameras is migrated.
• All Archiver events are migrated.
What is not included in the Archiver migration

The following items are not migrated from the Archiver to Security Center:

- Non-default Archiver extension settings are not migrated.
  Archiver extensions (called Manufacturer extensions in Security Center 5.0) are created automatically as needed in Security Center. Therefore, unless you use default settings, the settings will not be migrated.
  Workaround: You’ll have to change settings manually after the migration.

- Maximum number of simultaneously archived cameras per Archiver is not migrated.
  Archiver failover works differently in Security Center. Whenever standby Archiver is involved, the migration creates a single Archiver role with two servers, one primary and one secondary.
  If multiple Archiver roles end up being assigned to the same server, you’ll need to manually assign a priority to each Archiver role after the migration to ensure proper operation during failover.
  For more information on Archiver priority, see “Part III – Managing Omnicast – Protecting your video archives” in the Security Center Administrator Guide.
## Known migration limitations

The following entities/configurations are not migrated from Omnicast to Security Center:

<table>
<thead>
<tr>
<th>Item</th>
<th>What’s not migrated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>Custom events</td>
</tr>
<tr>
<td>Actions</td>
<td>Custom actions</td>
</tr>
<tr>
<td>Event-to-action</td>
<td>All configurations</td>
</tr>
<tr>
<td>Failover</td>
<td>Failover lists</td>
</tr>
<tr>
<td>HTML maps</td>
<td>HTML maps that are bound to the Omnicast SDK (URL will be migrated, but the map will not work).</td>
</tr>
<tr>
<td>Omnicast audit trail activity</td>
<td>Directory database log</td>
</tr>
<tr>
<td>Active Directory</td>
<td>• All settings</td>
</tr>
<tr>
<td></td>
<td>• Users and user groups</td>
</tr>
<tr>
<td>Multi-site membership</td>
<td>Only the first three partitions will be migrated.</td>
</tr>
<tr>
<td>Cameras</td>
<td>The following camera properties are not migrated:</td>
</tr>
<tr>
<td></td>
<td>• Video overlays</td>
</tr>
<tr>
<td></td>
<td>• Recorded video sequences from Auxiliary Archivers</td>
</tr>
<tr>
<td></td>
<td>• Current camera blocking priority</td>
</tr>
<tr>
<td></td>
<td>• PTZ motors distinct site security settings. The PTZ motor entity is merged with the camera entity in Security Center.</td>
</tr>
<tr>
<td>Camera groups</td>
<td>All camera groups</td>
</tr>
<tr>
<td>Monitor groups</td>
<td>All monitor groups</td>
</tr>
<tr>
<td>Analog monitors</td>
<td>All analog monitors</td>
</tr>
</tbody>
</table>
## Migrating from Omnicast 4.x | Known migration limitations

<table>
<thead>
<tr>
<th>Item</th>
<th>What’s not migrated</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alarms</strong></td>
<td>The following alarm properties are not migrated:</td>
</tr>
<tr>
<td></td>
<td>• Alarm display mode (Salvo, Block, Simple) and maximum number of alarms on each user</td>
</tr>
<tr>
<td></td>
<td>• Individual <em>Live, Playback, or Still frame</em> display option for each attached camera</td>
</tr>
<tr>
<td></td>
<td>• “Delete after x days” setting for acknowledged alarms</td>
</tr>
<tr>
<td></td>
<td>• Accepted acknowledgement types</td>
</tr>
<tr>
<td></td>
<td>• Metadata overlay configuration</td>
</tr>
<tr>
<td></td>
<td>• For active &amp; acknowledged alarms, the Instance ID is lost</td>
</tr>
<tr>
<td></td>
<td>• Alarm instance description</td>
</tr>
<tr>
<td></td>
<td>• Alarm context (used when alarm is generated from SDK)</td>
</tr>
<tr>
<td></td>
<td>• Alarm history</td>
</tr>
<tr>
<td></td>
<td>• History of alarm priority is lost. Priority history for active and acknowledged alarms. In Security Center, the alarm report shows the current priority configuration on the alarm.</td>
</tr>
<tr>
<td><strong>Virtual Matrix</strong></td>
<td>All settings and dependent entity types:</td>
</tr>
<tr>
<td></td>
<td>• CCTV keyboards</td>
</tr>
<tr>
<td></td>
<td>• Hardware matrices</td>
</tr>
<tr>
<td></td>
<td>• Virtual cameras</td>
</tr>
<tr>
<td><strong>Plug-ins</strong></td>
<td>All server and client plug-ins</td>
</tr>
<tr>
<td><strong>Sites</strong></td>
<td>The following site properties are not migrated:</td>
</tr>
<tr>
<td></td>
<td>• Hidden site property is ignored.</td>
</tr>
<tr>
<td></td>
<td>• You can re-create the same effect using the partition hierarchy created by the migration.</td>
</tr>
<tr>
<td></td>
<td>• “Inherit parent permission entries” when it is set to false.</td>
</tr>
<tr>
<td></td>
<td>• Multi-site membership</td>
</tr>
<tr>
<td></td>
<td>• Since site hierarchies are migrated as area hierarchies and partition hierarchies, only the first three site membership are covered by partitions.</td>
</tr>
<tr>
<td><strong>Logical IDs</strong></td>
<td>Logical IDs for all unit devices except for cameras.</td>
</tr>
<tr>
<td><strong>Macros</strong></td>
<td>• All macros</td>
</tr>
<tr>
<td></td>
<td>• Hot macro configurations for each user</td>
</tr>
</tbody>
</table>
This section explains how to migrate AutoVu versions 4.3 and earlier to Security Center. This section includes the following topics:

- "Differences between Security Center and AutoVu 4.3" on page 58
- "AutoVu migrating process" on page 59
- "Setting up the LPR Manager role" on page 60
- "Changing the location of the LPR Manager database" on page 63
Differences between Security Center and AutoVu 4.3

Security Center is the unified platform for managing all fixed and mobile Sharp units. The mobile Sharp units are vehicle mounted Sharp units for Law Enforcement and Parking Enforcement.

The following changes have been made to AutoVu for Security Center:

- Back Office is replaced by Security Center.
- Management of all LPR data (reads, hits, vehicle positions) is handled by the LPR Manager role in Security Center.
- Back Office desktop is replaced by Security Desk.

**NOTE** The migration from AutoVu to Security Center 5.0 was not supported in 5.0 LA release. The following procedure is described for 5.0 GA release.
AutoVu migrating process

To migrate from an earlier version (4.3 SR2) of AutoVu to Security Center 5.0, do the following:

1. Set up an LPR Manager role in Security Center.
   The LPR Manager will gradually replace the AutoVu Back Office.
   The migration is likely to take a few days, if not weeks. While you are performing the migration, your old AutoVu system remains fully operational.
   For more information, see Setting up the LPR Manager role on page 60.

2. Upgrade all Sharp units and Patrollers to 5.0.
   One by one, upgrade the Sharp Plate Reader Server and Patroller applications to 5.0.
   Once a fixed Sharp unit or a Patroller (including its connected Sharp units) is upgraded to 5.0, it can no longer offload data to the AutoVu Back Office. The LPR Manager role will immediately take charge of these units.
   For upgrade instructions, see the following guides:
   - AutoVu Hardware Installation Guide for Sharp units upgrade.
   - AutoVu Patroller Administrator Guide for Patroller application upgrade.
   For instructions on how to manage upgraded LPR units in Security Center, see the following guides:
   - LPR unit configuration in the Security Center Administrator Guide, for Sharp units.
   - Patroller configuration in the Security Center Administrator Guide, for Patrollers.

3. (Optional) Copy the MapInfo files to the Maps folder.
   If you are using MapInfo in Security Desk, copy your MapInfo files to a folder named Maps under the Security Center installation folder. For example: C:\Program Files\Genetec Security Center 5.0\Maps.
   Repeat this operation on every Security Desk workstation where MapInfo maps will be used.

4. Turn off the old system.
   Once the upgrade to Plate Reader Server 5.0 and Patroller 5.0 is complete, let both systems run for a few additional days (at least 3) before turning your old system off.
   This precaution is to give enough time to the old system to finish processing all LPR data and to the new system to import them before turning the switch off.
   To estimate how long you should wait before turning the old system off, see "Setting up the LPR Manager role" on page 60.
Setting up the LPR Manager role

This section describes how to set up the LPR Manager role as a replacement for AutoVu Back Office.

1. Install Security Center.
   
   For more information, see Installing Security Center 5.0 on page 11.

2. Create an LPR Manager role on your Security Center system.

   LPR Manager in Security Center is the role that replaces AutoVu Back Office.
   
   For instructions on how to create and configure an AutoVu LPR Manager, see “AutoVu setup process overview” in the Security Center Administrator Guide.
   
   If you need to move the LPR Manager database to a different location than the default one, see “Changing the location of the LPR Manager database” on page 63.

3. Configure the LPR data retention periods on the LPR Manager.

   In earlier AutoVu Back Office, the following parameters were used to set the LPR data retention period:
   
   - DBCleaner.FlagDayForCleanup (for reads, unit states and Patroller positions)
   - DBCleaner.FlagDayForCleanupHit (for hits)

   In Security Center, the following parameters are used to set the LPR retention period:
   
   - Patroller route retention period
   - Hit retention period
   - Read retention period
   - Event retention period

   The new retention periods must be equal to or longer than the old parameters for all the data to be fully imported into the new system. For example, Read retention period should be greater or equal to FlagDayForCleanup, and Hit retention period should be greater or equal to FlagDayForCleanupHit.

   These settings are found under General settings in the Options tab of the LPR Manager role entity in Config Tool. For more information, see “Configuring the LPR Manager” in the Security Center Administrator Guide.

4. (Optional: for Parking enforcement only). Import zone definitions from the legacy AutoVu system to the new system.

   What used to be called zones in the legacy AutoVu system are called Permits, Permit restrictions, and Overtime rules in Security Center. Each separate rule is represented by an entity in Security Center and they are collectively called LPR rules. For more information about these terms, see the Glossary at the end of the Security Center Administrator Guide.

   Zone import is only supported for AutoVu 4.2 and 4.3 systems. The LPR rules must be manually created for 4.0 and 4.1.
To import the zones:

a Copy the zones.xml file to the Root folder of the LPR Manager.

   The Root folder is defined under General settings in the Options tab of the LPR Manager in Config Tool.

   Once the file is copied, LPR Manager automatically creates the corresponding overtime rules, permits, and permit restrictions in Security Center. The only exception is the long term parking zone. It will not be created automatically for you.

b If a long term parking zone was in use in your legacy AutoVu system, you will have to manually create an Overtime rule in Security Center for it. For more information, see “Configuring overtime rules” in the Security Center Administrator Guide.

c For every Permit entity (list of permit holders) created by the system, you need to configure the path and the parsing of the permit holder data file. For more information, see “Configuring permits” in the Security Center Administrator Guide.

5 Connect LPR Manager to your existing AutoVu Back Office database.

a Select the Options tab of the LPR Manager in the Config Tool.

b Select the Data import option, but do not turn it on yet.

c Configure the Data server and the Database name of the existing Back Office database.

d Turn the Data import option ON and click the Apply button.

The data import starts immediately.

NOTES

The first time you run this migration, the LPR Manager will import everything that is in the existing Back Office database, from the most recent up to the limits of the retention periods defined for the LPR Manager.

Count approximately one hour for every 2.5 GB of data to transfer. For example, if you have 100 GB of data, the whole process will take approximately 40 hours.

As data from the legacy system is imported into Security Center, you can see the Patrollers and LPR units (Sharp units) being created under the LPR Manager in the Config Tool’s role view.

All imported units appear as inactive (red) in Security Center. This is normal. Other than the time zone (under the Location tab), there is not much you can configure for an imported AutoVu Patroller unit.

A few hours after the import process is started, you can start using the data with Security Desk. All legacy data will be associated to the new LPR rules, automatically created by the LPR Manager. The only exceptions are hits associated to long term parking zone. They are associated to the Unknown rule.

For instructions on how to use the Security Desk to view the legacy data, see “LPR investigation” in the Genetec Security Desk User Guide.
After the first round of data import is complete, the process will repeat itself every 12 hours. In the meantime, the old system can operate as usual.

If hotlists were in use in your legacy AutoVu system, corresponding Hotlist entities will be created by the LPR Manager. You need to configure the hotlist data files for each of them. For more information, see “Hotlist configuration” in the **Security Center Administrator Guide**.
Changing the location of the LPR Manager database

The Config Tool always creates the LPR Manager's database at its default location. If you need to move the database to a different location, do the following.

1. Open the SQL Server Management Studio.
   Install it if necessary. The application can be downloaded from Microsoft's web site.
2. Connect to the server containing the database to move.
3. Click the New Query button at the top left of the window.
4. Copy the following script into the query window.
   ```sql
   USE master
   EXECUTE sp_configure 'show advanced options', 1
   RECONFIGURE WITH OVERRIDE
   GO
   EXECUTE sp_configure 'xp_cmdshell', '1' -- use 1 to enable it, 0 to disable it
   RECONFIGURE WITH OVERRIDE
   GO
   EXECUTE sp_configure 'show advanced options', 0
   RECONFIGURE WITH OVERRIDE
   GO
   CREATE TABLE #tempInfo
   (type_desc nvarchar(255),
    name nvarchar(255),
    physical_name nvarchar(255))
   INSERT #tempInfo
   SELECT type_desc, name, physical_name FROM MyDatabase.sys.database_files;
   SELECT * FROM #tempInfo
   ```
5. Replace MyDatabase in the script with the name of the database to move (Ctrl+H).
6. Run the script.
   Make sure the script executed successfully. Otherwise start over.
7. Open a new query window by clicking on the New Query button and copy the follow-
   ing script into the new window.
   ```sql
   ALTER DATABASE MyDatabase SET OFFLINE WITH ROLLBACK IMMEDIATE
   ALTER DATABASE MyDatabase SET ONLINE
   GO
   ```
EXEC sp_detach_db MyDatabase;
GO
DECLARE @cmd nvarchar(255)
DECLARE @res int
SET @cmd = 'if not exist NEWPATH md NEWPATH'
EXEC @res = master..xp_cmdshell @cmd
GO
SELECT
(SELECT MAX(RIGHT(physical_name, CHARINDEX('\\', REVERSE(physical_name))-1))
FROM #tempInfo WHERE type_desc = 'ROWS') AS ROWSDBFILENAME,
(SELECT MAX(RIGHT(physical_name, CHARINDEX('\\', REVERSE(physical_name))-1))
FROM #tempInfo WHERE type_desc = 'LOG') AS LOGDBFILENAME,
(SELECT MAX(RIGHT(physical_name, CHARINDEX('\\', REVERSE(physical_name))-1))
FROM #tempInfo WHERE type_desc = 'FILESTREAM') AS FILESTREAMDBFILENAME

8 Replace ROWSDBNAME in the script by the content of the name column in the row where the content of the type_desc column equals ROWS from the result of the preceding query. (Ctrl+H)

9 Replace LOGDBNAME in the script by the content of the name column in the row where the content of the type_desc column equals LOG from the result of the preceding query. (Ctrl+H)

10 Replace FILESTREAMDBNAME in the script by the content of the name column in the row where the content of the type_desc column equals FILESTREAM from the result of the preceding query. (Ctrl+H)

11 Replace NEWPATH in the script by the path of the desired new database location. The path must not contain the ending back slash. (Ctrl+H)

12 Replace MyDatabase in the script with the name of the LPR Manager database. (Ctrl+H).

13 Run the query.
This could take some time depending on the size of the database. Continue if the query ran successfully.

14 Using Windows Explorer, copy the database files listed as the result of the preceding query to the destination folder.

15 Open a new query window by clicking on the New Query button and copy the following script in the new window:
CREATE DATABASE MyDatabase ON PRIMARY
(
  NAME = ROWSDBNAME,
  FILENAME = 'NEWPATH\ROWSDBFILENAME'
)
FILEGROUP FileStreamGroup1 CONTAINS FILESTREAM
{
NAME = FILESTREAMDBNAME,
FILENAME = 'NEWPATH\FILESTREAMDBFILENAME'
}
LOG ON
{
NAME = LOGDBNAME,
FILENAME = 'NEWPATH\LOGDBFILENAME'
}
FOR ATTACH

DROP TABLE #tempInfo

16 Replace ROWSFFILENANE in the script by the content of the ROWSFFILENANE column from the result of the preceding query. (Ctrl+H)

17 Replace LOGSFFILENANE in the script by the content of the LOGSFFILENANE column from the result of the preceding query. (Ctrl+H)

18 Replace FILESTREAMSFFILENANE in the script by the content of the FILESTREAMSFFILENANE column from the result of the preceding query. (Ctrl+H)

19 Verify that the files were properly copied to the destination folder as executed earlier.

20 Replace MyDatabase in the script with the name of the LPR Manager database. (Ctrl+H)

21 Run the script.