Security Center Administrator Guide 5.5

Copyright notice

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.

All specifications are subject to change without notice.

Document information

Document title: Security Center Administrator Guide 5.5

Document number: EN.500.003-V5.5.C4(1)

Document update date: November 24, 2016

You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.

About this guide

This guide provides the information you need to set up and configure your Security Center system. It explains the basic settings you must configure before your system can be used, as well as other settings you'll need to change such as adding additional users and resources (servers) to your system.

Notes and notices

The following notes and notices might appear in this guide:

- **Tip**. Suggests how to apply the information in a topic or step.
- **Note**. Explains a special case, or expands on an important point.
- **Important**. Points out critical information concerning a topic or step.
- **Caution**. Indicates that an action or step can cause loss of data, security problems, or performance issues.
- **Warning**. Indicates that an action or step can result in physical harm, or cause damage to hardware.

IMPORTANT: Topics appearing in this guide that reference information found on third-party websites were accurate at the time of publication, however, this information is subject to change without prior notice to Genetec Inc.

Contents

Preface: Preface

Part I: Introduction to Security Center

Chapter 1: Security Center at a glance

Chapter 2: Tasks

Chapter 3: Reports

Chapter 4: Keyboard shortcuts

Part II: Common Security Center administration

Chapter 5: Entities

Chapter 6: Servers and roles

Chapter 7: Databases and networks

Chapter 8: High availability

Chapter 9: System automation

Chapter 10: Federation

Chapter 11: Maps

Chapter 12: Plugins

Chapter 13: Health monitoring

Chapter 14: System audits

Part III: System security

Chapter 15: Introduction to system security

Chapter 16: Partitions

Chapter 17: Users and User groups

Chapter 18: TLS and Directory authentication

Chapter 19: Active Directory integration

Chapter 20: Claims-based authentication

Chapter 21: Fusion stream encryption

Part IV: Video

Chapter 22: Video at a glance

Chapter 23: Video deployment

Chapter 24: Cameras

Chapter 25: Video archives

Chapter 27: Access control at a glance

Chapter 28: Access control deployment

Chapter 29: Access control units

Chapter 30: Areas, doors, and elevators

Chapter 31: Cardholders

Chapter 32: Credentials

Chapter 33: Global cardholder management

Chapter 34: Import tool

Chapter 38: Hotlists

Chapter 39: AutoVu™ fixed systems

Chapter 40: AutoVu™ mobile systems

Chapter 46: Threat levels

Chapter 47: Zones and intrusion detection

Part VIII: Config Tool reference

Chapter 48: Entity types

Chapter 49: Role types

Chapter 50: Administration tasks

Chapter 51: Events and actions

Appendices

Part I

Introduction to Security Center

This part includes the following chapters:

- "Security Center at a glance" on page 2
- "Tasks" on page 33
- "Reports" on page 40
- "Keyboard shortcuts" on page 49

1

Security Center at a glance

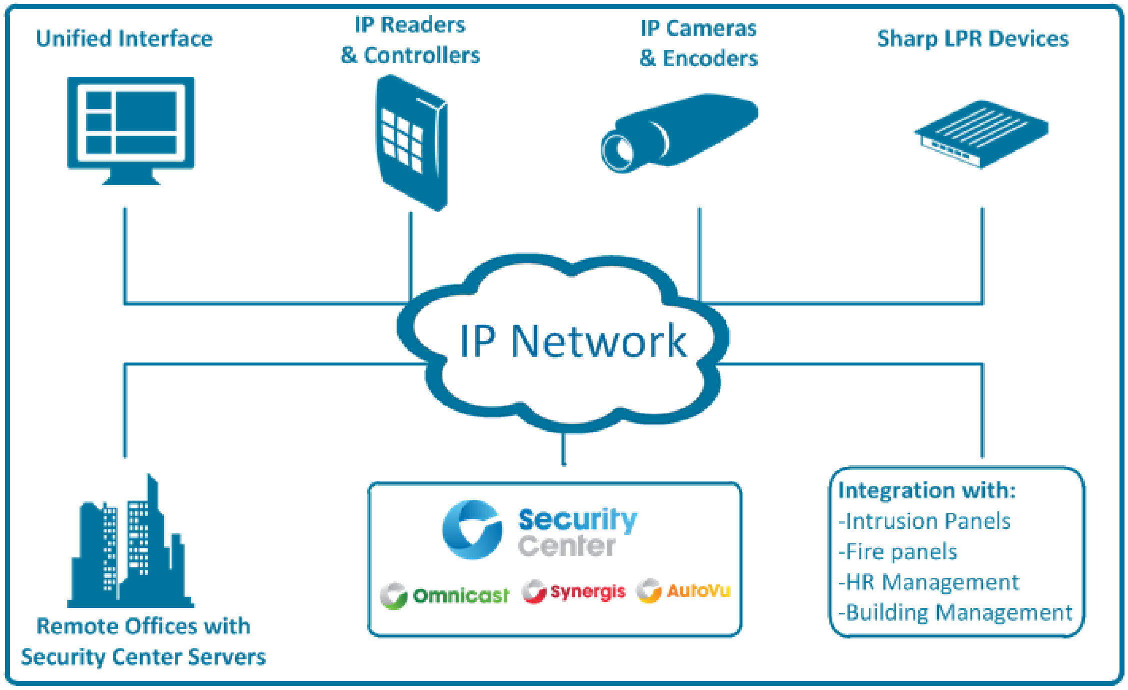
This section includes the following topics:

About Security Center

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

The Security Center unified security platform provides the following:

- One platform controlling and managing video/access/LPR edge devices.
- One user interface for monitoring, reporting, and managing events and alarms for video surveillance, access control, and LPR - *Security Desk*.
- One user interface for configuring video surveillance, access control, and LPR - *Config Tool*.
- Unified live video viewing with video searches and video playback.



Security Center features are divided into four main categories: Common, Video surveillance (Omnicast), Access control (Synergis), and License plate recognition (AutoVu™).

Common/Core features

- Alarm management
- Zone management
- Federation
- Intrusion panel integration
- Report management
- Schedule and scheduled task management
- User and user group management
- Windows Active Directory integration
- Programmable automated system behavior

Omnicast – Video surveillance features

- Full camera configuration and management
- View live and playback video from all cameras
- Full PTZ control using the PC or CCTV keyboard, or on screen using the mouse
- Digital zoom
- Motion detection
- Bookmark any important scene to ease future video archive search and retrieval
- Save and print video snapshots
- Search video by alarm, bookmark, event, motion, or date and time
- View all cameras on independent or synchronized timelines
- Visual tracking: follow individuals or moving objects across different cameras
- Export video
- Protect video against accidental deletion
- Protect video against tampering by using watermarks

Synergis™ – Access control features

- Cardholder management
- Credential management
- Visitor management
- Door management
- Access rule management
- People counting

AutoVu™ – License plate recognition (LPR) features

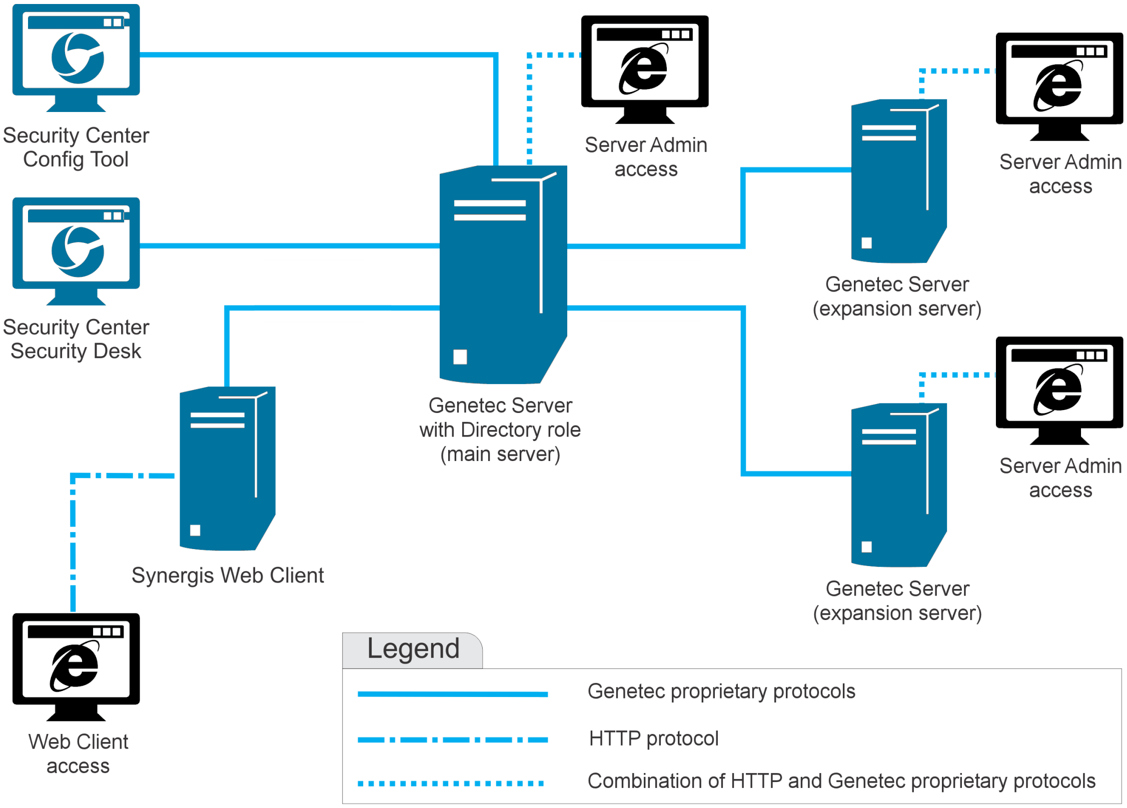
- Fixed and mobile (with Patroller) LPR solution management
- Automatic identification of stolen (or scofflaw) vehicles
- Enforcement of city parking regulations (not involving permits)
- Enforcement of parking lot regulations (involving permits)
- License plate inventory in large parking facilities

Security Center architecture overview

Security Center's architecture is based on a client/server model, where all system functions are handled by a pool of server computers distributed over an IP network.

Every Security Center system must have its own pool of servers. Their number can range from a single machine for a small system to hundreds of machines for a large scale system.

NOTE: The icons colored in blue represent the computers where Security Center server and client components are installed.


Security Center Config Tool
Security Center Security Desk
Server Admin access
Genetec Server with Directory role (main server)
Server Admin access
Genetec Server (expansion server)
Server Admin access
Genetec Server (expansion server)
Synergis Web Client
Web Client access
Legend
Genetec proprietary protocols
HTTP protocol
Combination of HTTP and Genetec proprietary protocols

How Security Center is organized

Security Center is organized by tasks. All tasks can be customized and multiple tasks can be carried out simultaneously. You might not see all the tasks and commands described about Security Center, depending on your license options and user privileges. There are user privileges for each task, and for many commands in Security Center.

Tasks in the home page are organized into the following categories:

- **Administration:** (Config Tool only) Tasks used to create and configure the entities required to model your system.
- **Operation:** Tasks related to day-to-day Security Center operations.
- **Investigation:** (Security Desk only) Tasks allowing you to query the Security Center database, and those of federated systems, for critical information.
- **Maintenance:** Tasks related to maintenance and troubleshooting.

Under each major category, the tasks are further divided as follows:

- **Common tasks:** Tasks that are shared by all three Security Center software modules. These tasks are always available regardless of which modules are supported by your software license.
- **Access control:** Tasks related to access control. Access control tasks are displayed with a red line under their icons. They are only available if *Synergis*™ is supported by your software license.
- **LPR:** Tasks related to *License Plate Recognition*. LPR tasks are displayed with an orange line under their icons. They are only available if *AutoVu*™ is supported by your software license.
- **Video:** Tasks related to video management. Video tasks are displayed with a green line under their icons. They are only available if *Omnicast*™ is supported by your software license.

Logging on to Security Center

To log on to Security Center, you must open Config Tool and connect to the Security Center *main server*.

Before you begin

You need your username, password, and the name of the *Directory* you want to connect to.

What you should know

Once you are logged on, you can disconnect from the Directory without closing Config Tool. Logging off without closing the application is helpful if you plan to log on again using a different username and password.

IMPORTANT: If *Active Directory integration* has been set up by your system administrator, and you are connecting over a VPN connection, you must clear the **Use Windows credentials** check box and type your username in the format *DOMAIN\Username*.

NOTE: More logon options are available when an Active Directory is integrated to Security Center.

To log on to Security Center:

1 To open Config Tool, click **Start** > **All Programs** > **Genetec Security Center5.5** > **Config Tool**.

2 In the **Logon** dialog box, do one of the following:

- If you have just installed Security Center, log on with the default administrative user **Admin** with a blank password.
- Enter your Security Center username and password.

3 In the **Directory** field, enter the name or IP address of your main server.

NOTE: If you are running Config Tool on your main server, you can leave the **Directory** field blank.

4 Click **Log on**.

5 To log off, click the **Home** (🏠) tab, and then click **Log off**.

Related Topics

Logging on to Security Center using an Active Directory user on page 329

Closing Config Tool

You can close Config Tool and save your workspace for the next time you log on.

What you should know

There are also some options you can customize for when you are closing Config Tool from the Options dialog box.

To close Config Tool:

1 In the upper-right corner of the Config Tool window, click **Exit** (⊗).

If you have unsaved tasks in your workspace, you are prompted to save them.

2 To automatically load the same task list the next time you open Config Tool, click **Save**.

Related Topics
Defining how your workspace is saved on page 8

Defining how your workspace is saved

To ensure that changes to your workspace are always treated in the same manner upon closing, you can define how you want your applicaton to behave regardless of whether you have unsaved changes in your task list.

What you should know

This setting is saved as part of your user profile and applies to Security Desk and Config Tool.

To define the save actions of your workspace:

1 From the home page, click **Options** > **User interaction**.

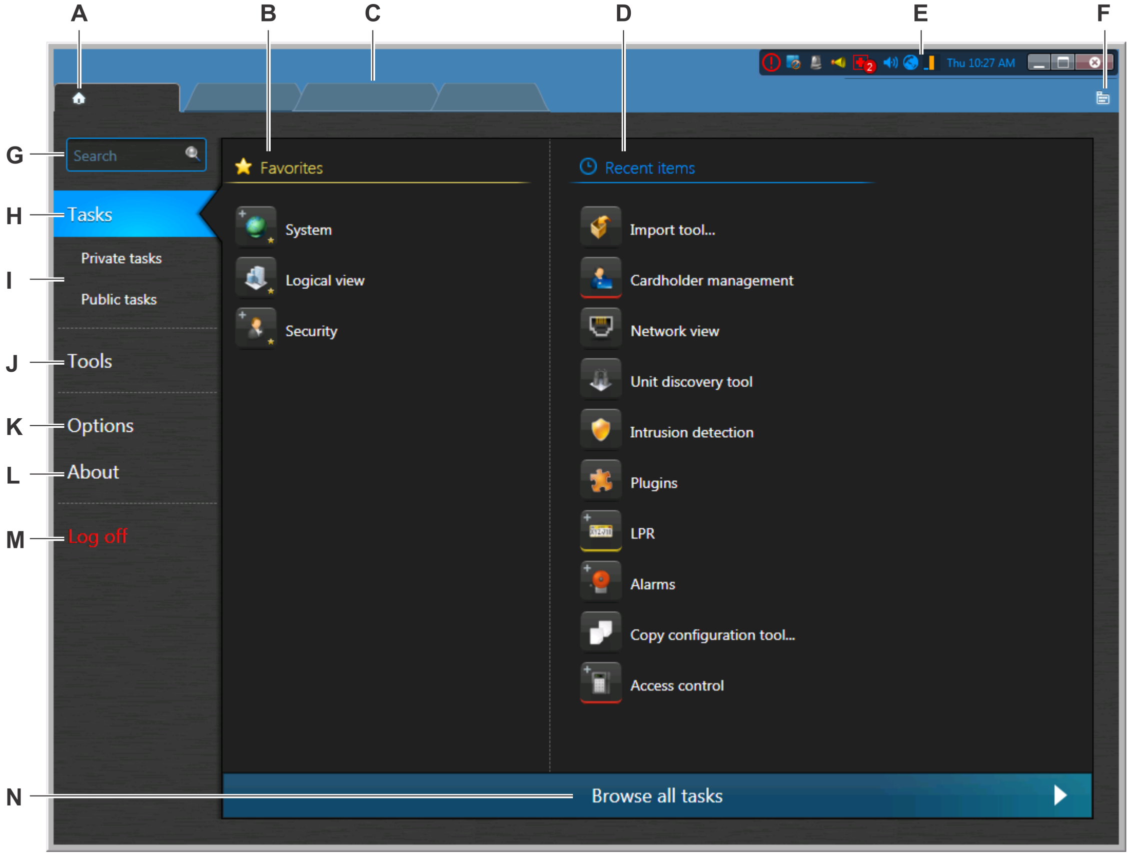
2 From the **Save the task list** drop-down list, select one of the following options:

- *Ask user*. Ask you before saving your task list.
- *Yes*. Save the workspace without asking you.
- *No*. Never save the workspace.

3 Click **Save**.

Home page overview

The home page is the main page. You can open the home page by clicking the home tab (🏠). It is also shown if the task list is empty.



A Home tab	- Click to show or hide the home page. - Right-click for a list of commands (for example, save the workspace, close tasks, and so on).
B Favorites	Right-click any task or tool to add or remove it from your *Favorites* list. You can also drag a task into this list. Tasks listed in your *Favorites* no longer appear in the *Recent items* list.
C Task list	Lists the tasks you currently have open and are working on. - Click a task tab to switch to that task. - Right-click a tab for a list of commands.
D Recent items	Lists your recently opened tasks and tools.
E Notification tray	Displays important information about your system. Hold your mouse pointer over an icon to view system information, or double-click the icon to perform an action. From the *Options* dialog box, you can choose which icons you want to have appear in the notification bar.

F	**List all tasks**	Click to view a list of all open tasks. This button only appears if the task tabs occupy the entire width of the taskbar.
G	**Search box**	Type the name of the task you are looking for. All tasks containing that text in their category, name, or description, are shown.
H	**Tasks**	Lists your recent items, favorites, and all the task types that are available to you. Select a task to open from this tab.
I	**Private tasks**, **Public tasks**	Click to view the saved tasks that are available to you. • **Private tasks**. A private task is a saved task that is only visible to the user who created it. • **Public tasks**. A public task is a saved task that can be shared and reused among multiple Security Center users.
J	**Tools**	Click to view the tools that you can start directly from your home page. The Tools page is divided into the following two sections: • **Tools**. This section shows the standard Security Center tools. • **External tools**. This section shows the shortcuts to external tools and applications.
K	**Options**	Click to configure the options for your application.
L	**About**	Click to view information regarding your Security Center software, such as your license, SMA, and software version.
M	**Log off**	Click to log off without exiting the application.
N	**Browse all tasks**	Click to view all the tasks that are available to you. Click a task icon to open the task. If it is a single-instance task, the task opens. If you can have multiple instances of the task, you are asked to type a name for the task.

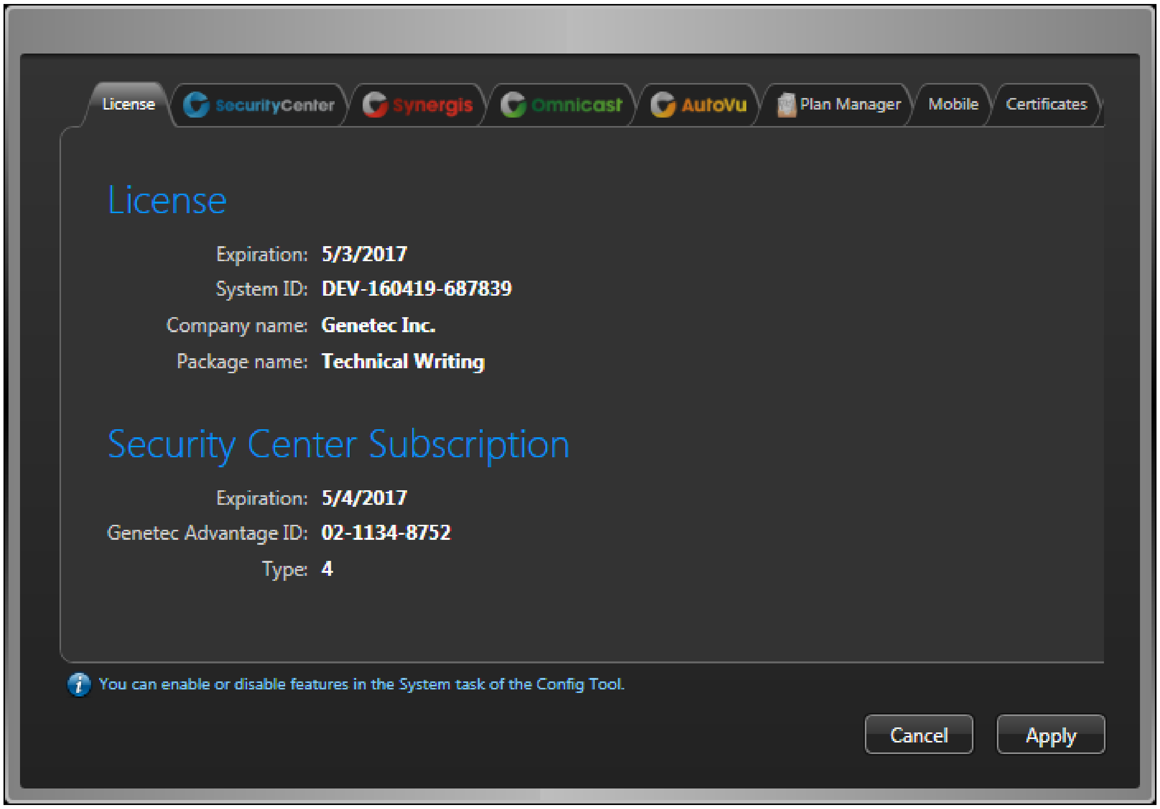
Related Topics

Configuring the notification tray on page 24
Saving tasks on page 35
Opening tasks on page 34
Shortcuts to external tools on page 31

Overview of the About page

The About page displays information regarding your Security Center software, such as your purchased license, SMA number, license expiration date, software version, and so on.

All license options are either supported, unsupported, or limited by a maximum use count. For options with a maximum use count, Config Tool shows the current use vs. the maximum allowed.



License

Expiration: 5/3/2017
System ID: DEV-160419-687839
Company name: Genetec Inc.
Package name: Technical Writing

Security Center Subscription

Expiration: 5/4/2017
Genetec Advantage ID: 02-1134-8752
Type: 4

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

The following tabs are available, depending on what your license supports:

- **License:** Indicates when your software license expires, and gives you the information you need to provide when contacting Genetec™ Technical Assistance Center: System ID, Company name, Package name, and your Service maintenance agreement (SMA) number.

  IMPORTANT: Thirty days before the expiry of either your license or your SMA, you'll receive a message in Config Tool alerting you that your license or your SMA is about to expire. Config Tool connects to GTAP to validate the SMA.
- **Security Center:** This tab shows all generic Security Center options.
- **Synergis:** This tab shows all the access control options. It is shown only if *Synergis™ (access control)* is supported.
- **Omnicast:** This tab shows all the video options. It is shown only if *Omnicast (video surveillance)* is supported.
- **AutoVu:** This tab shows all the LPR options. It is shown only if *AutoVu (LPR)* is supported.
- **Plan Manager:** This tab shows the Plan Manager options.
- **Mobile:** This tab shows all the Security Center Mobile options. It is shown only if Security Center Mobile is supported.
- **Certificates:** This tab lists the *SDK certificates* included in this license key.

- **Purchase order:** This tab reproduces your order.

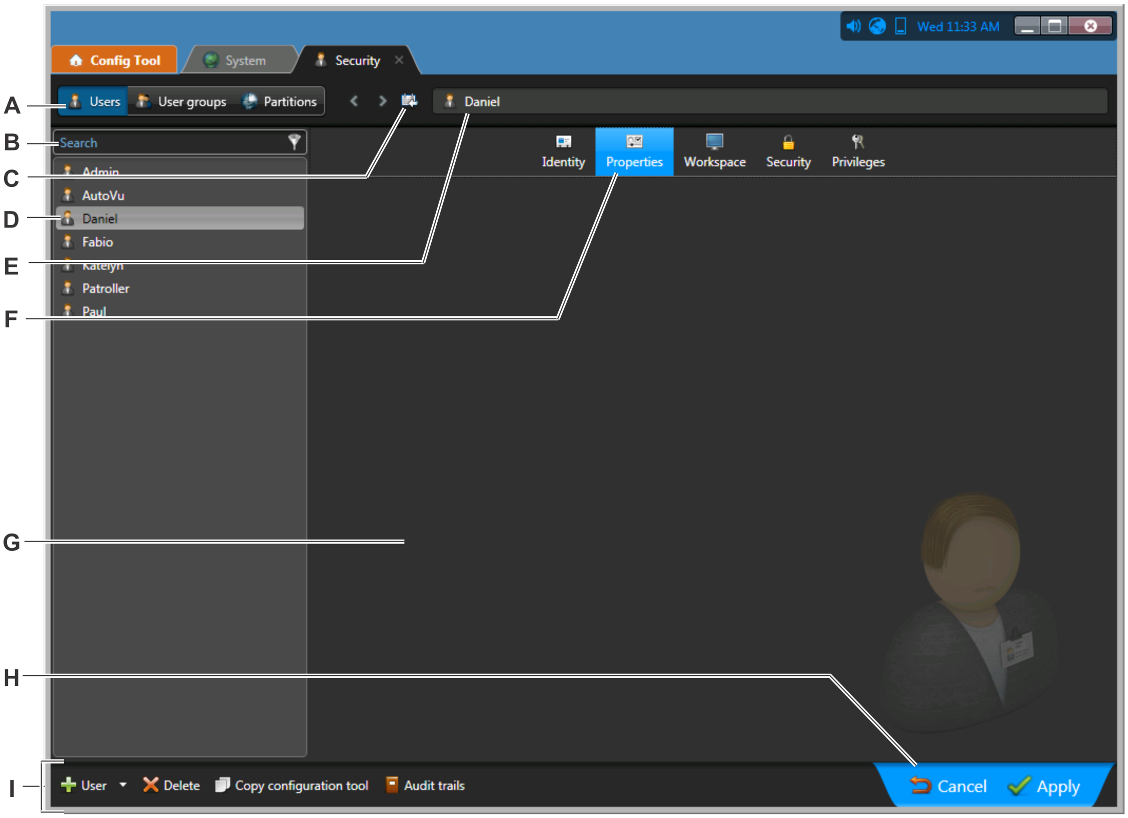
On the About page, the following buttons are also available:

- **Help:** Click to open the online help. You can also click F1.
- **Change password:** Click to change your password.
- **Contact us:** Click to visit GTAP or the GTAP forum. You need an Internet connection to visit these websites.
- **Installed components:** Click to view the name and version of all installed software components (DLLs).
- **Copyright:** Click to display software copyright information.
- **Send feedback:** Click to send us feedback.

Administration task workspace overview

Administration tasks are where you create and configure the *entities* required to model your system.

This section takes you on a tour of the administration task layout, and describes the common elements of most administration tasks. The *Security* task was used as an example. You can open the *Security* task by typing its name in the *Search* box on the home page.



A	**Entity views**	Views for each entity type managed by the task.
B	**Entity filter**	Type a string in this field and press *ENTER* to filter the entities in the browser by name. Click *Apply a custom filer* (Y) to pick the entities you want to show in the browser.
C	**Entity history**	Use these buttons to browse through recently used entities within this task.
D	**Entity browser**	Click an entity in the browser to show its settings on the right.
E	**Current entity**	The icon and name of the selected entity is displayed here.
F	**Configuration tabs**	The entity settings are grouped by tabs.
G	**Configuration page**	This area displays the entity settings under the selected configuration tab.

H	**Apply/cancel changes**	You must *Cancel* or *Apply* any change you make on the current page before you can move to a different page.
I	**Contextual commands**	Commands related to the selected entity are displayed in the toolbar at the bottom of the workspace.

Contextual commands in administration tasks

Commands related to the selected entity in the browser are displayed at the bottom of the task workspace in administration tasks.

The following table describes all the contextual commands in alphabetical order.

Icon	Command	Applies to	Description
	Activate role	All roles	Activate the selected role.
	Add a cardholder	Access rules and cardholder groups	Create a cardholder and assign it to the selected entity.
	Add a credential	Cardholders	Create a credential and add it to the selected cardholder.
✚	**Add an entity**	All entities	Create an entity.
	Assign to new door	Access control units	Create a door and assign it to the selected access control unit.
	Audit trails	All entities	Create an Audit trails task for the selected entity to find out which users made changes on the system.
⚠	**Conflict resolution**	Active Directory role	Open the Active Directory conflict resolution dialog box to resolve conflicts caused by imported entities.
	Copy configuration tool	All entities	Open the Copy configuration tool.
	Create an access rule	Areas, doors, elevators	Create an access rule and assign it to the selected entity.
	Deactivate role	All roles	Deactivate the selected role.
✖	**Delete**	All entities	Delete the selected entity from the system. Discovered entities can only be deleted when they are inactive.
✚	**Diagnose**	All roles, and some entities	Perform a diagnosis on the selected role or entity.
	Disable support logs	Access Manager and access control units	Disable support logs if requested by Genetec™ Technical Assistance.

Icon	Command	Applies to	Description
	Enable support logs	Access Manager and access control units	Enable support logs if requested by Genetec™ Technical Assistance.
	Health statistics	Roles and physical devices	Creates a Health statistics task for the selected entity to view the health status and availability of entities.
	Identify	Video units	Flash an LED on the selected unit to help locate it on a rack.
	Live video	Cameras	Open a dialog box showing live video from the selected camera.
	Maintenance mode	Roles and physical devices	Set a role or a physical device in maintenance mode so that its downtime does not affect its availability calculation from the Health Monitor.
	Move unit	Video and access control units	Open the Move unit tool, where you can move units from one manager to another.
	Ping	Video units	Ping the video unit to check if you can communicate with it. This is helpful for troubleshooting purposes.
	Print badge	Cardholders and credentials	Select a badge template and print a badge for the selected cardholder or credential.
	Reboot	Video and access control units	Restart the selected unit.
	Reconnect	Video units	Remove the selected video unit from the Archiver and add it again.
	Run macro	Macros	Run the selected macro.
	Trigger alarm	Alarms	Trigger the selected alarm so it can be viewed in Security Desk.
	Unit enrollment tool	Video and access control units	Open the Unit enrollment tool, where you can find IP units connected to your network.
	Unit's web page	Video units	Open a browser to configure the unit using the web page hosted on the unit.

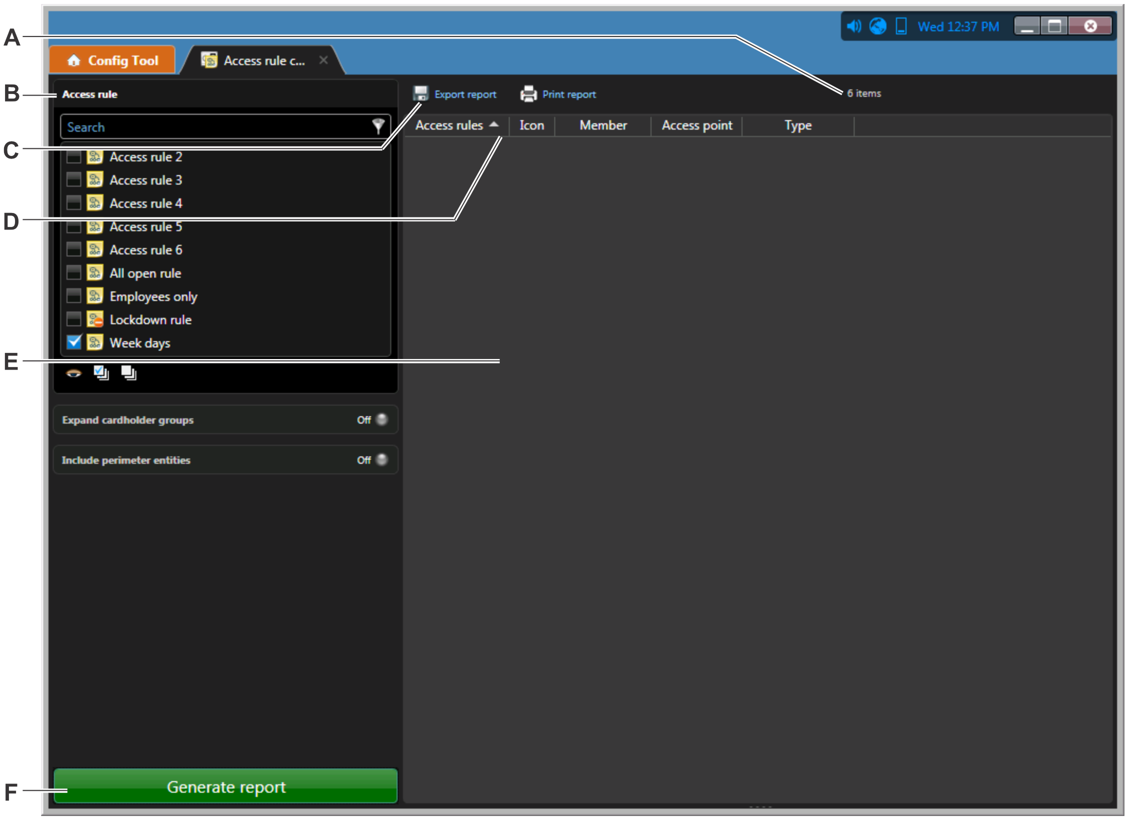
Related Topics

Finding out what changes were made to the system configuration on page 269
Resolving conflicts caused by imported entities on page 327
Copying configuration settings from one entity to another on page 60
Setting entities in maintenance mode on page 245
Creating macros on page 187
Testing alarms on page 740

Maintenance task workspace overview

Maintenance tasks are where you generate customized queries on the entities, activities, and events in your Security Center system for maintenance and troubleshooting purposes.

This section takes you on a tour of the maintenance task layout, and describes the common elements of most maintenance tasks. The *Access rule configuration* task was used as an example. You can open the Access rule configuration task by typing its name in the *Search* box on the home page.



A	**Number of results**	Displays the number of returned results. A warning is issued when your query returns too many rows. If this happens, adjust your query filters to reduce the number of results.
B	**Query filters**	Use the filters in the query tab to set up your query. Click on a filter heading to turn it on (●) or off. Invalid filters display as *Warning* or *Error*. Hover your mouse over the filter to view the reason it is invalid.
C	**Export/print report**	Click to export or print your report once it is generated.
D	**Select columns**	Right-click a column heading to select which columns to display.

E	**Report pane**	View the results of your report. Drag an item from the list to a tile in the canvas, or right-click an item in the list to view more options associated with that item, if applicable.
F	**Generate report**	Click to run the report. This button is disabled if you have not selected any query filters, or when you have invalid filters. While the query is running, this button changes to *Cancel*. Click on *Cancel* to interrupt the query.

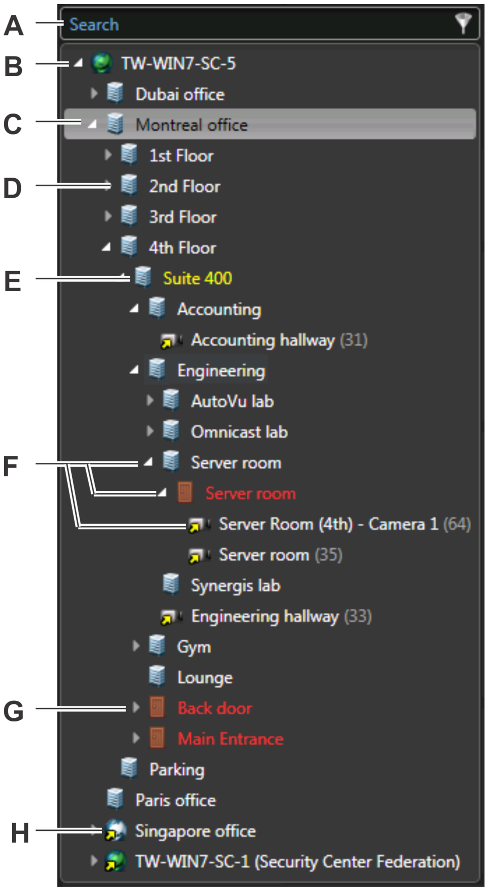
About the area view

Using the area view, you can find and view all the entities in your system quickly.

The *entities* in the area view are organized in a hierarchy (or *entity tree*) according to their logical relationships with *areas*. For example, the doors leading to an area, and other devices located within the area, such as cameras, are displayed below that area in the hierarchy as *child entities*.

From the area view, you can do the following:

- Find entities you want to view in the canvas.
- Drag multiple entities from the area view into the canvas.
- Rename local entities.
- Jump to entity configuration pages, if you have the required privileges.



A	**Search box**	Type in the *Search* box to find the entities containing that text in their category, name, or description.
B	**System entity**	The system entity (🌐) cannot be viewed in the canvas.
C	**Additional commands-**	Right-click an entity in the area view to use additional commands, such as creating or deleting entities, diagnosing the selected entity, launching a report on the selected entity, or refreshing the area view.
D	**Area entity**	Area entities (🗄) can represent a concept or physical location. It is a logical grouping.

E	**Yellow entity**	Whenever an entity name is displayed in yellow, it means that there is a problem with the settings.
F	**Arrow icons**	Click the arrows in the entity tree to show or hide child entities.
G	**Red entity**	Indicates that the entity is offline and the server cannot connect to it, or the server is offline.
H	**Federated entity**	All entities imported from *federated systems* are shown with a yellow arrow superimposed on the regular entity icon (↗). They are called *federated entities*.

Related Topics

Searching for entities on page 58

About areas

An area is a type of entity that represents a concept or a physical location (room, floor, building, site, and so on) used for grouping other entities in the system.

You can use areas to group system entities logically or to prevent unauthorized users from viewing selected system entities. A secured area is an area entity that represents a physical location where access is controlled. A secured area consists of perimeter doors (doors used to enter and exit the area) and access restrictions (rules governing the access to the area).

Related Topics

Organizing the area view on page 21
Defining who can access Security Center on page 278
About secured areas on page 523

Organizing the area view

As the system administrator, you need to create an area view structure that is easy for everyone to understand and navigate.

What you should know

You can re-organize the entities in the area view by dragging them to another area, selecting multiple entities at once and drag them to another area, renaming entities, and copying entities. You can also create and delete entities.

NOTE: You cannot edit the names of federated entities.

The way you structure the area view in Config Tool is also how it is displayed in Security Desk.

To organize the area view:

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

   NOTE: The area view *task* in Config Tool is the only place where you can change the area view structure. Do not confuse this administrative task with the area view *tab* found in most investigation tasks available in Security Desk.

2. To move entities under another area, do one of the following:
   - Select an area or entity, and then drag it to a different area.
   - Hold the **SHIFT** key, select multiple entities, and then drag them to a different area.

   The selected entities are now a child entities of that area (below that area in the hierarchy).
3. To rename an entity, select the entity, press **F2**, type a new name, and press **ENTER**.

   TIP: You can rename any entity from the area view of any task as long as you have the administrative privilege to modify that entity.

4. To copy an entity into another area, hold the **CTRL** key, and then drag the entity into that area.

   A copy of the entity is created under the area. If you copied an area under another area, all its child entities (entities below that area) are also copied.
5. If necessary, create new areas for grouping entities.
6. If necessary, delete entities.

Creating areas

To organize the area view, use areas to group entities based on their logical or physical relationship.

What you should know

An area is a concept or a physical location (room, floor, building, site, and so on) that is used for the logical grouping of entities in the system.

You can create new areas anywhere in the area view hierarchy.

To create an area:

1 Open the **area view** task.

2 Click a partition (🌐) or an area entity (🏢) you want to create the new area under.

3 Click **Add an entity** (➕) > **Area**.

4 Type a name for the area, and press **ENTER**.

After you finish

If you are defining an area for access control, then secure the area.

Related Topics
Organizing the area view on page 21

Turning features on and off

To simplify your interface, you can turn off the features you are not using.

To turn features on or off:

1 Open the **System** task, click **General settings** view, and click the *Features* page.

2 Select the features you want to use and clear the options of the features you want to turn off.

   NOTE: You can only select from features that are supported by your license. Unsupported features are not listed.

3 Click **Apply**.

Example

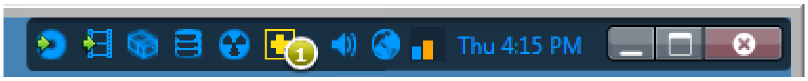
Active Directory integration is a feature that is supported by default in your license. However, if you do not plan on importing users from a Windows Active Directory, then you can turn off the Active Directory feature so the Active Directory role is no longer available.

Configuring the notification tray

You can choose which icons to display in the notification tray.

What you should know

The notification tray appears in the upper-right corner of the application by default.



The notification tray settings are saved as part of your user profile and apply to Security Desk and Config Tool.

BEST PRACTICE: It is a good idea to show the icons that you use on a daily basis, so you can easily jump to the associated tasks.

To customize the notification tray icons:

1 From the home page, click **Options** > **Visual**.

2 From the drop-down list beside the icons in the **Tray** section, select how you want to display each item:

- **Show:** Always show the icon.
- **Hide:** Always hide the icon.
- **Show notifications only:** Only show the icon when there is a notification.

3 Click **Save**.

Related Topics
Home page overview on page 9

Notification tray icons

The following table lists the notification tray icons, and what you can use them for.

Icon	Name	Description
9:53 AM	**Clock**	Shows the local time. Hover your mouse pointer over that area to see the current date in a tooltip. You can customize the time zone settings.
▮	**Resources meter**	Shows the usage of your computer resources (CPU, Memory, GPU, and Network). Hover your mouse pointer over the icon to view the resources usage in percentages. Click to open the Hardware information dialog box to view addtional information and troubleshooting hints.
🌐	**Session info**	Shows the current username and Security Center Directory name. Click to toggle between the long and short display.
🔊	**Volume**	Shows the volume setting (0 to 100) of Security Desk. Click to adjust the volume using a slider, or to mute the volume.

Icon	Name	Description
✚	**System messages**	Shows the number of current system messages (health issues, warnings, messages, and health events) on your system. Click to open the System messages dialog box to read and review the messages. If there are health issues, the icon turns red (✚6). If there are warnings, the icon turns yellow. If there are only messages, the icon turns blue. For more information, see Viewing system messages on page 247.
☢	**Firmware upgrade**	Appears only when there are unit firmware upgrades currently under way. The upgrade count is displayed over the icon. Click the icon to view the details.
☰	**Database actions**	Appears only when there are database upgrades currently under way. The upgrade count is displayed over the icon. Click the icon to view the details.
▣	**Add unit status**	Appears only when there are newly added units in the system. The unit count is displayed over the icon. Click the icon to view the details.
◌	**Background process**	Indicates that a process is running in the background, such as video files being exported. Click the icon to view more details about the specific process that is running.
▭	**Card requests**	Shows the number of pending requests for credential cards to be printed (▭1). Click to open the *Card requests* dialog box and respond to the request. For more information, see Responding to credential card requests on page 565.
▤	**Video file conversion**	Shows the number of G64 or G64x files currently being converted to ASF or MP4 format. Click to open the Conversion dialog box and view the status of the conversion. When the icon changes to ▤✓, the file conversion is complete. For more information about converting G64 files to ASF or MP4 format, see the *Security Desk User Guide*.

Related Topics

Creating databases on page 123
Deleting databases on page 124
Backing up databases on page 127
Restoring databases on page 129

Changing passwords

After you log on to Security Center, you can change your password.

What you should know

As a best practice, it is recommended to change your password regularly.

To change your password:

1 From the home page, click **About**.
2 In the *About* page, click **Change password**.
3 In the **Change password** dialog box, enter your old password, then enter your new password twice.
4 Click **OK**.

Opening Security Desk from Config Tool

You can open the Security Desk application from the *Tools* page in Config Tool.

What you should know

When you open Security Desk application from Config Tool, you are logged on using the same credentials you are currently logged on with.

To open Security Desk from Config Tool:

- From the Config Tool home page, click **Tools** > **Security Desk** ().

Sending feedback

You can send feedback to Genetec Inc. if there is something you want to bring to our attention, such as an issue in the interface or a setting that is unclear.

To send feedback:

1 From the home page, click **About** > **Send feeback**.

2 In the *Send feedback* dialog box, type your feedback.

3 To add attachments, click **Attachments** and select from the following options:

- To attach system information, select **System information**.
- To attach files such as a log file, select **Files**, click ➕, select a file, and click **Open**.
- To attach a screenshot of your current screen, select **Screenshots**, and click ➕.

  TIP: You can move the feedback dialog box over to the side and navigate to the relevant screen to take your screenshot while it is still open.

4 Click **Send**.

Collecting diagnostic data

For troubleshooting purposes, the *Diagnostic Data Collection Tool* conveniently collects and packages system information so that you can easily send it to Genetec™ Technical Assistance.

Before you begin

To run the Diagnostic Data Collection Tool:

- You must have Windows administrative privileges on your computer.
- You must have Security Center administrative privileges.
- All clients and servers must be at version 5.3 SR1 or later.

What you should know

- The tool collects different types of system information (collection types), such as Genetec system information, Archiver collection and Video inventory. See the steps below for a complete list of these collections and what they contain.
- Running the Diagnostic Data Collection tool may temporarily impact system performance.
- If your system is running Windows XP or 2003, Windows event logs and performance monitor data are not collected.

To collect diagnostic information:

1 From the Home page, click **Tools** > **Diagnostic Data Collection Tool.**

2 From the dialog box, select one of the following:

  - **Default data collection on all Security Center servers:** Sends only a set of predefined data collections (default)"
  - **Specific data collection and servers:** Sends a set of data collection and server information that you have selected.

3 If selecting **Specific data collection and servers**, do the following:

  a) On the left pane, select the server(s) you need information from.

  b) On the right pane, select the specific collection type(s) from that server.

  You can select from the following collections:

  - **System Information Collection (default):** A data collection used for diagnostic testing that includes system logs and system information not specific to Genetec applications. This collection contains:
    - Genetec Event logs
    - System Event logs
    - Application Event logs
    - Security Event logs
    - Installed applications
    - Installed updates
    - Currently running applications
    - Currently active network connections
    - .NET CLR assemblies required for debugging
  - **Genetec System Information Collection (default):** A data collection used for diagnostic testing that includes Genetec applications specific information. It contains:
    - Security Center configuration files
    - Security Center trace logs

    - Security Desk and Config Tool error logs (when the clients are selected)
    - Performance monitor data
    - Running processes information
    - Security Center running processes information with loaded assemblies
    - Memory dumps
    - Registry Keys (only the ones that are used or created by Genetec)
  - **Archiver collection:** A data collection used for diagnostic testing that includes Genetec Archiver specific information such as Archiver cache and Archiver logs.
  - **Access Manager collection:** A data collection used for diagnostic testing that includes Genetec Access Manager specific information. It includes configuration files, currently active network connections, VertX file cache and VertX temp files.
  - **Video Unit Inventory:** A data collection used for diagnostic testing that lists video units enrolled by the system and Security Center federated cameras

4. Click **Start**.

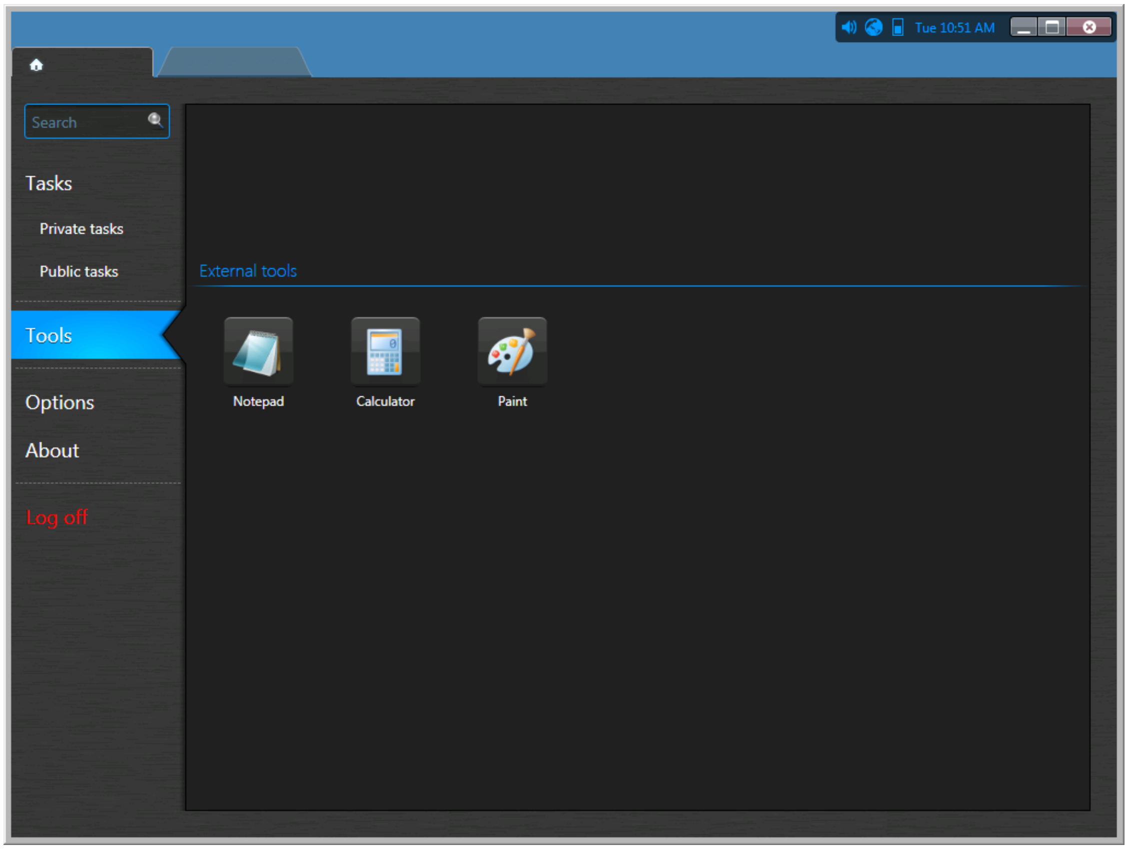
   The status bars show the progress for each data collection. The information is saved on the computer from which the tool was run to folder: *C:\ProgramData\Genetec Security Center 5.5\Diagnostics*. For Windows XP and 2003, the data is saved in: *C:\Documents and Settings\All Users\Application Data\Genetec Security Center 5.5\Diagnostics*.
5. To open the folder, click **Open drop folder**.

You can now send the diagnostic information to Genetec™ Technical Assistance.

Shortcuts to external tools

You can add shortcuts to frequently used external tools and applications to the Tools page in Security Center, by modifying the *ToolsMenuExtensions.xml* file.

This file is located in *C:\Program files (x86)\Genetec Security Center 5.5* on a 64-bit computer, and in *C:\Program files\Genetec Security Center 5.5* on a 32-bit computer.



The original content of this file looks as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfToolsMenuExtension xmlns:xsi="http://www.w3.org/2001/XMLSchema-...>
    <ToolsMenuExtension>
    </ToolsMenuExtension>
</ArrayOfToolsMenuExtension>
```

Each shortcut is defined by an XML tag named `<ToolsMenuExtension>`. Each `<ToolsMenuExtension>` tag can contain four XML elements:

- `<Name>` – Command name displayed in the Tools page.
- `<FileName>` – Command to execute (executable file).
- `<Icon>` – (Optional) Alternate icon file (.ico). Use this element to override the default icon extracted from the executable file.
- `<Arguments>` – (Optional) Command line arguments when applicable.

All XML tag names are case sensitive. You can edit this XML file with any text editor. Changes to this file only become effective the next time you launch Security Desk.

NOTE: If a full path is not provided in the `<FileName>` tag, the application is not be able to extract the icon associated with the executable. In this case, explicitly supply an icon with the `<Icon>` tag.

Example

The following sample file adds the three shortcuts (*Notepad*, *Calculator*, and *Paint*) to the Tools page. The *Notepad* shortcut is configured to open the file *C:|SafetyProcedures.txt* when you click on it.

```
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfToolsMenuExtension xmlns:xsi="http://www.w3.org/2001/XMLSchema-...>
    <ToolsMenuExtension>
        <Name>Notepad</Name>
        <FileName>c:\windows\notepad.exe</FileName>
        <Arguments>c:\SafetyProcedures.txt</Arguments>
    </ToolsMenuExtension>
    <ToolsMenuExtension>
        <Name>Calculator</Name>
        <FileName>c:\windows\system32\calc.exe</FileName>
    </ToolsMenuExtension>
    <ToolsMenuExtension>
        <Name>Paint</Name>
        <FileName>c:\windows\system32\mspaint.exe</FileName>
    </ToolsMenuExtension>
</ArrayOfToolsMenuExtension>
```

2

Tasks

This section includes the following topics:

Opening tasks

To do most things in Security Center, you must first open your tasks.

What you should know

Some Security Center tasks can only have one instance, and other tasks can have multiple instances. Single-instance tasks cannot be renamed.

To open a task:

1. From the home page, do one of the following:
   - Type the task name in the *Search* box.
   - Click the *Tasks* tab, and then click **Browse all tasks**
   - To open a saved task, click the **Private tasks** or **Public tasks** tab.
2. Click the task.
   If only one instance of the task is allowed, the new task is created.
3. If more than one instance of the task is allowed, enter the task name, and click **Create**.
   The new task opens and is added to your task list.
4. (Only Administration tasks) If the task contains more than one entity view, select a view to configure.
   Tasks that allow you to configure more than one entity are indicated with a plus sign on the task icon.

Related Topics
Home page overview on page 9

Saving tasks

You can save your tasks in a private task list that only you can access, or in a public task list that everyone can access.

What you should know

When you save a task, the query filter settings, the task layout (report pane column order, canvas layout, and so on), and the entities displayed in each tile are also saved.

NOTE: The query results are not saved. They are regenerated every time you run the query.

The benefits of saving a task are:

- You can close your task, and reload it with the same layout when you need it.
- You can share public tasks with other users.
- You can use public tasks as a report template with the *Email a report* action.

To save a task:

1 Right-click the task tab, and click **Save as**.

   NOTE: The **Save as** button is only available if your report query filters are valid. You know that your query is valid when the **Generate report** button is activated.

2 In the dialog box that opens, select how you want to save the task:

   - **private task:** A private task is a saved task that is only visible to the user who created it.

     Enter a name for the saved task, or select an existing one to overwrite it.

   - **public task:** A public task is a saved task that can be shared and reused among multiple Security Center users.

     Enter a name for the saved task or select an existing one to overwrite it, and select the *partition* that the task should belong to. Only users that are members of the partition can view or modify this task.

3 (Optional) Rename the saved task.

   Example: You can save a Monitoring task that displays your parking lot cameras with the name *Parking lot - Monitoring*, or save an investigation task that searches for video bookmarks added within the last 24 hours with the name *Today's bookmarks*.

4 Click **Save**.

After you finish

- To save changes you make to the task later on, right-click the task tab, and click **Save**.
- If you change the task layout (for example, resize or hide report columns), you can revert back to the layout used when the task was saved by right-clicking the task tab, and clicking **Reload**.

Related Topics

Home page overview on page 9

Adding tasks to your Favorites list

You can add tasks and tools to your Favorites so they are listed beside the Recent items in your home page instead of the full task list.

What you should know

The tasks you add to the Favorites list are specific to your user account. The tasks that appear in the Favorites list do not appear in the Recent items list.

To add a task to your Favorites list:

1 Do one of the following:
   - On the home page, move the mouse pointer over a task, and click **Add to Favorites** (☆).
   - On the home page, drag a task from the *Recent items* list into the Favorites list.
   - Right-click the task tab, and click **Add to Favorites**.

2 To remove a task from the Favorites list, do one of the following:
   - On the home page, move the mouse pointer over a task, and click **Remove from Favorites** (★).
   - Right-click the task tab, and click **Remove from Favorites**.

Hiding the Favorites and Recent items lists from your home page

You can turn off the display of the Favorites and Recent items lists in your home page so the full task list is always displayed instead.

What you should know

When you turn off the display of the Favorites and Recent items lists in your home page, the system does not forget the items that are registered in those lists. Even when this feature is turned off, the system continues to keep track of your recently used items.

To hide the Favorites and Recent items lists from your home page:

1 From the home page, click **Options** > **Visual**.
2 Clear the option **Display recent items and favorites in home page**.
3 Click **Save**.

From now on, only the full task list will be displayed when you click **Tasks** from the home page.

Sending tasks to other users

You can send your current tasks to another user on another workstation.

What you should know

Sending tasks to another user is helpful if you have selected specific entities to monitor and you want to share the task with someone else. Or, perhaps you have configured the query filters for a certain investigation task, and you want somebody else to run the same report.

To send a task to another user:

1. Open the task you want to send.
2. Configure the task.

   Example: You can modify the tile layout, display certain cameras, configure query filters, add entities to be monitored, and so on.
3. Right-click the task tab, and then click **Send**.
4. In the **Send task** dialog box, click ⊕.
5. Select whether to send the task to a user (**User**) or a workstation (**Monitor**).
6. Select your recipient.
7. If you are sending the task to a user, write a message in the **Message** field.
8. Click **Send**.

   The recipient receives a pop up message explaining that someone has sent them a task. They are prompted to accept the task before it loads in their application.

Moving the taskbar

You can configure the *taskbar* to appear on any edge of the application window, or to set it to auto-hide so it is only shown when you hover your mouse over the taskbar location.

What you should know

When you auto-hide the taskbar, the notification tray is also hidden. These settings are saved as part of your user profile and apply to Security Desk and Config Tool.

To change the taskbar position:

1. From the home page, click **Options** > **Visual**.
2. From the **Taskbar position** drop-down list, select the edge where you want the taskbar to appear.
3. To auto-hide the taskbar, select the **Auto-hide the taskbar** option.
4. To show the current task name when *task cycling* is enabled and the taskbar is hidden, select the **Show task name in overlay** option.
5. Click **Save**.

Customizing task behaviour

Once you are familiar with how to work with tasks in Security Center, you can customize how the system handles tasks, from the *Options* dialog box.

What you should know

The task settings are saved as part of your Security Center user profile and apply to Security Desk and Config Tool.

To customize task behavior:

1. From the home page, click **Options** > **User interaction**.
2. In the **System messages** section, set the following options as desired:
   - **Ask for a name when creating a task:** Select this option if you want Security Desk to ask you for a name every time you create a task that accepts multiple instances.
   - **Ask for confirmation before closing a task:** Select this option if you want Security Desk to ask for confirmation every time you remove a task from the interface.
   - **Ask for confirmation when opening tasks sent by other users:** Select this option if you want Security Desk to ask for confirmation every time you open a task sent by another user.
3. In the **Reload task** section, specify how you want Security Desk to behave when someone updates a *public task* you currently have open:
   - *Ask user*. Ask you before loading the updated task definition.
   - *Yes*. Reload the task without asking.
   - *No*. Never reload the task.
4. Click **Save**.

3

Reports

This section includes the following topics:

Generating reports

To generate a report in any reporting task, you must set the query filters, and then run the query. After you generate the report, you can work with your results.

What you should know

Reporting tasks are where you generate customized queries on the entities, activities, and events in your Security Center system for investigation or maintenance purposes. Most investigation and maintenance tasks are reporting tasks.

The maximum number of report results you can receive in Security Center is 10,000. By default, the maximum number of results is 2000. This value can be changed from the *Options* dialog box.

If you want to generate a report with more than 10,000 results, then use the **Generate and save report** command.

NOTE: These steps only describe the general process for running a report.

To generate a report:

1. Open an existing reporting task, or create a new one.
2. In the *Filters* tab, use the query filters to create a customized search.

   NOTE: Some of the filters have a **Select all** button. This button does not appear if there are more than 100 entities to select from (for example, if you have a list of 1500 cardholders), because if you query too many entities the report takes too long to generate.
3. Set a date and time range for the report.
4. Click **Generate report**.

   If there are invalid filters, the **Generate report** button is unavailable.

   The query results are displayed in the report pane. You can sort the results by column.
5. Analyze the query results.

   The query results depend on the type of reporting task. When video sequences or LPR data are attached to the query results, you can view them in the canvas by dragging a report item to a tile.
6. Work with the query results.

   Depending on the items in the query results, you can print the report, save the report as an Excel or PDF document, export the video sequences, and so on.
7. (Optional) Save the report as a template.

   If you save the report layout (query filters and report columns) as a template, it can be sent to another user or workstation using the *Email a report* action.

Related Topics

Customizing the report pane on page 45
Customizing report behavior on page 46

Exporting generated reports

In every reporting task, you can export your report once it is generated.

What you should know

The maximum number of report results that can be exported is 10, 000.

To export a generated report:

1. At the top of the report pane, click **Export report** (💾).
2. In the dialog box, set the following options:
   - **File format:** Select the file format (CSV, Excel, or PDF).
   - **Destination file:** Select the file name.
   - **Orientation:** (PDF only) Select whether the PDF file should be in portrait or landscape mode.
   - **Attached files folder:** (CSV only) Specify where the attached files, such as cardholder pictures or license plate images, are saved.
3. Click **Export**.

Printing generated reports

In every reporting task, you can print your report once it is generated.

To print a report:

1. At the top of the report pane, click **Print report** (🖨).
2. In the Report preview window, click **Print**, and select a printer.

   You can also export the report as a Microsoft Excel, Word, or Adobe PDF document.

Customizing time zone settings

If your Security Center system includes devices operating in different time zones, you must select whether the report queries are based on a fixed time zone, or on each device’s local time zone.

What you should know

The time zone settings affect how the time range filters in your reports work. If you select a fixed time zone, the results that come from a device (such as an *access control unit* or a *video unit*) in another time zone are adjusted for time differences.

The time zone settings are saved as part of your user profile and apply to Security Desk and Config Tool.

To customize time zone settings:

1. From the home page, click **Options** > **Date and time**.
2. To add time zone abbreviations to all time stamps in Security Center, select the **Display time zone abbreviations** option.
3. Select how time fields are displayed and interpreted in Security Center:
   - To display and interpret time according to each device’s local time zone, select the **each device's time zone** option.

     This option allows each device to follow a different time zone. Select this option to display and interpret the time according to each device’s local time zone.
   - To display and interpret time according to a fixed time zone, select **the following time zone** option, and choose a time zone from the drop-down list.
4. Click **Save**.

Example

If you create a report with a time range between 9 A.M. and 10 A.M. Eastern time, and devices located in Vancouver (Pacific time) are included in the search, one of the following happens based on your time zone settings:

- Time zone based on each device’s local time zone: The report results are from events that occurred between 9 A.M. and 10 A.M. Pacific time.
- Fixed time zone (set to Eastern time): The report results are from events that occurred between 6 A.M. and 7 A.M. in the Pacific time zone, because of the three-hour time difference between Montreal and Vancouver.

Generating and saving reports

Instead of waiting for a report to generate and then exporting the results, you can generate a report and save it to a file location directly.

What you should know

Generating and saving a report is helpful, because you do not have to wait at your workstation for the report to generate. It is also helpful if your query has many results, because you are not limited to 10, 000 results like when you generate a report normally.

You can select CSV, Excel, or PDF file format. If you have many results, then only CSV format is available.

NOTE: The tasks that support this command are those where the results are queried from a role database, and not the directory.

To generate and save a report:

1 Open an existing reporting task, or create a new one.

2 In the *Filters* tab, use the query filters to create a customized search.

   NOTE: Some of the filters have a **Select all** button. This button does not appear if there are more than 100 entities to select from (for example, if you have a list of 1500 cardholders), because if you query too many entities the report takes too long to generate.

3 Right-click a column heading in the report pane, and click **Select columns** (▤).

4 Select which columns to include in the saved report, and click **Save**.

5 Click the drop-down arrow next to **Generate report**, and click **Generate and save report**.

6 In the dialog box, set the following options:

   - **File format:** Select the file format (CSV, Excel, or PDF).
   - **Destination file:** Select the file name.
   - **Orientation:** (PDF only) Select whether the PDF file should be in portrait or landscape mode.
   - **Attached files folder:** (CSV only) Specify where the attached files, such as cardholder pictures or license plate images, are saved.

7 Click **Export**.

The report is saved in the location you specified.

Customizing the report pane

Once you have generated your report, you can customize how the results are displayed in the report pane.

To customize the report pane:

1 Generate your report.

2 Choose which columns to show, as follows:

   a) In the report pane, right-click on a column heading, and then click **Select columns** (▤).

   b) Select the columns you want to show, and clear the columns you want to hide.

   c) To change the column order of appearance, use the ▲ and ▼ arrows.

   d) Click **OK**.

3 To adjust the width of a column, click between two column headings and drag the separator to the right or left.

4 To change the column order, click and hold a column heading in the report pane, and dragging it to the desired position.

5 To sort the report by one of the columns, click the column heading. Click the column heading a second time to sort the report in the reverse order.

   NOTE: All columns containing timestamps are sorted according to their UTC time value. If you choose to display the times in Security Center according to each device's local time zone rather than a fixed time zone, the times might appear out of order if the report contains devices from different time zones.

6 To increase the size the report pane, drag the separator bar between the report pane and the canvas to the bottom of the application window.

7 Save your task layout with the changes you made to the report pane as follows:

   - To save the task as a *private* or *public* task, right-click the task tab, and then click **Save as**.
   - To save the workspace for the next time you open the application, right-click in the taskbar, and then click **Save workspace**.

Related Topics

Customizing time zone settings on page 42

Customizing report behavior

You can select how many report results to receive, and when you want to receive error messages about reports, from the *Options* dialog box.

What you should know

When the query reaches the specified limit, it automatically stops with a warning message. The maximum value you can set is 10,000. The report settings are saved as part of your user profile and apply to Security Desk and Config Tool.

To customize report behavior:

1. From the home page, click **Options** > **Performance**.
2. In the **Reports** section, set the **Maximum number of results** option value.

   This option determines the maximum number of results that can be returned by a query using a reporting task. This limit helps ensure stable performance when too many results are returned if your query is too broad.
3. Click the **User interaction** tab.
4. If you want Security Center to display a warning message every time you are about to execute a query that might take a long time, select the **Display warning if query may take a long time to execute** option.
5. Click **Save**.

About the Report Manager role

Report Manager is a type of role that automates report emailing and printing based on schedules.

Only one instance of this role is permitted per system.

This role is created by default at system installation and hosted on your *main server*.

Setting maximum report results for automated reports

You can select the maximum number of results that can be generated using the *Email a report* or *Export report* actions, to prevent report that has too many results from freezing your computer.

What you should know

The maximum number of results only applies if you are saving the report in PDF or Excel format. It does not apply to CSV format.

The *Email a report* or *Export report* actions can be triggered using event-to-actions, or triggered as a one-time action or hot action from Security Desk.

To set the maximum number of report results:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the Report Manager role, and click the **Properties** tab.
3. Set a value in the **Maximum number of results for batch reports** option, and click **Apply**.

4

Keyboard shortcuts

This section includes the following topics:

Default keyboard shortcuts

This table lists the default keyboard shortcuts you can use to control task, tiles, and entities on your local workstation. This list is categorized alphabetically by command category.

NOTE: You can change the keyboard shortcuts from the *Options* dialog box.

Command	Description	Shortcut
General commands		
Apply changes	Apply the changes made to your current configuration tab.	Ctrl+S
Exit application	Close the application.	Alt+F4
Full screen	Toggle between displaying the application in full screen and windows mode.	F11
Go to next page	Switch to the next task tab.	Ctrl+Tab
Go to previous page	Switch to the previous task tab.	Ctrl+Shift+Tab
Help	Open the online help.	F1
Home page	Go to the home page.	Ctrl+Grave accent (‘)
Options	Open the Options dialog box.	Ctrl+O
Select columns	Select which columns to show/hide in the report pane.	Ctrl+Shift+C
Camera commands		
Add a bookmark	Add a bookmark to video in the selected tile (for live video only).	B
Add bookmark (all)	Add bookmarks to video in all selected tiles (for live video only).	Ctrl+Shift+B
Copy statistics of the currently selected video tile	Copy the statistics of the selected tile.	Ctrl+Shift+X
Show diagnostic timeline	Show the timeline of the video stream diagnosis.	Ctrl+Shift+T
Show video stream diagnosis	Show/hide the video stream diagnosis, where you can troubleshoot your video stream issues.	Ctrl+Shift+D
Show video stream statistics on the tile	Show/hide the statistics summary of the video in the selected tile.	Ctrl+Shift+A
Show video stream status	Show/hide the status summary of the video stream connectins and redirections in the selected tile.	Ctrl+Shift+R

Command	Description	Shortcut
PTZ commands		
Go to preset	Jump to a PTZ preset you select.	<PTZ preset>+Shift +Insert
Pan left	Pan the PTZ camera image to the left.	Left arrow
Pan right	Pan the PTZ camera image to the right.	Right arrow
Tilt down	Tilt the PTZ camera image down.	Down arrow
Tilt up	Tilt the PTZ camera image up.	Up arrow
Zoom in	Zoom in the PTZ camera image.	Hold the Plus sign (+)
Zoom out	Zoom out the PTZ camera image.	Hold the En dash (-) key
Task commands		
Rename task	Rename the selected task.	F2
Save as	Save a task under a different name and scope (private or public).	Ctrl+T
Save workspace	Save the task list so that it is automatically restored the next time you log on to the system with the same user name.	Ctrl+Shift+S
Saved tasks	Open the *public tasks* page from the home page.	Ctrl+N

Related Topics

Customizing keyboard shortcuts on page 52

Customizing keyboard shortcuts

You can assign, modify, import, or export the keyboard shortcuts mapped to frequently used commands in Security Center.

What you should know

A keyboard shortcut can only be assigned to a single command. Assigning an existing keyboard shortcut to a new command removes it from the previous one. The keyboard shortcut configuration is saved as part of your user profile and applies to Security Desk and Config Tool. If your company is using a standard set of shortcuts, you can also export the keyboard shortcut configuration to an XML file and send it to another workstation, or import one to your workstation.

To customize your keyboard shortcuts:

1 From the home page, click **Options** > **Keyboard shortcuts**.

2 (Optional) Import a keyboard shortcut configuration as follows:

   a) Click **Import**.

   b) In the dialog box that appears, select a file, and then click **Open**.

3 In the *Command* column, select the command you want to assign a keyboard shortcut to.

4 Click **Add an item** (➕) and press the desired key combination.

   If the shortcut is already assigned to another command, a pop-up message appears.

   - Click **Cancel** to choose another shortcut.
   - Click **Assign** to assign the shortcut to the selected command.

5 Click **Save**.

6 If you need to send your short configuration to another user, export the configuration as follows:

   a) From the home page, click **Options** > **Keyboard shortcuts**.

   b) Click **Export**.

   c) In the dialog box that appears, select a filename, and then click **Save**.

7 To restore the default keyboard shortcuts:

   a) From the home page, click **Options** > **Keyboard shortcuts**.

   b) Click **Restore default** > **Save**.

Related Topics

Default keyboard shortcuts on page 50

Part II

Common Security Center administration

This part includes the following chapters:

5

Entities

This section includes the following topics:

About entities

Entities are the basic building blocks of Security Center. Everything that requires configuration is represented by an entity. An entity can represent a physical device, such as a camera or a door, or an abstract concept, such as an alarm, a schedule, a user, a role, a plugin, or an add-on.

Entities created automatically in Security Center

Although most *entities* are created manually in Security Center, some entities can also be discovered or created automatically.

The entities that are *discovered* in Security Center are those that represent hardware devices, such as video units or access control units. Usually, Security Center needs a live connection to the hardware device before the entity can be created.

The following table lists the entities that are automatically created in Security Center:

Entity type	Automatic creation	Manual creation
Servers	Always.	Not supported.
Networks	Adding a new server automatically creates a new network.	Supported, but generally not required.
Access control units	Only for units that support *automatic discovery*.	Supported, but requires a live connection to the unit.
Video units	Only for units that support *automatic discovery*.	Supported, but requires a live connection to the unit.
Cameras	Always. Camera (or video encoder) entities are created when the encoding video units are added to your system.	Not supported.
Analog monitors	Always. Analog monitor (or video decoder) entities are created when the decoding video units are added to your system.	Not supported.
LPR units	• Fixed LPR units are discovered by the LPR Manager roles. • Mobile LPR units (mounted on patrol vehicles) are added when the Patroller entities are added.	Supported for fixed LPR units, but generally not required.
Patrollers	Always.	Not supported.
Intrusion detection units	Never.	Supported, but requires a live connection to the intrusion panel.
Intrusion detection areas	Created by the Intrusion Manager role when the intrusion panel is enrolled.	Supported only if the Intrusion Manager cannot read the area configurations from the unit.

Related Topics

Automatic enrollment of access control units on page 507
Discovering units on your network on page 73

Setting geographical locations of entities

To calculate the rising and setting of the sun for video units, or to plot a map for LPR units, you can set the latitude and longitude of that entity.

What you should know

The geographical location (latitude, longitude) of an entity has two different uses:

- The geographical location of video units is used to automatically calculate the time when the sun rises and sets on a given date. This is helpful if you want the system to only record video during the daytime (for cameras that are placed outside), or adjust the brightness of a camera based on the time of day.
- The geographical location of fixed *LPR units* without a GPS receiver is used to plot the LPR events (*reads* and *hits*) associated with the LPR unit on the map in Security Desk.

To set the geographical location of an entity:

1. In the **Location** tab of an entity, click **Select**.

   A map window appears.
2. Navigate to the location of your entity on the map.

   You can click and drag to zoom in, zoom out, and pan.
3. Click **Select** in the map window.

   The cursor changes to a cross.
4. Click on the desired location on the map.

   A pushpin appears on the map.
5. Click **OK**.

The latitude and longitude fields display the coordinates of the location you clicked on the map.

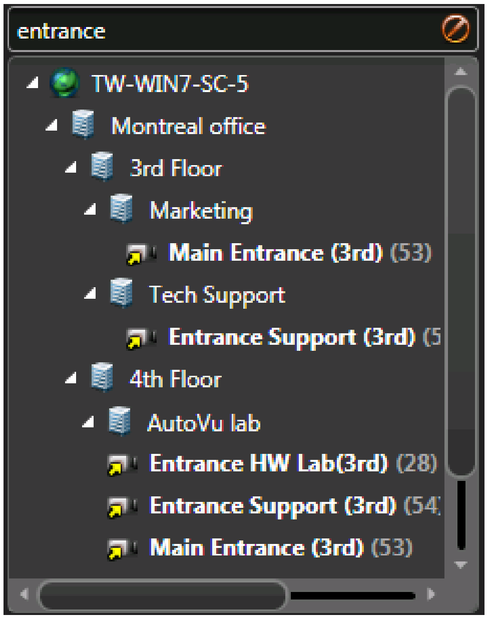
Searching for entities

If you cannot find the entity you need in a task, you can search for the entity by name.

To search for an entity:

1 In the *Search* box in the selector, type the entity name you are searching for.

2 Click **Search** (🔍).



entrance

- TW-WIN7-SC-5
  - Montreal office
    - 3rd Floor
      - Marketing
        - Main Entrance (3rd) (53)
      - Tech Support
        - Entrance Support (3rd) (5
    - 4th Floor
      - AutoVu lab
        - Entrance HW Lab(3rd) (28)
        - Entrance Support (3rd) (54
        - Main Entrance (3rd) (53)

Only entities with names containing the text you entered are displayed.

3 Click **Clear filter** (⊘) to stop using the search filter.

Related Topics

About the area view on page 18

Entity states on page 67

Searching for entities using the search tool

You can apply a set of filters to find the entities you need using the *Search* tool.

What you should know

The *Search* tool is available for many tasks. The available filters depend on the task you are using. For example, you can filter entities by name, description, entity type, partitions, and so on.

To search for an entity using the Search tool:

1 In the *Search* box in the selector, click **Apply a custom filter** (▽).

2 In the *Search* window, use the filters to specify your search criteria.

- To turn on a filter, click on the filter heading. Active filters are shown with a green LED (🟢).
- To turn off a filter (●), click on the filter heading.

NOTE: Invalid filters are shown in red. Hover your mouse cursor over the heading to see why the filter is invalid.

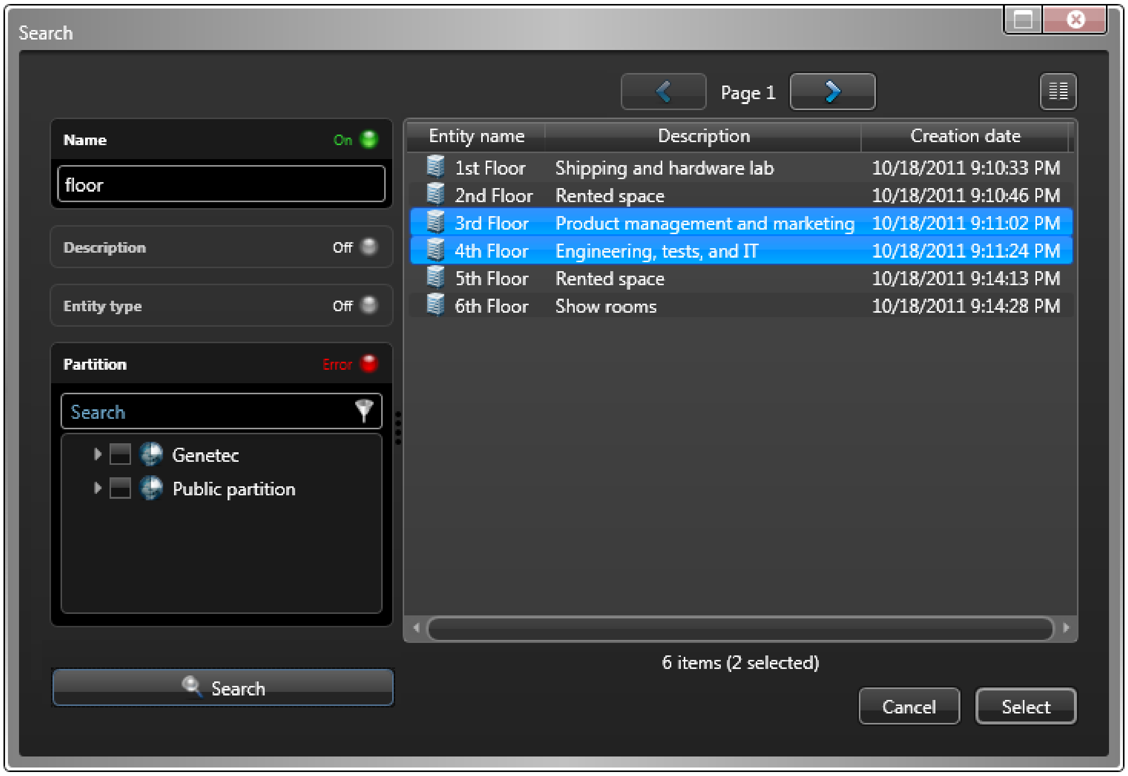
3 Click **Search** (🔍).

The search results appear on the right. The total number of results is displayed at the bottom of the list.

4 Click **Select columns** (▤) to choose which columns to display in the result list.

5 Select the entities you want.

TIP: Hold the **CTRL** key for multiple selections. Click ‹ and › to scroll through multiple pages of results.



Name: On ●
floor

Description: Off ●

Entity type: Off ●

Partition: Error ●

Search

Genetec

Public partition

Entity name	Description	Creation date
1st Floor	Shipping and hardware lab	10/18/2011 9:10:33 PM
2nd Floor	Rented space	10/18/2011 9:10:46 PM
3rd Floor	Product management and marketing	10/18/2011 9:11:02 PM
4th Floor	Engineering, tests, and IT	10/18/2011 9:11:24 PM
5th Floor	Rented space	10/18/2011 9:14:13 PM
6th Floor	Show rooms	10/18/2011 9:14:28 PM

6 items (2 selected)

6 Click **Select**.

Only the entities you selected appear in the selector.

7 Click **Clear filter** (⊘) to stop using the search filter.

Copying configuration settings from one entity to another

When you have many similar entities to configure, you can save time by copying the settings of one entity to others of the same type using the *Copy configuration tool*.

Before you begin

If you are copying camera settings, make sure the cameras are the same brand and model so the settings match.

What you should know

Only administrative users can use this tool.

(Cameras only) If you are copying the camera's network settings, only the streaming settings are copied (*Connection type* and *UDP port*). The Multicast address is not copied.

To copy the configuration settings of one entity to another entity:

1 Open the **Copy configuration tool** one of the following ways:
   - From the Config Tool home page, click **Tools** > **Copy configuration tool**.
   - From the Config Tool, right-click an entity in any entity tree, and then click **Copy** > **Copy configuration tool**.

2 If you opened the **Copy configuration tool** from the home page, then select an entity type, and click **Next**.

3 In the *Source* page, select which entity you want to copy the settings from, and click **Next**.

4 In the *Options* page, select the types of settings you want to copy, and click **Next**.
To know which options are available for each entity, see the following list.

5 In the *Destinations* page, select the entities you want to copy the settings to, and click **Next**.

6 When the copying process is completed, click **Close.**

After you finish

If you copied camera settings, test the settings that are dependent on camera location (for example, motion detection or color) on the camera you copied the configuration to. You might have to adjust the settings, depending on whether the camera is inside or outside, in a busy or quiet location, and so on .

Related Topics

Testing motion detection settings on page 413
Adjusting camera color settings on page 415
Replacing fixed Sharp units on page 674

Settings copied for each entity using the Copy Configuration tool

You can determine which categories of settings are copied when using the Copy Configuration tool. The available categories are different for each entity.

The following table lists the categories of settings that are available for each entity when using the Copy Configuration tool:

Entity type	Setting categories available
Access Control unit	• Actions • Properties (HID units only) • Synchronization • Time Zone
Access rule	• Attached entities • Members • Properties
Alarm	• Actions • Attached entities • Properties • Recipients
Camera	• Actions • Boost quality • Color • Encryption • Hardware specific settings • Motion detection • Network • PTZ • Recording • Stream Usage • Video quality
Cardholder	• Access rules • Actions • Options • Parent cardholder groups • State
Cardholder group	• Access rules • Members • Parent cardholder groups • Properties

Entity type	Setting categories available
Credential	• Actions • Badge template • State
Door	• Access rules • Actions • Cameras • Properties • Unlock schedules
Hotlist	• Advanced • Attributes • Path • Properties
LPR Unit	• Hotlists
Patroller	• Actions • Custom fields • Hotlists • Permits • Properties
Permit	• Advanced • Attributes • Parking lots • Path • Properties
User	• Access rights • Actions • Advanced • Alarms • Privileges • Properties • Security Desk settings

Entity type	Setting categories available
User group	• Access rights • Advanced • Alarms • Privileges • Properties
Video unit	• Actions • Audio • Hardware specific settings • Motion detection • Network • Security • Time Zone
Zone	• Actions

Assigning logical IDs to entities

You can assign a logical ID (unique number) to entities, public tasks, and workstations in your system so that you can control them using keyboard shortcuts.

What you should know

If you want to use keyboard shortcuts to switch to different public tasks, control other workstations, or display entities in the Security Desk canvas, you must assign unique numbers (logical IDs) to entities. The logical IDs can then be used in a keyboard shortcut. For more information about using keyboard shortcuts in Security Desk, see the *Security Desk User Guide*.

There are a few entities that are often used together in a keyboard shortcut. These entities are grouped, and cannot have the same logical ID. For example, *cameras* and *public tasks* are in the same group, because they are often used together in a keyboard shortcut to open a saved task and display a camera.

TIP: You can also change the logical ID from the *Identity* tab of each entity’s configuration page.

To assign a logical ID to an entity:

1 Open the **System** task, click **General settings** view, and click the **Logical ID** page.

2 From the **Show logical ID for** drop-down list, select the group that lists the entity, public task, or workstation you want to use.

   If the item you want is not listed in one of the groups, select **All types**.

3 Next to the item you want to assign the logical ID to, type a number in the **ID** column.

4 Click **Apply**.

   If the logical ID is already assigned, you receive an error message. Select a different ID and try again.

Modifying logical IDs

If there are duplicate logical IDs, or you want to change an ID to a number that is easier to remember when using your keyboard shortcuts, you can modify the logical ID of an entity.

To modify a logical ID:

1 Open the **System** task, click **General settings** view, and click the **Logical ID** page.

2 From the **Show logical ID for** drop-down list, select the group to configure.

3 If you have a large system, select the **Hide unassigned logical IDs** option to only show entities, public tasks, and workstations that have a logical ID.

4 If there are still multiple pages, use the ‹ and › buttons to scroll through the pages.

5 Next to the entity, public task, or workstation you want to modify, type a new logical ID in the **ID** column.

6 Click **Apply**.

Customizing how entities are displayed in the canvas

You can show the logical ID (unique ID number) of entities in the area view to help you identify them. You can also display the name of the *Active Directory* the entity is imported from.

What you should know

These settings are saved as part of your user profile and are applied to Security Desk and Config Tool.

To customize how entities are displayed:

1. From the home page, click **Options** > **User interaction**.
2. To display the logical ID in brackets after the entity name, select the **Show logical ID** option.
3. To display the username and domain name of the Active Directory, select the **Show Active Directory domain name where it is applicable** option.
4. Click **Save**.

Deleting entities

You can delete entities that you have manually created, and those that were discovered automatically by the system.

Before you begin

If the entity was automatically discovered, it must be offline or inactive (shown in red) before you can delete it.

What you should know

If you delete a parent entity that has entities underneath it in the entity tree, those entities are also deleted.

To delete an entity:

1 In the entity view of any task, select the entity.

2 At the bottom of the window, click **Delete** (✕).

3 In the confirmation dialog box that appears, do one of the following:

- If there is only one copy of the entity in the entity tree, click **Delete**.
- If more than one copy of the entity exists, choose to delete them all, or just the selected copy.

Entity states

Entities can appear in several different states in the area view, which are represented by different colors.

The following table lists the three entity states:

State	Color	Description
Online	White	The server can connect to the entity.
Offline	Red	The server cannot connect to the entity.
Warning	Yellow	The server can connect to the entity, but there are problems.

Entity warnings usually appear because of invalid configurations. For example, when it comes to cameras the following two conditions can cause the camera to fall into a yellow warning state:

- Multiple, conflicting recording schedules have been applied to the same camera.
- A *Transmission lost* event has occurred. This means that the Archiver is still connected to the camera, but it has not received any video packets for more than 5 seconds.

To troubleshoot offline and warning states of cameras, you do one of the following:

- Change the conflicting schedules.
- Troubleshoot the Archiver role.

Related Topics

Searching for entities on page 58
Troubleshooting: entities on page 68
About schedules on page 167

Troubleshooting: entities

You can troubleshoot entities and roles using the *diagnostic* tool.

What you should know

An entity or role that is not properly configured is displayed in yellow. An entity that is offline is displayed in red. The *diagnostic* tool can help you troubleshoot the problem with the entity.

To troubleshoot an entity:

1 Open the **System status** task.

2 From the **Monitor** drop-down list, select the entity type you want to diagnose.

3 If required, select an area in the *Selector*.

4 To include entities within nested areas, select the **Search member entities** option.

The related entities are listed in the report pane.

5 Select a trouble entity, and click **Diagnose** (✚).

A troubleshooting window opens, showing the results from the diagnostic test performed on the selected entity.

6 To save the results of the test, click **Save**.

7 Click **Close**.

Related Topics

Entity states on page 67

About custom fields

A custom field is a user defined property that is associated to an entity type and is used to store additional information that is useful to your particular organization.

Custom fields can include any information that you define. They can use data types that are available by default in Security Center, or you can create your own data types. Once custom fields are added, they are available in all database reports and queries related to the entity they are defined for. If custom a field contains private information, you can restrict certain groups of users from seeing that field.

For example, you can add *Gender*, *Home number*, and *Cellphone number* as custom fields for cardholder entities, and only allow the *Human Resource* user group to access that information.

Limitations of custom fields

Custom fields are always local to the system where they are defined.

- In a *Federation* scenario, custom fields are not imported from the federated system. However, you can associate custom fields as local attributes to *federated entities*.
- In an *Active Directory (AD)* integration scenario, custom fields can be mapped to AD attributes to display their values in your local system, but not to update the AD.

Standard data types

Security Center includes the following default data types for custom fields:

- **Text:** Alphanumeric text.
- **Numeric:** Integers in the range -2147483648 to 2147483647.
- **Decimal:** Real numbers from -1E28 to 1E28.
- **Date:** Gregorian calendar date and time.
- **Boolean:** Boolean data, represented by a check box.
- **Image:** Image file. The supported formats are: .bmp, .jpg, .gif, and .png.
- **Entity:** Security Center entity.

Related Topics
About federated entities on page 190
Mapping custom fields to synchronize with Active Directory on page 326

Creating custom data types for custom fields

To use something other than the standard data types when creating custom fields, you can create your own custom data types.

What you should know

Custom data types define a list of values based on a standard data type. Custom data types appear in a drop-down list in the *Custom fields* tab of the entity's configuration page.

To create a custom data type for a custom field:

1. Open the **System** task, and click the **General settings** view.
2. Click the **Custom fields** page, and click the **Custom data types** tab.
3. Click ➕ at the bottom of the custom data type list.
4. In the **Edit custom data type** page, enter the **Name**, **Description**, and **Type** for your custom data type, and click **Next**.
5. In the **Data entry** page, enter a value in the **Value** field and click ➕.

   The entered value is added to the enumerated list.
6. Define other possible values for this data type.
7. When you are finished, click **Next**, **Next**, and **Close**.

Modifying custom data types

You can modify custom data types (rename, add or delete values, and so on) before or after the custom data type is being used in a custom field.

What you should know

The following limitations apply when modifying custom data types:

- You cannot delete a value if it is being used as the default value for a custom field.
- You cannot change the standard data type on which the custom data type is based.

To modify a custom data type:

1. Open the **System** task, and click the **General settings** view.
2. Click the **Custom fields** page, and click the **Custom data types** tab.
3. Select the data type, click **Edit the item** (✏), and follow the wizard.

Creating custom fields

To add more information to the properties of entities in your system, you can create custom fields.

Before you begin

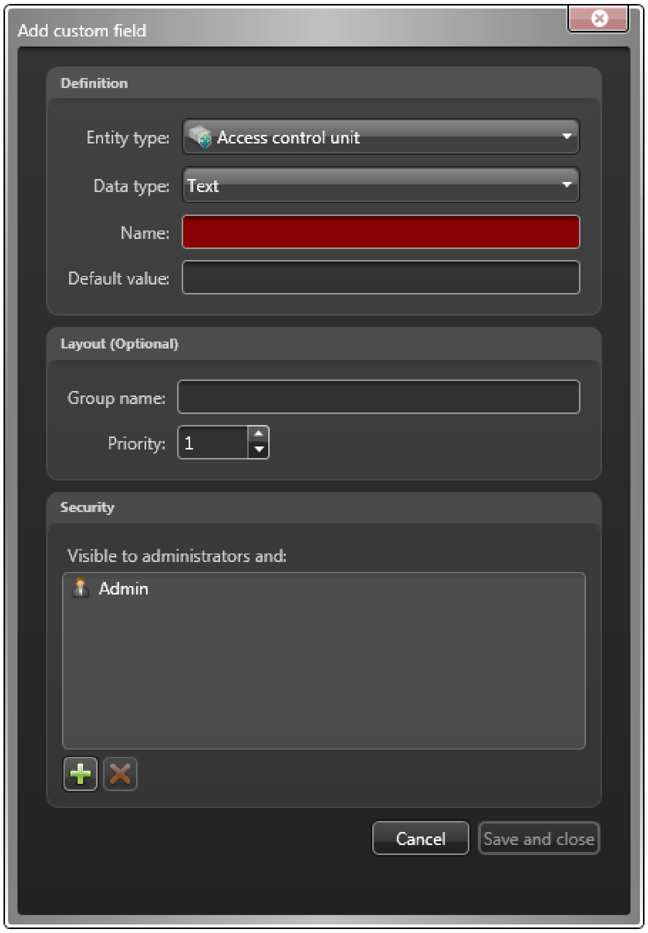
If you want to create a custom field using your own custom data type, the data type must already be created.

To create a custom field:

1 Open the **System** task, and click the **General settings** view.

2 Click the **Custom fields** page, and click ➕ at the bottom of the custom field list.

3 From the **Entity type** drop-down list in the **Add custom field** dialog box, select the entity type this custom field applies to.



Add custom field

Definition

Entity type: Access control unit

Data type: Text

Name:

Default value:

Layout (Optional)

Group name:

Priority: 1

Security

Visible to administrators and:

Admin

4 From the **Data type** drop-down list, select a standard or custom data type for the custom field.

5 In the **Name** field, type the name for the custom field.

6 (Optional) In **Default value** field, type or select the default value for this field.

This value is displayed by default when an entity that uses this custom field is created.

7 Depending on the selected data type, the following additional options appear:

- **Mandatory:** Select it if the custom field cannot be empty.
- **Value must be unique:** Select it if the value of the custom field must be unique.

> **NOTE:** The *unique value* option can only be enforced after the field is created. To enforce this option, you must first make sure that all entities in your system have a distinct value for this custom field, then come back to this tab to apply the unique value option to it. Selecting this option automatically selects the **Mandatory** option.

8. Under the **Layout** section, type the **Group name,** and select the **Priority** from the drop-down list.

   These two attributes are used when displaying the field in the **Custom fields** tab of associated entity. The group name is used as the group heading, and the priority dictates the display order of the field within the group.

9. Under the **Security** section, click + to add users and user groups that will be able to see this custom field.

   By default, only administrators can see a custom field.

10. Click **Save and close**.

The new custom field is now available in the **Custom fields** tab of the selected entity type, and can be used to search for those entity types in the *Search* tool.

Related Topics
About custom fields on page 69

About the unit enrollment tool

The *Unit enrollment tool* allows you to discover IP units (video and access control) connected to your network, based on their manufacturer, and network properties (discovery port, IP address range, password, and so on). Once discovered, the units can be added to your system.

- The *Unit enrollment* tool opens automatically after the *Security Center installer assistant* unless you cleared the **Open the unit enrollment tool after the wizard** option.
- When adding access control units, only HID and Synergis™ units can be enrolled with unit enrollment tool. For complete details on how to enroll Synergis™ units, see the *Synergis™ Appliance Configuration Guide*.

Configuring unit enrollment settings

You can use the **Settings and manufacturers** button in the *Unit enrollment* tool to specify which manufacturers to include when searching for new units. You can also configure the discovery settings for units, and specify username and passwords for units so they can be enrolled easily.

To configure your discovery settings:

1 From the home page, click **Tools** > **Unit enrollment**.

2 In the upper right corner of the *Unit enrollment* dialog box, click **Settings and Manufacturers** (⚙).

3 Configure the following options:

- **Always run extensive search**. Turn this on if you want all units on the system to be discovered.

  NOTE: Units from other manufacturers may also be discovered because UPnP and *Zero config* are also used in the discovery process.

- **Refuse basic authentication** (video units only). Use this switch to enable or disable basic authentication. This is useful if you turned off basic authentication in the Security Center InstallShield, but you need to turn it back on to perform a firmware upgrade, or enroll a camera that only supports basic authentication. To turn basic authentication back on, you must switch the **Refuse basic authentication** option to **Off**.

  NOTE: This option is only available to users with Administrator privileges.

4 Click **Add manufacturer** (➕) to add a manufacturer to the list of units that will be discovered.

To delete a manufacturer from the list, select it and click ✖.

5 Configure the individual settings for any manufacturers you added. To do this, select the manufacturer and click ✎.

IMPORTANT: You must enter the correct username and password for the unit to enroll properly.

6 (Optional) Remove units from the list of ignored units (see Removing units from list of ignored units on page 75).

7 Click **Save**.

Discovering units on your network

If you do not know the IP address of the video or access control unit you want to add, you can find the unit on your network using the *Unit enrollment tool*.

Before you begin

If you want to discover an access control unit, read Adding access control unit manufacturer extensions on page 497.

To discover units:

1 From the home page, click **Tools** > **Unit enrollment**.
2 Configure your unit enrollment settings.
3 Click **Save** > **Start discovery** (🔭).

The units discovered on your network are listed, using the enrollment settings you configured for each manufacturer. You can stop the discovery process at any time.

Adding units

Once new units have been discovered, you can use the *Unit enrollment tool* to add them to your system.

To add a unit:

1 From the home page, click **Tools** > **Unit enrollment**.
2 There are three ways to add newly discovered units:

- Add all the new discovered units at the same time by clicking the **Add all** (➕) button at the lower right side of the dialog box.
- Click on a single unit in the list, then click **Add** in the **Status** column
- Right-click a single unit from the list and click **Add or Add Unit**.

When a video unit does not have the correct username and password, the **Status** for the unit will be listed as **Bad logon** and you will be prompted to enter the correct information when you add the unit. If you want to use the same username and password for all the cameras on your system, select the **Save as default authentication for all manufacturers** option.

You can also add a unit manually, by clicking the **Manual add** button at the bottom of the **Unit enrollment** tool dialog box.

NOTE:

- For video units, if the added camera is an encoder with multiple streams available, each stream is added with the *Camera - n* string appended to the camera name, *n* representing the stream number. For an IP camera with only one stream available, the camera name is not modified.
- If you are enrolling a Sharp camera running SharpOS 11.3 or earlier under the Archiver (to access the camera’s video streams, or if LPR Processing Unit input/output control is required), you must configure the AutoVu™ extension to allow basic authentication. In Config Tool, from the Archiver's *Extensions* tab, select the Genetec™ AutoVu™ extension, and turn off **Refuse Basic Authentication**.

Related Topics

Adding video units manually on page 375
Adding access control units on page 504

Clearing added units

You can clear units that have already been added to your system so they are not displayed every time you use the *Unit enrollment tool* to discover units on your system.

What you should know

The **Clear completed** option in the *Unit enrollment tool* is permanent, it cannot be reversed.

To clear added units:

1 Add the desired discovered units to your system, see Adding units on page 74.
2 Once the units have been added, click **Clear completed**.

Any unit that has **Added** displayed in the **Status** column will be cleared from the list of discovered units.

Ignoring units

You can choose to ignore units so they don't appear in the list of discovered units of the *Unit enrollment tool*.

To ignore a unit:

1 From the home page, click **Tools** > **Unit enrollment**.

The *Unit enrollment* tool opens with the list of units that have been discovered on the system.

2 Right-click the unit you want to ignore, and select **Ignore**.

The unit is removed from the list and will be ignored when the *Unit enrollment* tool discovers new units. For information about removing a unit from the list of ignored units, see Removing units from list of ignored units on page 75.

Removing units from list of ignored units

You can remove a unit from the list of ignored units so it's not ignored when a discovery is performed by the *Unit enrollment tool*.

What you should know

To remove a unit from the list of ignored units:

1 From the home page, click **Tools** > **Unit enrollment**.

2 In the upper right corner of the *Unit enrollment* dialog box, click **Settings and Manufacturers** (⚙).

3 Click **Ignored units** and click **Remove all ignored units**, or you can select a single unit and click the **Remove ignored unit** button (✖).

Viewing properties of units

At a glance, you can view a list of all the local units that are part of your system, and can see their information, such as unit type, manufacturer, model, IP address, and so on, using the *Hardware inventory* report.

What you should know

As an example, you can use the *Hardware inventory* report to see what firmware version a unit has, and determine if it needs to be upgraded.

The *Hardware inventory* report does not include information for federated units.

To view the properties of units in your system:

1. From the home page, open the **Hardware inventory** task.
2. Set up the query filter for your report. Choose one or more of the following filters:
   - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
   - **Source group:** Source entity group of the event. Usually a role or a unit.
   - **Units:** Select the access control, video, intrusion detection, and LPR units to investigate.
3. Click **Generate report**.

   The unit properties are listed in the report pane.

Report pane columns for the Hardware inventory task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Unit:** Access control, video, intrusion detection, or LPR unit involved.
- **Unit type:** Type or model of unit involved.
- **Manufacturer:** Manufacturer of the unit.
- **Product type:** Model of the unit involved.
- **Role:** Role type that manages the selected entity.
- **Firmware version:** Firmware version installed on the unit that generated the event.
- **IP address:** IP address of the unit or computer that generated the event.
- **Physical address:** The MAC address of the equipment's network interface.
- **Time zone:** Time zone of the unit.
- **User:** The user name used to connect to the unit.
- **Password:** Strength of the password on the unit. When you hover over the password strength value, a tooltip indicates if the manufacturer default password is being used.
- **Authentication scheme:** Indicates the type of authentication being used by the camera unit, such as basic, digest, anonymous, or third party. If the unit suddenly requests to connect using a less secure authentication scheme, the Archiver rejects communication and the camera goes offline. For example, the Archiver expects the camera to be using digest authentication, but the camera tries to connect using basic authentication. The connection is rejected and the camera goes offline.

- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.

Customizing Security Center behavior when renaming hardware units

You can configure how Config Tool behaves when a you rename a hardware unit, such as an *access control unit* or a *video unit*.

What you should know

This settings is saved as part of your user profile.

To customize the options when renaming hardware units:

1. From the home page, click **Options** > **User interaction**.
2. In the **Administration tasks** section, select how Config Tool behaves when you rename a unit from the **Rename all the devices inside the unit** drop-down list:
   - **Ask user:** Ask you before renaming all the devices related to the unit.
   - **Yes:** Rename all related devices without asking you.
   - **No:** Never rename the related devices.
3. Click **Save**.

6

Servers and roles

This section includes the following topics:

About servers

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

Server entities are automatically created when the Security Center Server software is installed on a computer, and that computer is connected to the *main server* of your system.

Main server

The main server is the computer that hosts the *Directory* role. All other servers (expansion servers) on the system must connect to the main server in order to be part of the same system.

You can have only one main server on a Security Center system.

Expansion servers

An expansion server is a computer that you add to your system to increase its overall computing power. An expansion server must connect to the main server, and can host any role in Security Center, except the Directory role.

You can increase the computing poster of your system at any time by adding more expansion servers to your pool of resources.

Genetec Server service

The Genetec Server service is a Windows service that is automatically installed when you install Security Center Server on a computer.

Security Center Server and the *Genetec Server* service must be installed on every computer that you want to include in the pool of servers available for Security Center. After the *Genetec Server* service is installed, you can change its password and other settings using the *Server Admin* web application.

Related Topics
Adding expansion servers on page 91

Opening Server Admin using a web browser

Using a web browser, you can open Server Admin on any server in your system and then change the settings of any server in your system.

Before you begin

To log on to a server in your system using Server Admin, you must know the server's DNS name or IP address, the web server port, and the server password. The server password is specified during Security Center Server installation, and is the same or all servers in your system.

What you should know

Regardless of which expansion server you try to connect to, Server Admin always redirects you to the main server, if the following conditions are met:

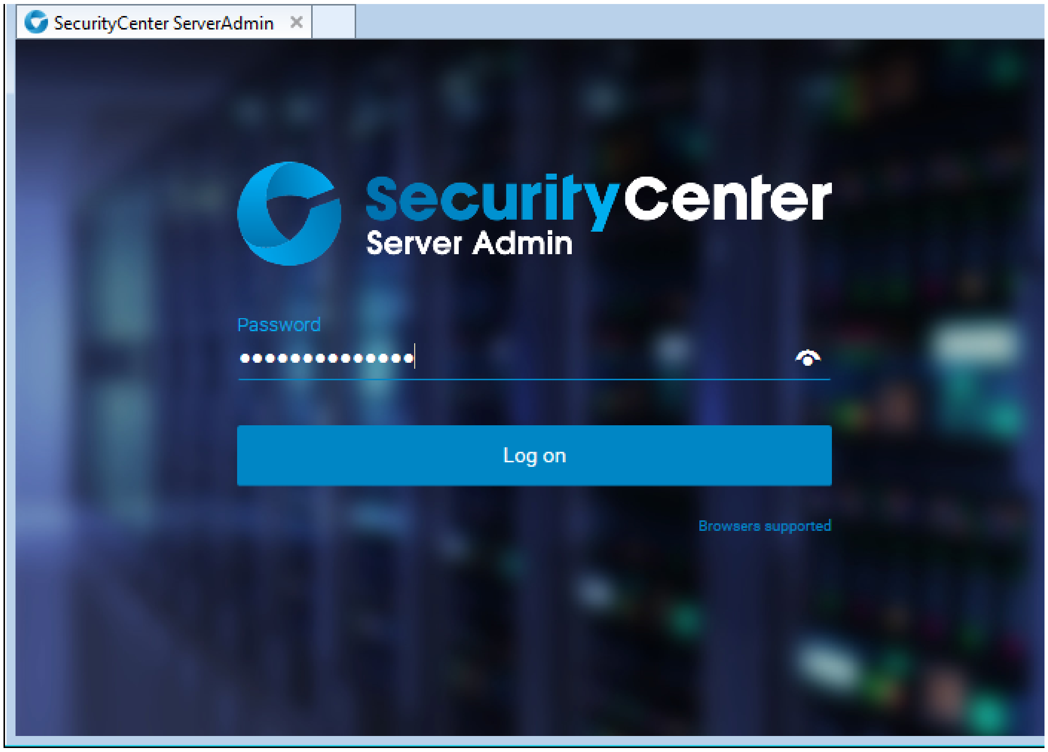
- The expansion server is currently connected to the main server.
- The expansion server and the main server are running the same version (X.Y) of Security Center.

To open Server Admin using a web browser:

1. Do one of the following:
   - In the address bar of your web browser, type `http://computer:port/Genetec`, where `computer` is the DNS name or the IP address of your server, and `port` is the web server port specified during the Security Center Server installation.

     You can omit the web server port if you are using the default value (80).
   - If connecting to Server Admin from the local host, double-click **Genetec Server Admin** (⚙) in the *Genetec Security Center* folder in the Windows Start menu.

   NOTE: If you are connecting to a remote server, Server Admin always uses a secure connection (HTTPS). If your server is using a self-signed certificate, the browser warns you that your connection is unsafe. If you get the warning message, ignore it and proceed with the unsafe connection.
2. Enter the server password that you set during the server installation, and click **Log on**.

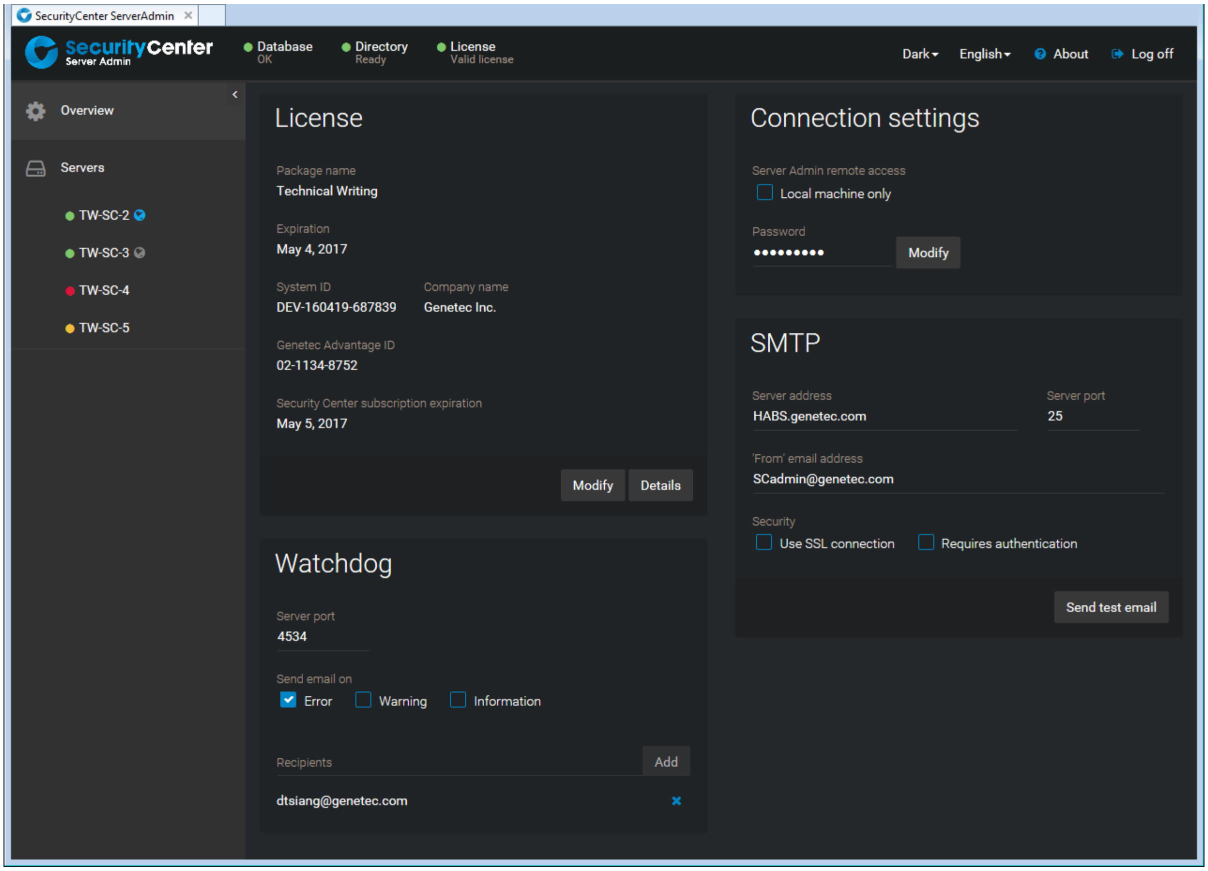


The Server Admin *Overview* page appears.

Related Topics
Server Admin - Overview page on page 83
What is Transport Layer Security protocol? on page 307

Server Admin - Overview page

The Server Admin - *Overview* page shows your Security Center license information, and the common settings (Watchdog, Connection, SMTP) that apply to all servers in your system.



Database OK

Directory Ready

License Valid license

License

Package name: Technical Writing

Expiration: May 4, 2017

System ID: DEV-160419-687839

Company name: Genetec Inc.

Genetec Advantage ID: 02-1134-8752

Security Center subscription expiration: May 5, 2017

Watchdog

Server port: 4534

Send email on: ☑ Error □ Warning □ Information

Recipients: dtsiang@genetec.com

Connection settings

Server Admin remote access: □ Local machine only

Password: •••••••••

SMTP

Server address: HABS.genetec.com

Server port: 25

'From' email address: SCadmin@genetec.com

Security: □ Use SSL connection □ Requires authentication

Dashboard (top left)

The dashboard indicates the status (🟢=ready, 🟠=getting ready, 🔴=not ready) of your system at all times, for the following components:

- **Database:** Directory database. Click to go to the Directory database configuration section.
- **Directory:** Directory role. Click to start, stop, or restart the Directory role.
- **License:** Security Center license. Click to activate the license or display the license details.

Servers (left pane)

List of all servers found on your system (only if you are connected to the main server). Click a server from the list to display its configuration page.

The status and function of each server is indicated as follows:

- 🌐: Primary Directory server (main server).
- 🌐: Secondary Directory server.
- **No icon:** Expansion server.
- 🟢: The server is up.

- 🔴: The server is down.
- 🟠: The server has problems.

License

Security Center license status and information.

- **Package name:** Software package name.
- **Expiration:** Date when your license expires.
- **System ID:** Your System ID number.
- **Company name:** Name of your company.
- **Genetec Advantage ID:** ID of your Genetec™ Lifecycle Management (GLM) contract. If you did not purchase a GLM contract, this field will not be set.
- **Security Center subscription expiration:** Expiry date of your Genetec™ Lifecycle Management (GLM) contract.
- **Modify:** Click to activate or modify your Security Center license.
- **Details:** Click to view the details of your Security Center license.

Watchdog

Use this section to configure the *Genetec™ Watchdog* service. The role of the Watchdog is to ensure that the Genetec Server service is always running.

- **Server port:** Communication port between the Watchdog and the server.
- **Send email on:** Send email notifications from the Watchdog to a list of recipients for *Error*, *Warning*, and *Information* events.
- **Recipients:** Security Center users who receive the Watchdog emails.

Connection settings

Use this section to configure the connection settings to Server Admin.

- **Local machine only:** Enable this option to restrict the Server Admin connections to the local machine.
- **Password:** Log on password for Server Admin.

SMTP

Use this section to configure the SMTP server responsible for handling email messages in Security Center.

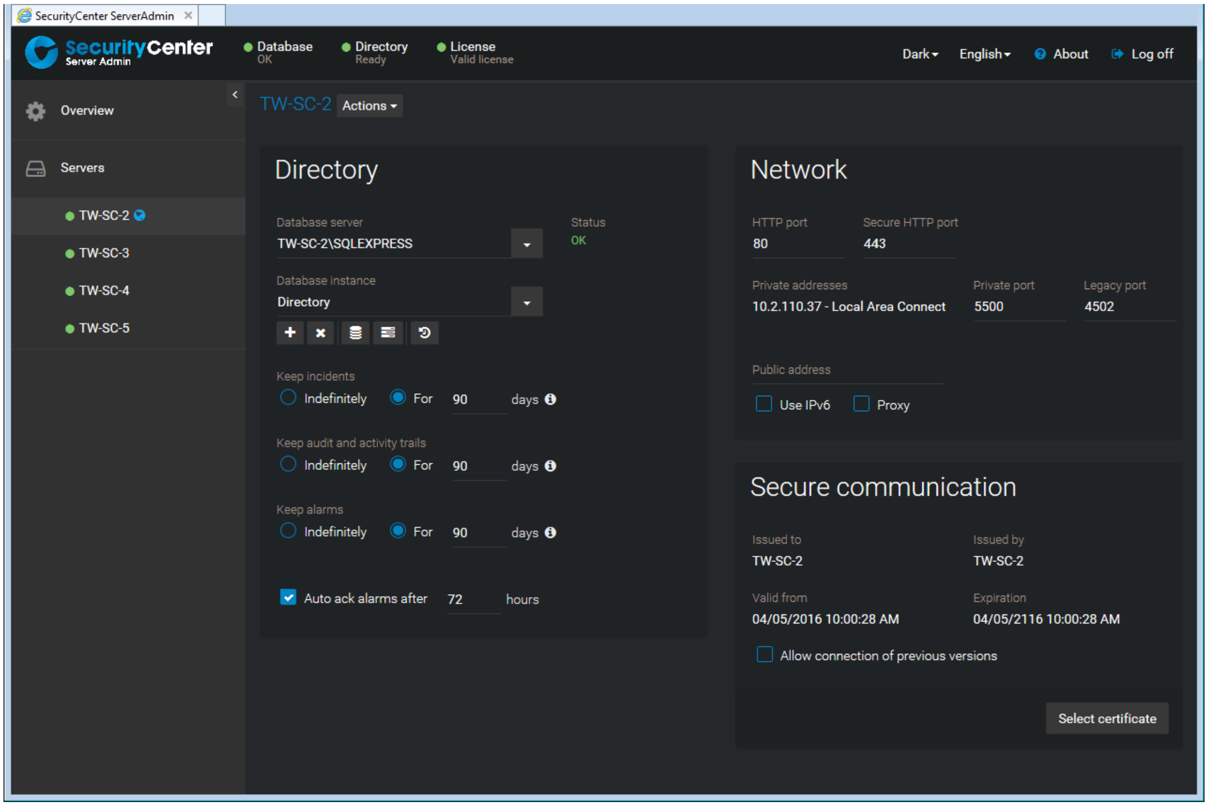
- **Server address:** DNS name or IP address of your SMTP mail server.
- **Server port:** The server port is usually 25, though your mail server might use a different port.
- **“From” email address:** Email address shown as the sender of the email.
- **Use SSL connection:** Enable secure communication with the mail server.
- **Requires authentication:** Enable this option if your mail server requires authentication. If so, you need to enter a username and password.
- **Send test email:** Send a test email to validate your SMTP configuration.

Related Topics
Server Admin - Main server page on page 86
Server Admin - Expansion server page on page 89

Activating Security Center license using the web on page 97
Activating Security Center license without Internet access on page 100
Server - Properties tab on page 841

Server Admin - Main server page

The Server Admin - *Main server* page lets you configure your Directory database and the settings pertaining to your main server.



Directory

Database server: TW-SC-2\SQLEXPRESS
Status: OK
Database instance: Directory

Keep incidents: ○ Indefinitely ● For 90 days
Keep audit and activity trails: ○ Indefinitely ● For 90 days
Keep alarms: ○ Indefinitely ● For 90 days
☑ Auto ack alarms after 72 hours

Network

HTTP port: 80
Secure HTTP port: 443
Private addresses: 10.2.110.37 - Local Area Connect
Private port: 5500
Legacy port: 4502
Public address:
□ Use IPv6 □ Proxy

Secure communication

Issued to: TW-SC-2
Issued by: TW-SC-2
Valid from: 04/05/2016 10:00:28 AM
Expiration: 04/05/2116 10:00:28 AM
□ Allow connection of previous versions

Actions

Click the **Actions** drop-down list beside the server name to see what actions can be applied to the main server.

The available actions are:

- **Directory:**
  - **Start/Stop:** Start or stop the Directory.
  - **Restart:** Restart the Directory.
  - **Deactivate:** Convert the main server to an expansion server.
- **Genetec Server:**
  - **Console:** Open the *Debug Console* page (reserved for Genetec™ Technical Support Engineers).
  - **Restart:** Restart the Genetec Server service. This action renders the server temporarily unavailable.

Directory

The *Directory* section shows the status and settings of the Directory database. The Directory database contains all system and entity configurations, the incident reports, and the alarm history.

NOTE: If you accessed Server Admin from Config Tool instead of through a web browser, you do not see the database commands (upgrading or restoring the database) because you are still connected to the Directory. You cannot modify the Directory database while you are still connected to it.

- **Database server:** Server where the SQL Server is hosted.
- **Database instance:** Name of the database instance (default=Directory).
- **Actions:** Actions related to the maintenance of the Directory database.
  - **Create database (+):** Create a new database.
  - **Delete database (✖):** Delete the database.
  - **Database properties (🛢):** Opens a dialog box showing the database information, and the automatic backup and Email notification settings.
  - **Show progress (☰):** Opens a dialog box showing the past and current actions being performed on the database.
  - **Update database (🔄):** Upgrade the database schema to the current version.
  - **Resolve conflicts (⚠):** Resolve conflicts for imported entities.
  - **Backup/restore (↺):** Back up or restore the database.
- **Keep incidents:** Specify how long the incident reports are kept in the Directory database.
- **Keep audit and activity trails:** Specify how long the entity configuration history and the activity history are kept in the Directory database.
- **Keep alarms:** Specify how long the alarm history is kept in the Directory database.
- **Auto ack alarms after:** Turn this option on to let the system automatically acknowledge all active alarms that do not get acknowledged before the specified time (in hours). When turned on, this option supersedes the **Automatic acknowledgment** option configured for each individual alarm. When the automatic acknowledgment of alarms is turned on at both the system and individual alarm level, it is the shortest delay that applies.

Network

Use this section to configure the network card and the TPC listening port used by the Genetec Server service.

- **HTTP port:** Port used by the Genetec Server service to listen to commands received from other Security Center servers on the public address.
- **Secure HTTP port:** Port used by Genetec Server service for secured HTTP connections.
- **Private address:** List of private addresses corresponding to the network interface cards (NIC) installed on this server. Only select the ones that are used for the communication between Security Center applications.
- **Private port:** Port used by the main server to listen to incoming connection requests, and by all servers for communication between themselves, on the private IP address. (default=5500).

  NOTE: If you change this port on the main server, then all users must specify the new port number after the **Directory** name in the *Logon* dialog box, separated by a colon (:). This applies to all expansion servers. You must specify the new port number after the **Security Center Directory** name in Server Admin, in the *Main server connection* section.
- **Legacy port:** Port used by the Genetec Server service to listen to commands received from servers running an older version of Security Center (default=4502).
- **Public address:** Public address of the server.
  - **Use IPv6:** Use *IPv6* for video streaming and communication between servers (only if your network supports it).

- **Proxy:** Select this option if the server is used as the proxy server for a private network protected by a firewall.

Secure communication

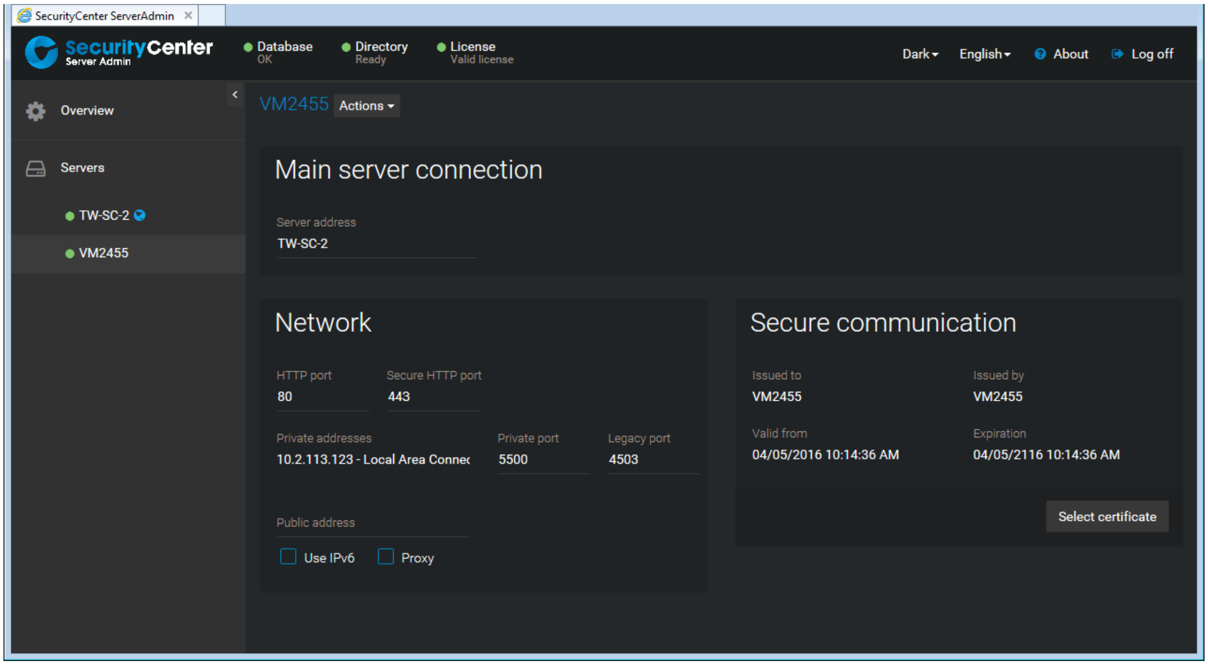
Use this section to view the current *identity certificate* used by the server to communicate with other Security Center servers.

- **Issued to:** Subject of the current certificate. A *self-signed certificate* created at software installation appears in the form *GenetecServer-{MachineName}*.
- **Issued by:** Name of the *certificate authority* that issued the certificate. The issuer and the subject are the same for self-signed certificates.
- **Valid from/to:** Validity period of the current certificate.
- **Select certificate (button):** Dialog box listing all certificates installed on this machine. You can use this dialog box to change the certificate used for this server.
- **Allow connection of previous versions:** To increase system security, turn this option off (default=on). Turning this option off prevents older Security Center clients and servers (5.3 and earlier) from connecting to the main server. For more information, see Disabling backward compatibility on page 312.

Related Topics
Server Admin - Overview page on page 83
Server - Properties tab on page 841

Server Admin - Expansion server page

The Server Admin - *Expansion server* page shows all settings pertaining to the selected expansion server.



Main server connection

Server address: TW-SC-2

Network

HTTP port	Secure HTTP port
80	443

Private addresses	Private port	Legacy port
10.2.113.123 - Local Area Connec	5500	4503

Public address

☐ Use IPv6 ☐ Proxy

Secure communication

Issued to	Issued by
VM2455	VM2455

Valid from	Expiration
04/05/2016 10:14:36 AM	04/05/2116 10:14:36 AM

Actions

Click the **Actions** drop-down list beside the server name to see what actions can be applied to the expansion server.

The available actions are:

- **Directory:**
  - **Activate:** Convert the expansion server to a main server.
- **Genetec Server:**
  - **Console:** Open the *Debug Console* page (reserved for Genetec™ Technical Support Engineers).
  - **Restart:** Restart the Genetec Server service. This action renders the server temporarily unavailable.

Main server connection

This section identifies the main server that the expansion server must connect to.

- **Server address:** The DNS name or the IP address of the main server.
- **Change password:** Only appears when no connection has been established between the expansion server and the main server. Click to set the password. Once the first contact is made, the expansion server sends its *identity certificate* to the main server, and the password is not needed again.

Network

Use this section to configure the network card and the TPC listening port used by the Genetec Server service.

- **HTTP port:** Port used by the Genetec Server service to listen to commands received from other Security Center servers on the public address.

- **Secure HTTP port:** Port used by Genetec Server service for secured HTTP connections.
- **Private address:** List of private addresses corresponding to the network interface cards (NIC) installed on this server. Only select the ones that are used for the communication between Security Center applications.
- **Private port:** Port used by the main server to listen to incoming connection requests, and by all servers for communication between themselves, on the private IP address. (default=5500).

  NOTE: If you change this port on the main server, then all users must specify the new port number after the **Directory** name in the *Logon* dialog box, separated by a colon (:). This applies to all expansion servers. You must specify the new port number after the **Security Center Directory** name in Server Admin, in the *Main server connection* section.
- **Legacy port:** Port used by the Genetec Server service to listen to commands received from servers running an older version of Security Center (default=4502).
- **Public address:** Public address of the server.
  - **Use IPv6:** Use *IPv6* for video streaming and communication between servers (only if your network supports it).
  - **Proxy:** Select this option if the server is used as the proxy server for a private network protected by a firewall.

Secure communication

Use this section to view the current *identity certificate* used by the server to communicate with other Security Center servers.

- **Issued to:** Subject of the current certificate. A *self-signed certificate* created at software installation appears in the form *GenetecServer-{MachineName}*.
- **Issued by:** Name of the *certificate authority* that issued the certificate. The issuer and the subject are the same for self-signed certificates.
- **Valid from/to:** Validity period of the current certificate.
- **Select certificate (button):** Dialog box listing all certificates installed on this machine. You can use this dialog box to change the certificate used for this server.

Related Topics

Server Admin - Overview page on page 83
Server - Properties tab on page 841

Adding expansion servers

You can add expansion servers to your system at any time to increase the overall computing power of your system.

What you should know

An expansion server is any server machine in a Security Center system that does not host the Directory role. The purpose of the expansion server is to add to the processing power of the system.

Every Security Center system requires its own pool of servers to run the system's functions. You must ensure that enough computing power is available for your system to carry out its required functions.

To add an expansion server:

1. Install Security Center Server on the computer that you want to add to the server pool.

   For more information about installing Security Center Server, see the *Security Center Installation and Upgrade Guide*.
2. Connect that computer to the Security Center's main server.

   The main server is the one that hosts the Directory role. This is done with the Server Admin through a web browser.
3. Open Config Tool on any workstation.
4. From the home page, open the **Network view** task.

   The server you just added should appear in the network tree. The name of the server entity should match the domain name of the server.
5. Select the new server entity, and click the **Properties** tab.

   If the server is used as the proxy server for a private network protected by a firewall, set its **Public address** and **Port** as configured by your IT department.
6. Click **Apply**.

You can now assign roles to the server.

Related Topics
Security Center architecture overview on page 5

Converting the main server to an expansion server

You can convert your main server to an expansion server, if you want a different machine to take on the role of the main server.

Before you begin

- Prepare another server to take over as the new main server on your system. For more information about installing Security Center on a main server, see the *Security Center Installation and Upgrade Guide*.
- If you need to keep your system configuration, and if the Directory database is currently hosted on your main server, then move the Directory database to a different server (this could be the new main server you prepared).

What you should know

You convert a main server to an expansion server by deactivating the Directory role on your server using Server Admin.

CAUTION: This operation restarts the Genetec™ Server service which temporarily deactivates all roles hosted on your server. You must log on again to Server Admin to connect your old main server (converted to an expansion server) to the new main server you prepared.

To convert the main server to an expansion server:

1. Log on to Server Admin on your computer using a web browser.
2. From the server list, select the main server (🌐).

   The Server Admin - Main server page is displayed.
3. Beside the server name, click **Actions** > **Deactivate**.
4. In the confirmation dialog box that appears, click **Continue**.

   The Genetec™ Server service restarts. You are temporarily logged off from Server Admin.
5. Reset the server identification ID.
   a) In a text editor, open the file *GenetecServer.gconfig* found in the *ConfigurationFiles* folder under the Security Center installation folder (*C:\Program Files (x86)\Genetec Security Center 5.5*).
   b) Find and delete the following phrase `<serverIdentification id="<guid>" />`.
   c) Save your changes and close the file.
6. Open a web browser and enter `http://machine/Genetec` in the address bar, where `machine` is the DNS name or the IP address of your server.
7. Log on again to Server Admin.

   The Server Admin - Expansion server page is displayed.
8. Under the *Main server connection* section, enter the name and password of the main server that the expansion server is supposed to connect to, and click **Save**.
9. In the confirmation dialog box that appears, click **Yes**.

   The Genetec™ Server service restarts. You are temporarily logged off from Server Admin.
10. Close your browser page and open a new page.
11. Log on again to Server Admin, and verify that you are connected to the new main server.

Converting an expansion server to the main server

To replace your existing main server or to start a new system, you can convert an expansion server into the main server.

Before you begin

If you are replacing an old main server, and if the Directory database was hosted on your old main server, move the Directory database to the server you want to convert, or to a third computer.

What you should know

You convert an expansion server to a main server by activating the Directory role on your server using Server Admin.

CAUTION: This operation restarts the Genetec™ Server service which temporarily deactivates all roles hosted on your server. You must log on again to Server Admin to activate your software license on your new main server.

To convert an expansion server to the main server:

1. Log on to Server Admin on your computer using a web browser.
2. From the server list, select the expansion server you want to convert.

   The Server Admin - Expansion server page is displayed.
3. Beside the server name, click **Actions** > **Activate**.
4. In the confirmation dialog box that appears, click **Continue**.

   The Genetec™ Server service restarts. You are temporarily logged off from Server Admin.
5. Open a web browser, and enter `http://machine/Genetec` in the address bar, where `machine` is the DNS name or the IP address of your server.
6. Log on again to Server Admin.

   The Server Admin - Overview page is displayed.
7. Activate the software license on the new main server.
8. If you are replacing an old main server, configure the database settings on the Server Admin - Main server page so that this server connects to your existing Directory database.

   This operation forces the expansion server (promoted to main server) to take on the identity of the old main server. This means that if there were roles hosted on the expansion server before, they must be moved to the *new* main server, because the ID of the expansion server has changed.
9. From the Config Tool home page, open the *Network view* task.
10. In the network view, if you see an offline copy of the expansion server you just converted (), delete it.

After you finish

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

Related Topics

Connecting expansion servers to the main server on page 94

Connecting expansion servers to the main server

Whenever you move your main server to a new computer, you must use Server Admin to reconnect all the expansion servers on your system to the new computer.

Before you begin

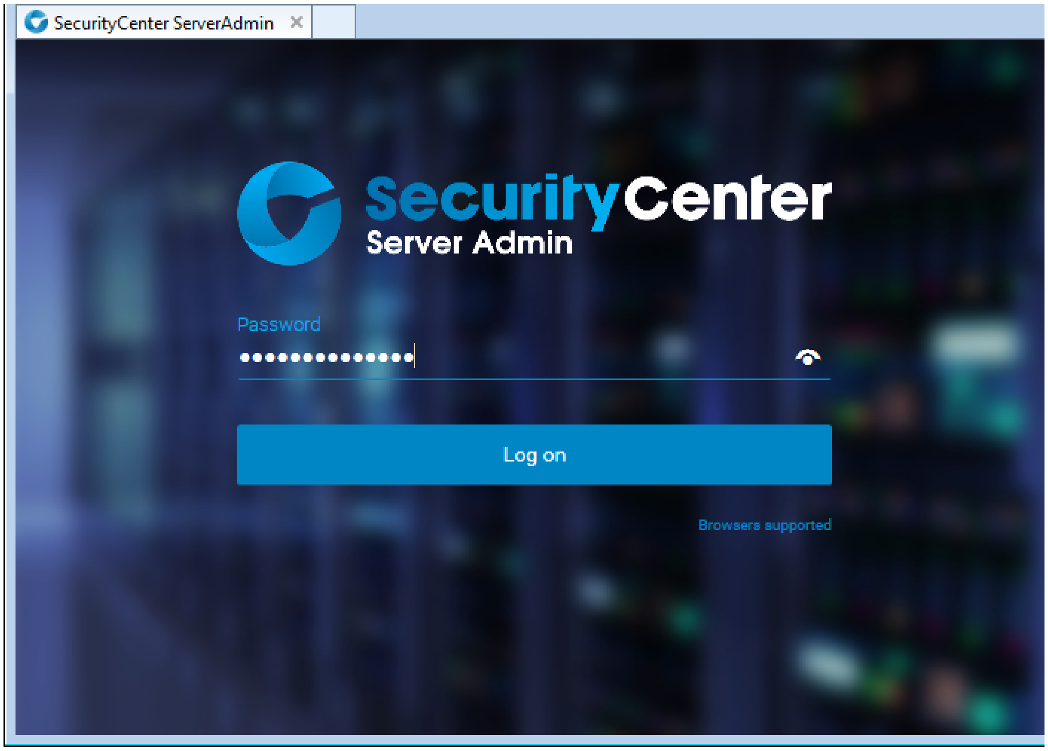
After completing an expansion server installation, the expansion server automatically connects to the main server. You must only go through the steps of connecting your expansion server to your main server if:

- You entered the wrong connection parameters to the main server during the expansion server installation.
- You moved the main server to a different computer.
- You changed the password on the main server while the expansion server was down.
- You enabled Directory authentication on your expansion server, but your Directory certificate is not signed by a trusted certificate authority.

To connect an expansion server to the main server:

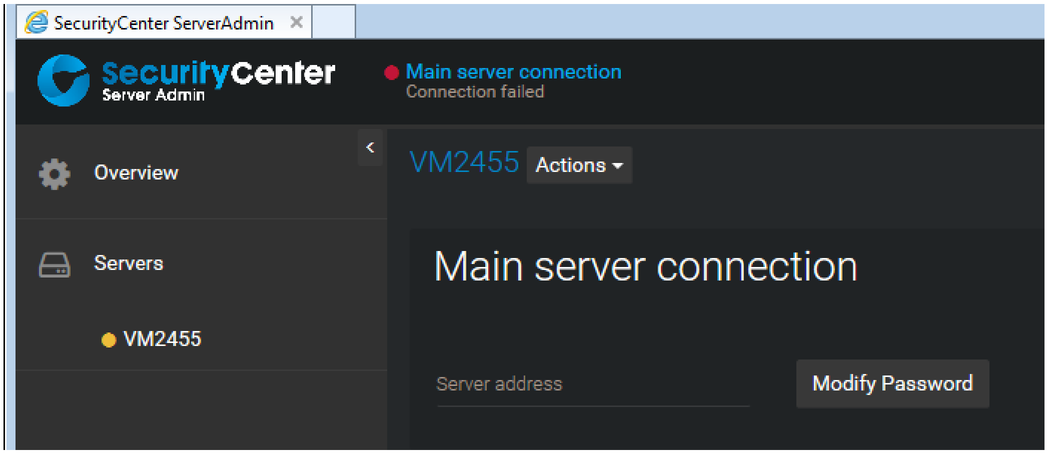
1. Open the Server Admin web page by doing one of the following:
   - In the address bar of your web browser, type `http://computer:port/Genetec`, where `computer` is the DNS name or the IP address of your server, and `port` is the web server port specified during the Security Center Server installation.

     You can omit the web server port if you are using the default value (80).
   - If connecting to Server Admin from the local host, double-click **Genetec Server Admin** (⚙) in the *Genetec Security Center* folder in the Windows Start menu.
2. Enter the server password that you set during the server installation, and click **Log on**.



   The Server Admin *Overview* page appears.

3 If you are not connected to the main server, click **Main server connection** at the top of the Server Admin window.



Main server connection
Connection failed

Main server connection

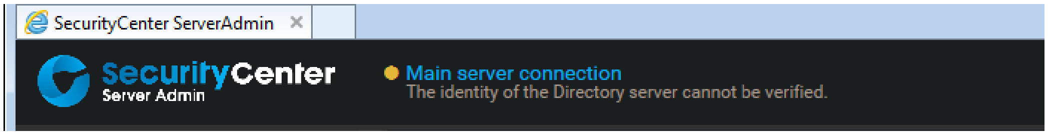
Server address

4 Enter the **Server address** (main server's DNS name or IP address) and **Password**, and then click **Save**.

5 When prompted to restart the service, click **Yes**.

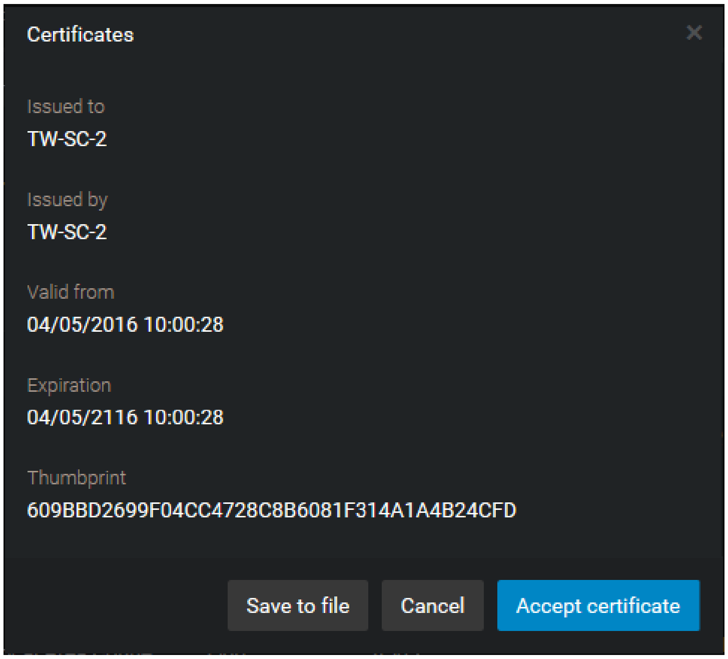
While the *Genetec Server* service restarts, you are temporarily logged off from Server Admin.

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



Main server connection
The identity of the Directory server cannot be verified.

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



Certificates

Issued to
TW-SC-2

Issued by
TW-SC-2

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

Expiration
04/05/2116 10:00:28

Thumbprint
609BBD2699F04CC4728C8B6081F314A1A4B24CFD

IMPORTANT: Once accepted, the certificate is stored in a local whitelist, and you should not be prompted to accept it again. If you are, then you should immediately notify your IT department.

BEST PRACTICE: To avoid the burden of having to accept the certificate of your main server every time someone tries to connect to it from a new machine, only use certificates signed by a certification authority that is trusted by your company's IT.

8 Click **Save**.

9. When prompted to restart the service, click **Yes**.

   While the *Genetec Server* service restarts, you are temporarily logged off from Server Admin.

The expansion server is now connected to the main server. The two servers will remain connected, even when you change the certificate, on either one or both of the servers, as long as the two servers are connected while the change is being made.

Related Topics

What is Directory authentication? on page 308

Activating Security Center license using the web

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

Before you begin

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

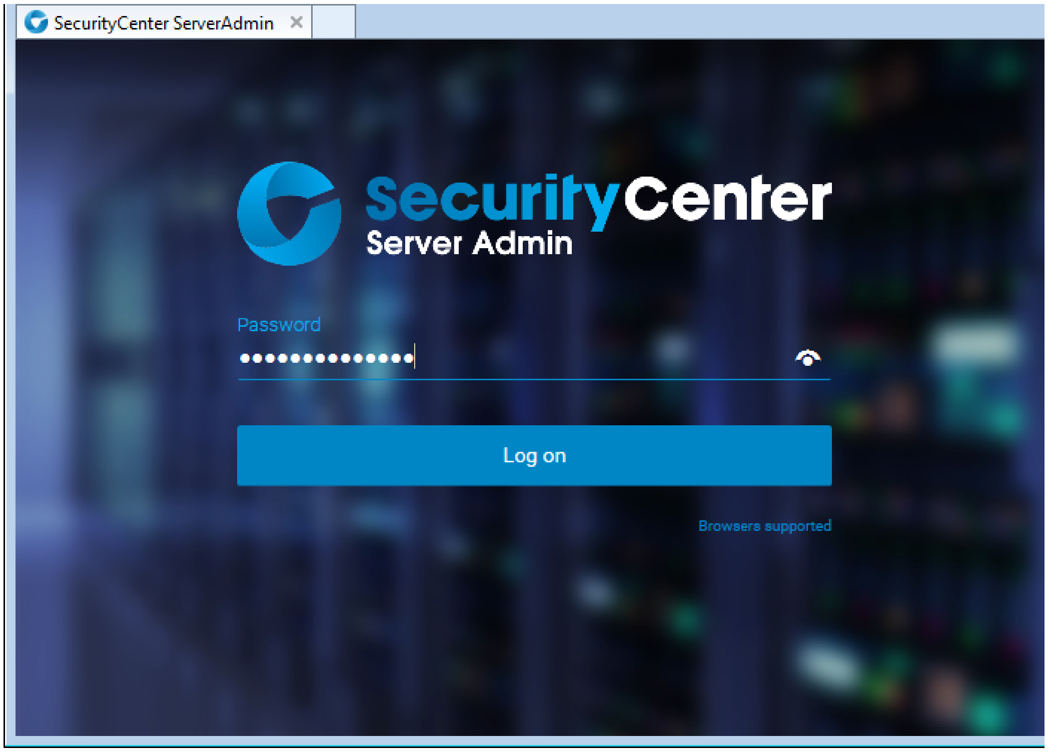
- **Internet connection:** If your server does not have Internet access, then see Activating Security Center license without Internet access on page 100.
- **System ID and password:** The System ID and password are found in the *Security Center License Information* document. Genetec™ Customer Service sends you this document when you purchase the product.
- **Server password:** The server password is used to log on to Server Admin. The server password is set during the installation.

To activate your Security Center license using the web:

1 Open the Server Admin web page by doing one of the following:
  - In the address bar of your web browser, type `http://computer:port/Genetec`, where `computer` is the DNS name or the IP address of your server, and `port` is the web server port specified during the Security Center Server installation.

    You can omit the web server port if you are using the default value (80).
  - If connecting to Server Admin from the local host, double-click **Genetec Server Admin** (⚙) in the *Genetec Security Center* folder in the Windows Start menu.

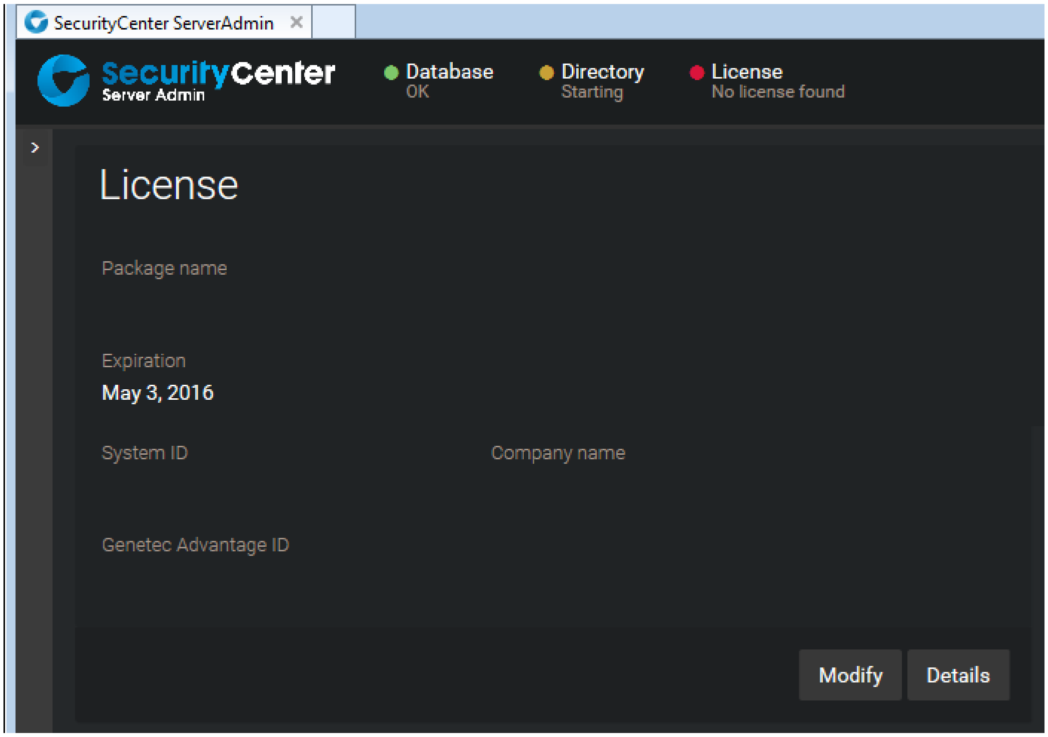
2 Enter the server password that you set during the server installation, and click **Log on**.



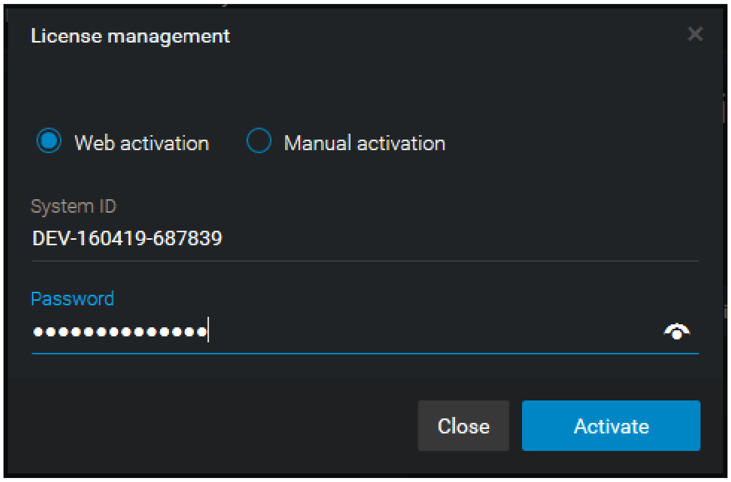
The Server Admin *Overview* page appears.

3 Do one of the following:

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



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



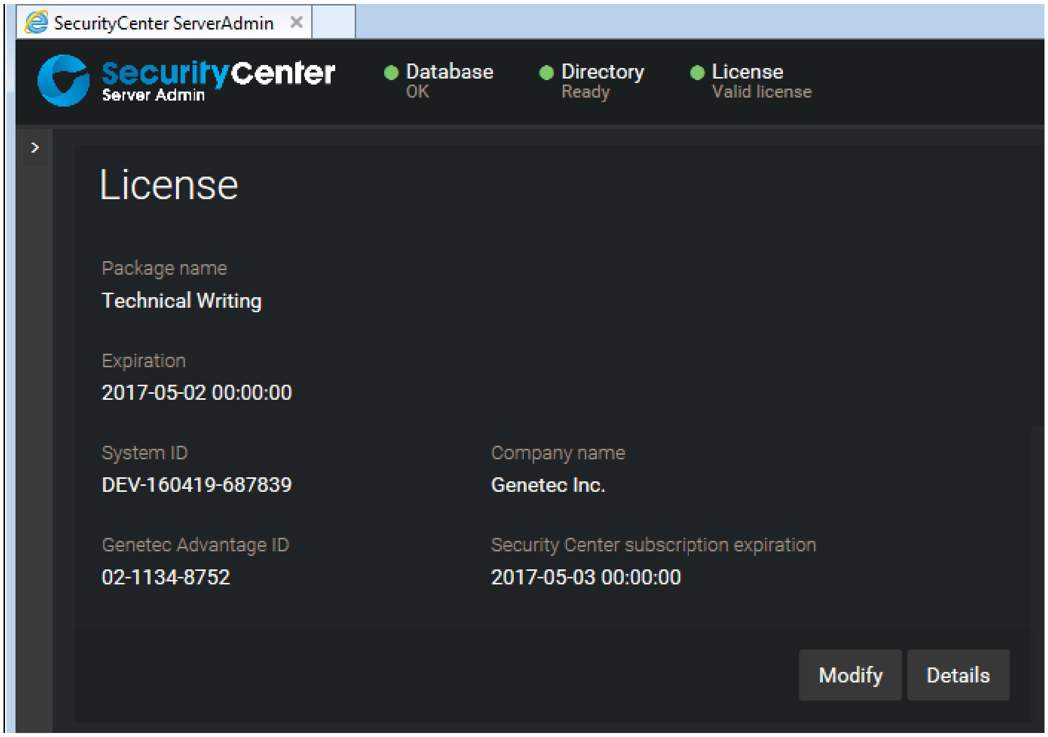
● Web activation ○ Manual activation

System ID: DEV-160419-687839

Password: ••••••••••••••

5 Click **Activate**.

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



License

Package name
Technical Writing

Expiration
2017-05-02 00:00:00

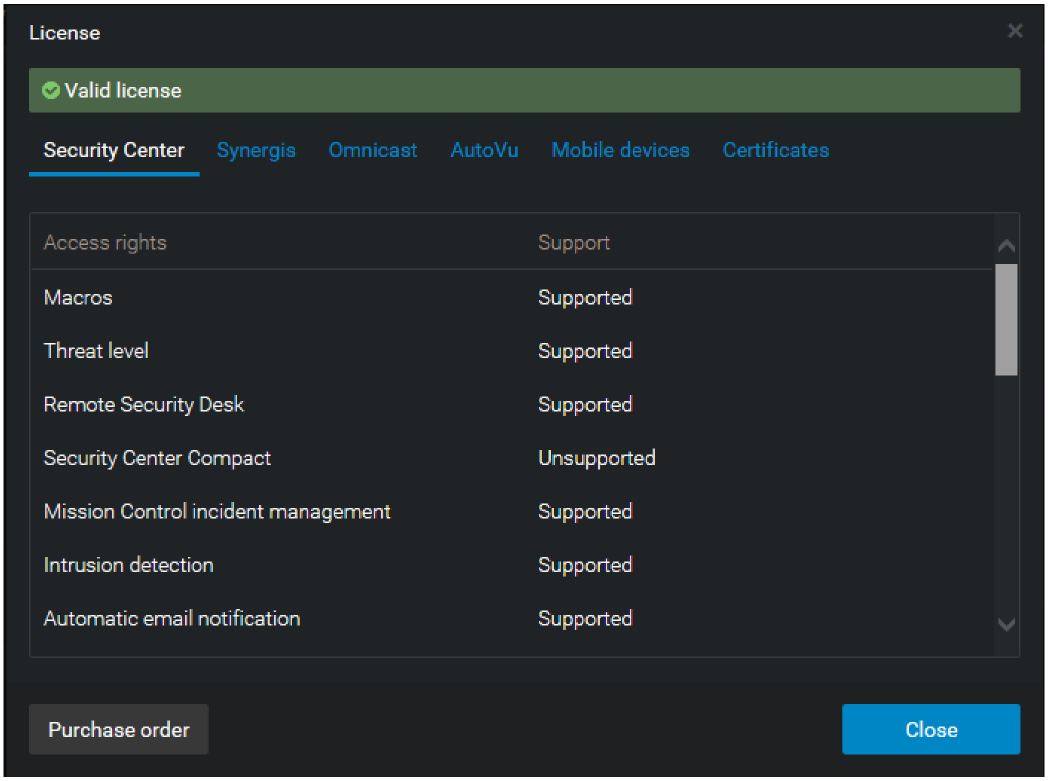
System ID
DEV-160419-687839

Company name
Genetec Inc.

Genetec Advantage ID
02-1134-8752

Security Center subscription expiration
2017-05-03 00:00:00

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


License

✓ Valid license

Access rights	Support
Macros	Supported
Threat level	Supported
Remote Security Desk	Supported
Security Center Compact	Unsupported
Mission Control incident management	Supported
Intrusion detection	Supported
Automatic email notification	Supported

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

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

Activating Security Center license without Internet access

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

Before you begin

To activate your license, you need the following:

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

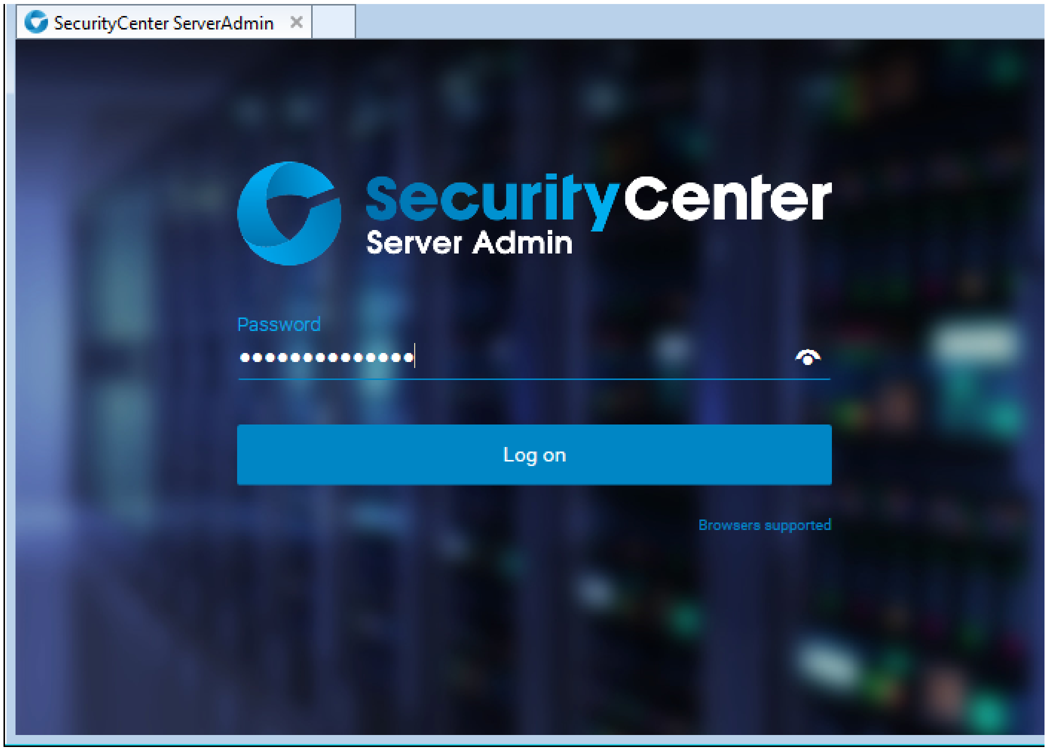
To activate your Security Center license without Internet access:

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

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

  You can omit the web server port if you are using the default value (80).
- If connecting to Server Admin from the local host, double-click **Genetec Server Admin** (⚙) in the *Genetec Security Center* folder in the Windows Start menu.

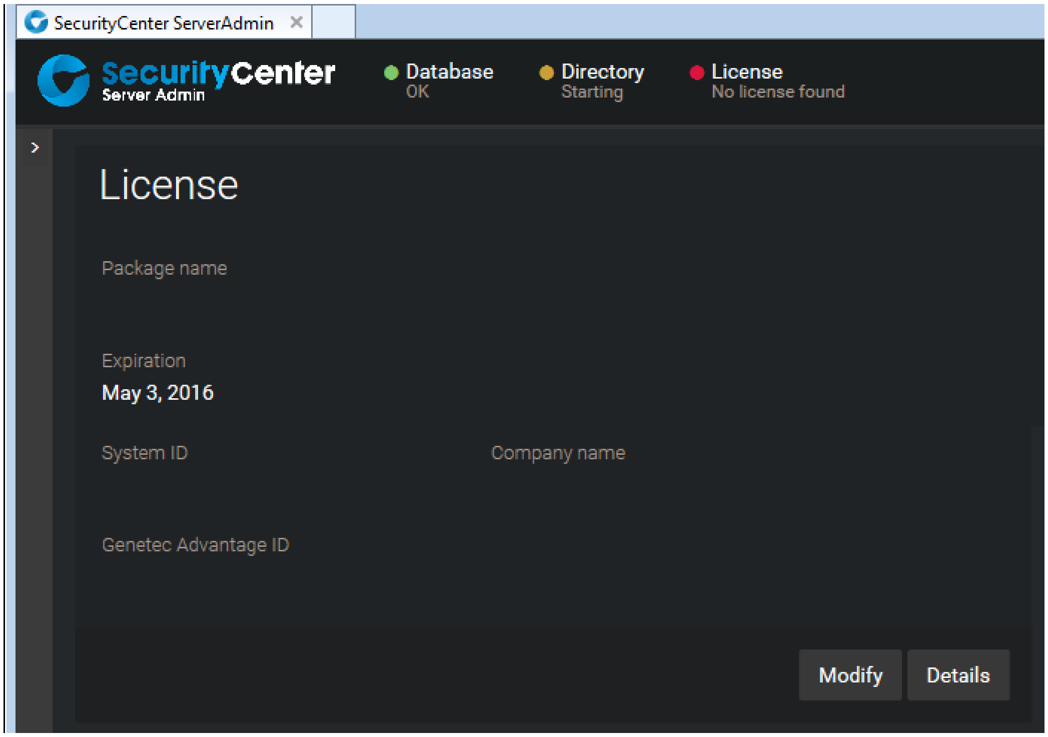
2 Enter the server password that you set during the server installation, and click **Log on**.



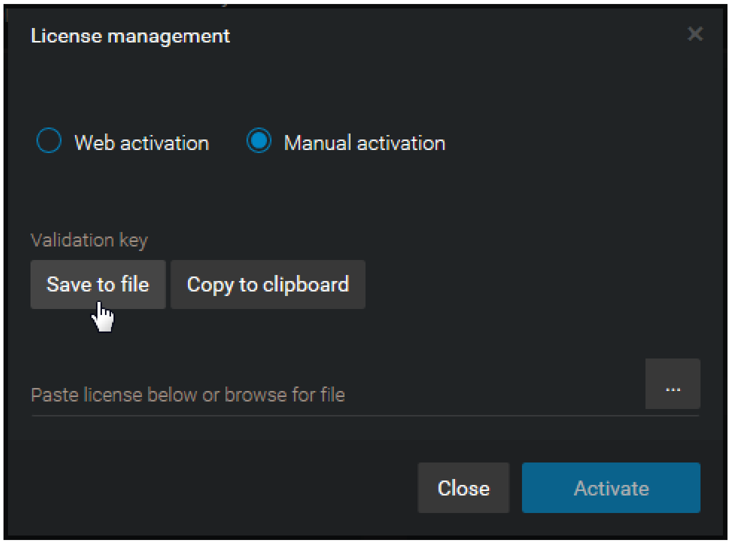
The Server Admin *Overview* page appears.

3 Do one of the following:

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



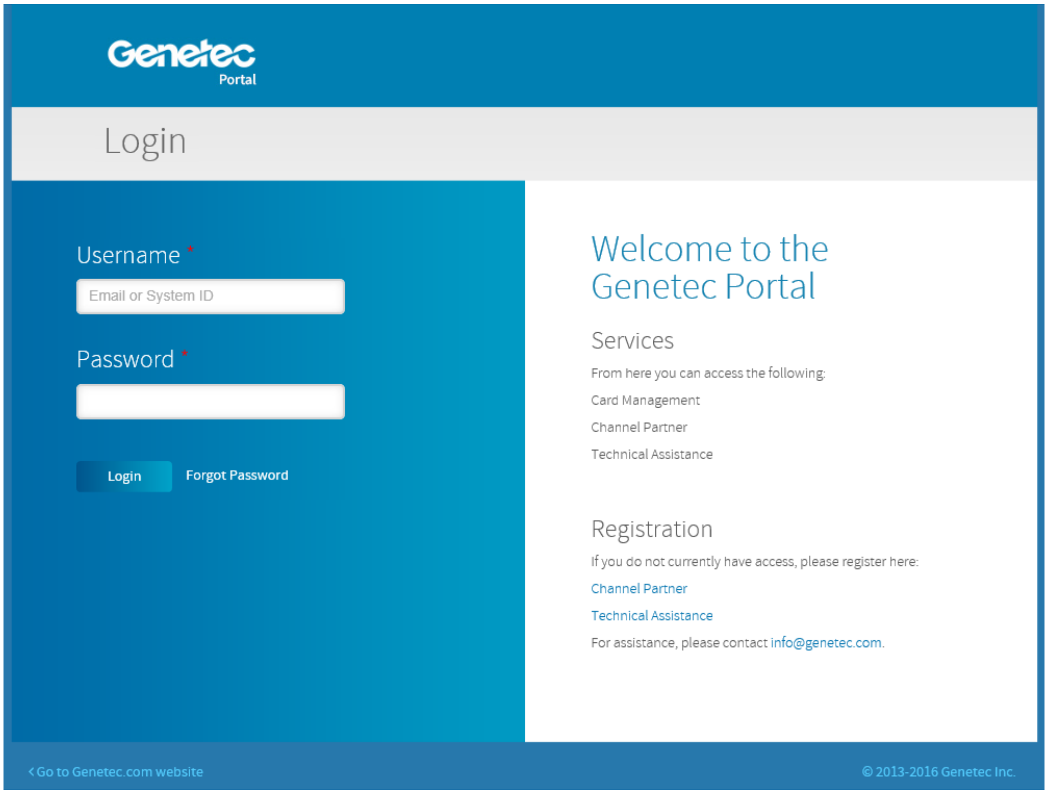
4 In the *License management* dialog box, click **Manual activation**, and then under *Validation key*, click **Save to file**.



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

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

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



Genetec Portal

Login

Username *

Email or System ID

Password *

Login Forgot Password

Welcome to the Genetec Portal

Services

From here you can access the following:

Card Management

Channel Partner

Technical Assistance

Registration

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

Channel Partner

Technical Assistance

For assistance, please contact info@genetec.com.

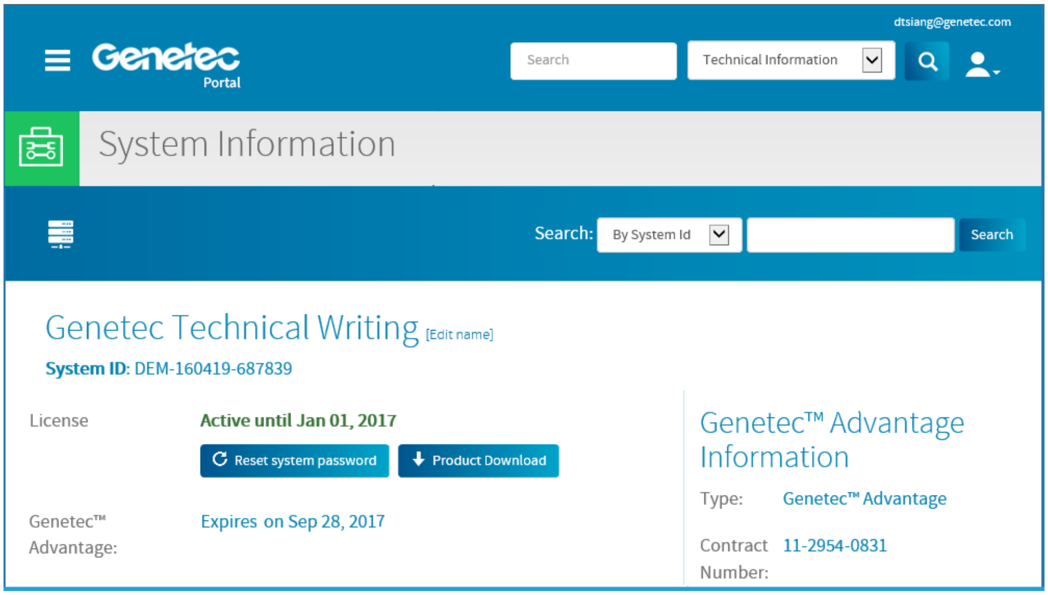
< Go to Genetec.com website

© 2013-2016 Genetec Inc.

6 On the GTAP login page, do one of the following:

- Enter the System ID and the Password specified in the *Security Center License Information* document, and click **Login**.
- Enter your GTAP user account (your email address) and Password, and click **Login**.
  1. On the *Genetec Portal - Home* page, click **Activate new system**.
  2. From the **System ID** drop-down list, select your system, and click **Submit**.

The browser opens to the *System Information* page.



dtsiang@genetec.com

Genetec Portal

Search

Technical Information

System Information

Search: By System Id Search

Genetec Technical Writing [Edit name]

System ID: DEM-160419-687839

License: **Active until Jan 01, 2017**

Reset system password Product Download

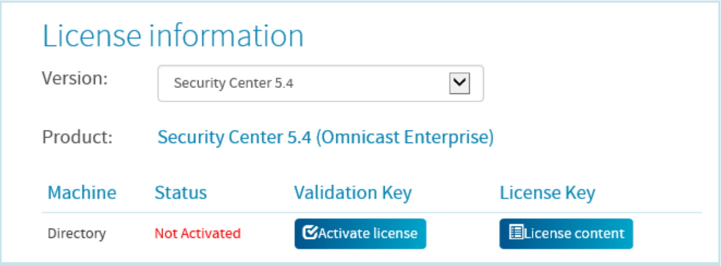
Genetec™ Advantage: Expires on Sep 28, 2017

Genetec™ Advantage Information

Type: Genetec™ Advantage

Contract Number: 11-2954-0831

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



License information

Version: Security Center 5.4

Product: Security Center 5.4 (Omnicast Enterprise)

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

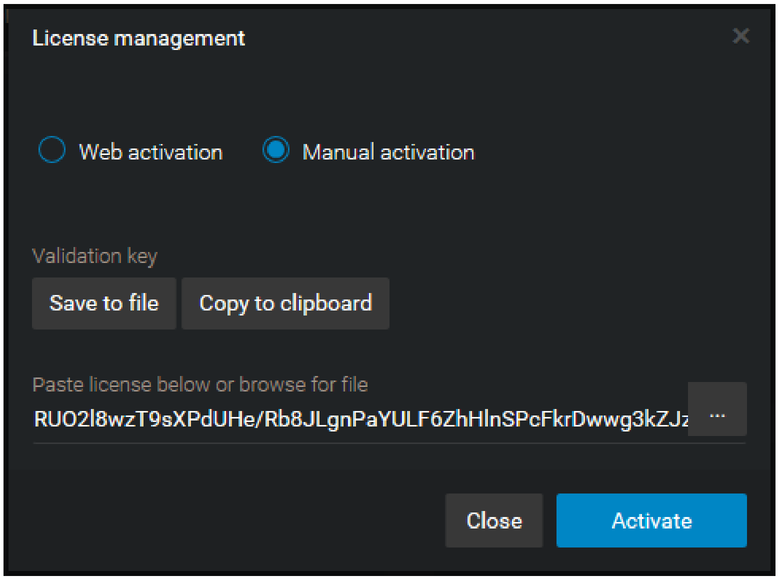
8 In the dialog box that opens, browse to your validation key (.vk file), and click **Submit**.
The message **License activation successful** appears.

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

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

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

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



License management

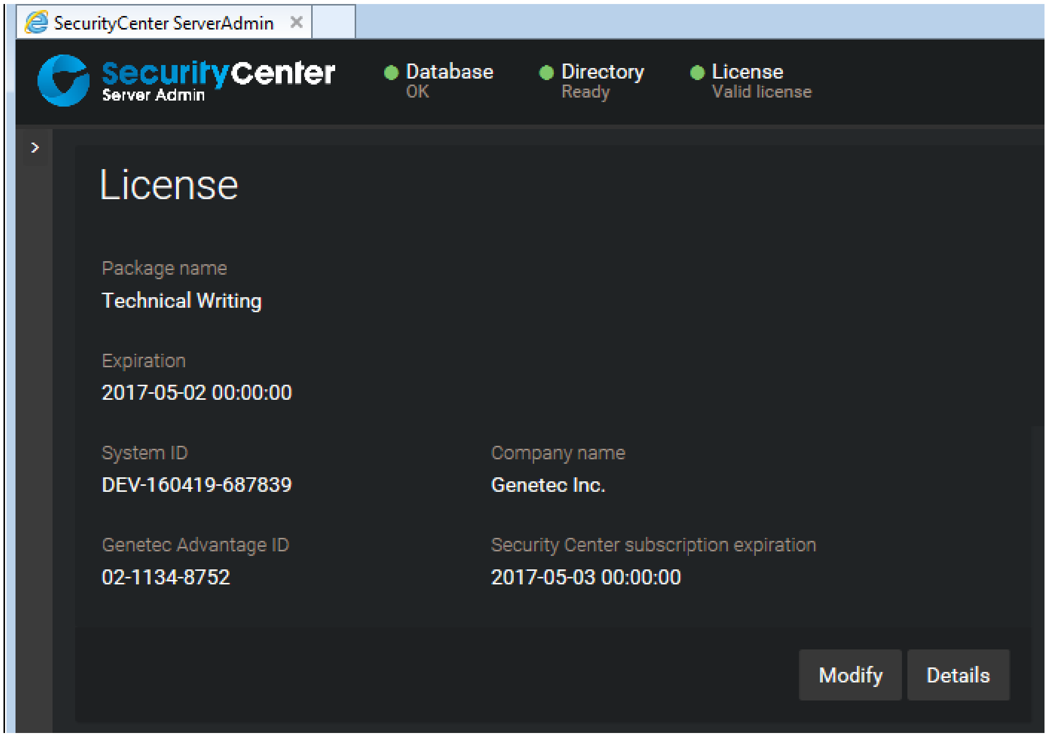
○ Web activation ● Manual activation

Validation key

Paste license below or browse for file

RUO2l8wzT9sXPdUHe/Rb8JLgnPaYULF6ZhHlnSPcFkrDwwg3kZJz

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



License

Package name
Technical Writing

Expiration
2017-05-02 00:00:00

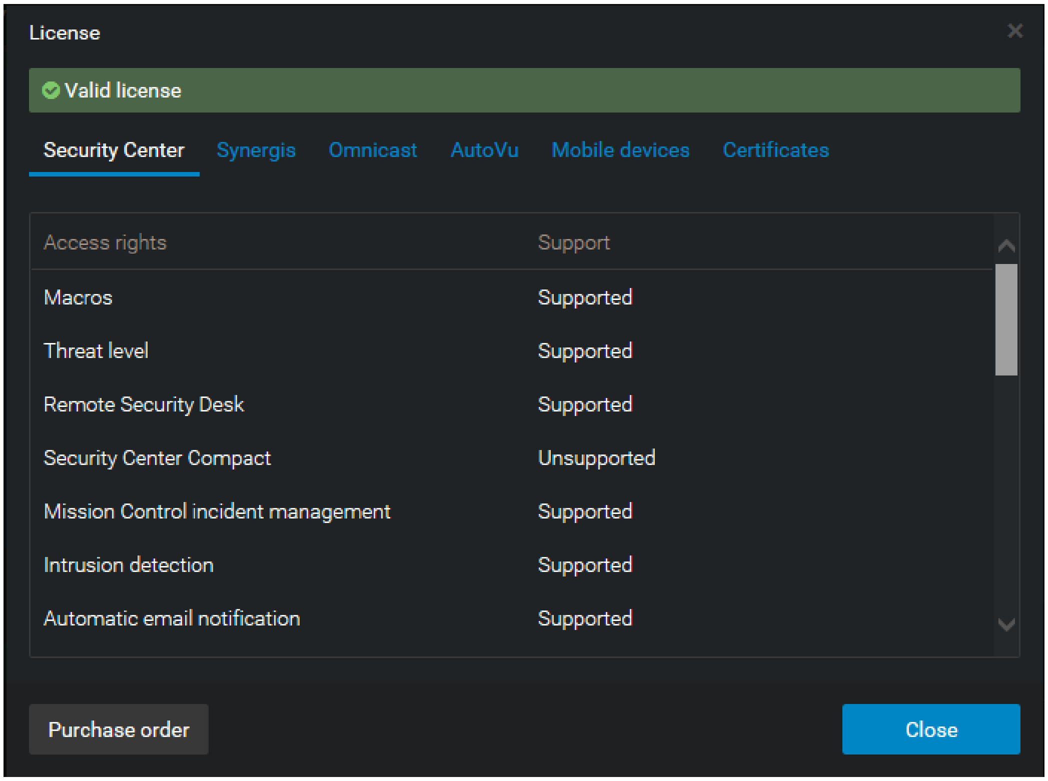
System ID
DEV-160419-687839

Company name
Genetec Inc.

Genetec Advantage ID
02-1134-8752

Security Center subscription expiration
2017-05-03 00:00:00

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



Access rights	Support
Macros	Supported
Threat level	Supported
Remote Security Desk	Supported
Security Center Compact	Unsupported
Mission Control incident management	Supported
Intrusion detection	Supported
Automatic email notification	Supported

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

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

Reapplying your Security Center license

Every time your Security Center license is updated (new camera connections added, expiry date extended, and so on), you must reapply it to your main server for the changes to take effect.

Before you begin

To reapply your license, you need the following:

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

What you should know

If you replace your main server with a new machine, you need to activate your license on the new machine. You do not need to reactivate your license if your main server remains the same.

IMPORTANT: If you have a configuration with multiple Directory servers, you must reactivate your license from Config Tool instead.

To reapply your Security Center license:

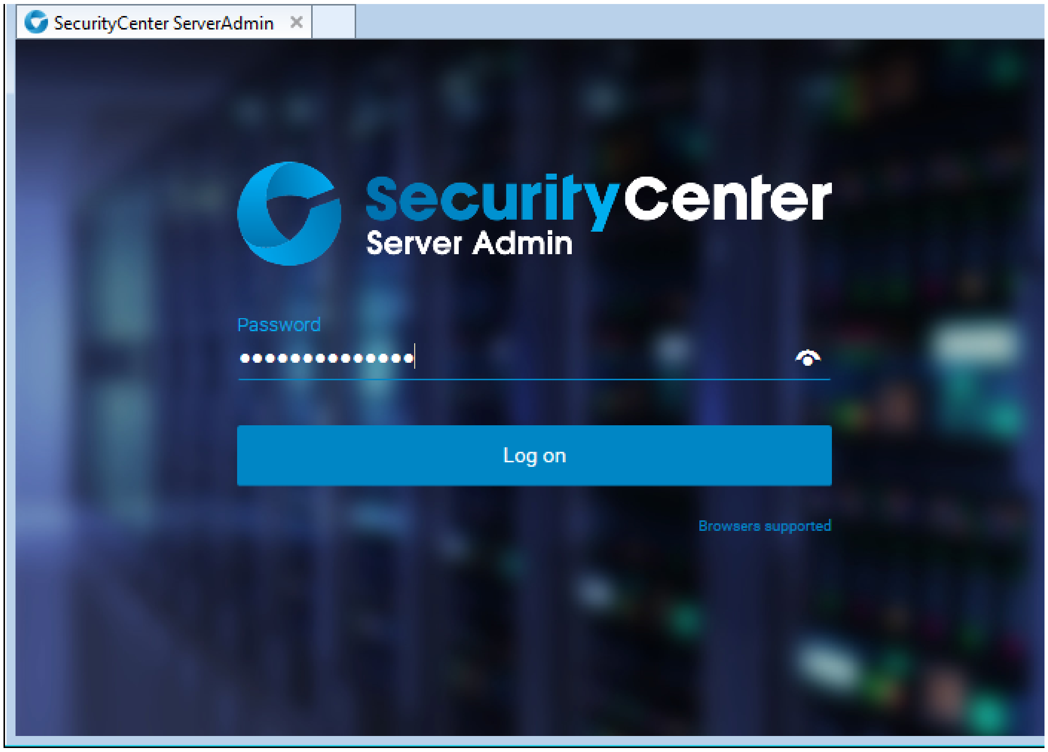
1 Open the Server Admin web page by doing one of the following:

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

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

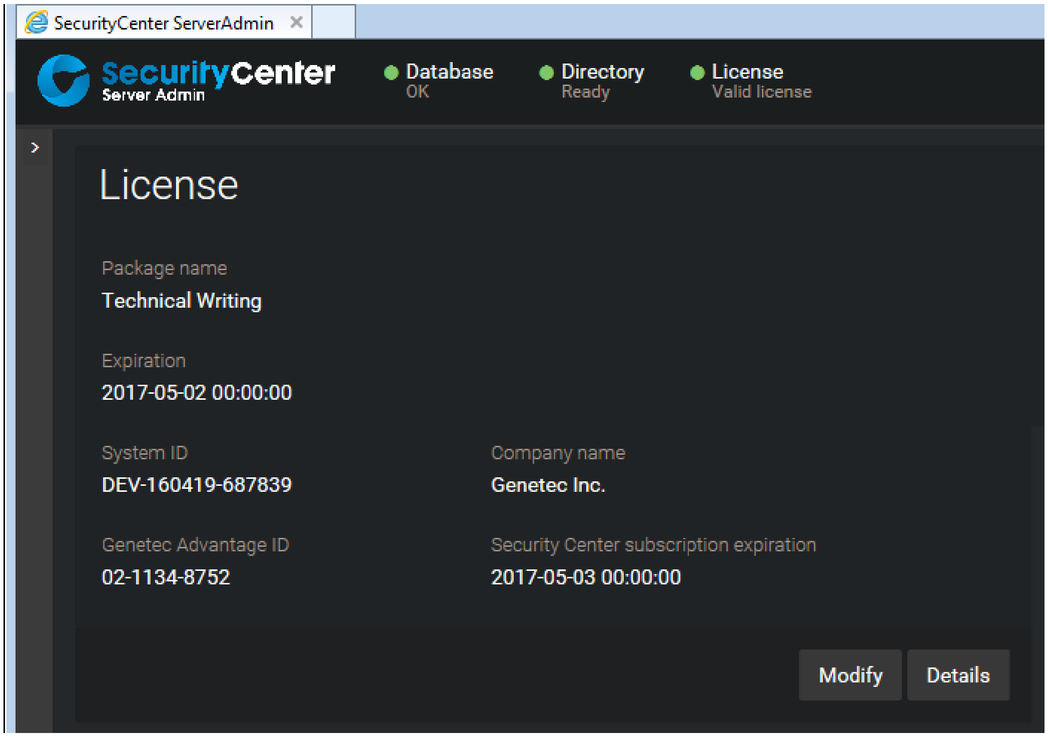
- If connecting to Server Admin from the local host, double-click **Genetec Server Admin** (⚙) in the *Genetec Security Center* folder in the Windows Start menu.

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



The Server Admin *Overview* page appears.

3 Under the *License* section, click **Modify**.



License

Package name
Technical Writing

Expiration
2017-05-02 00:00:00

System ID
DEV-160419-687839

Company name
Genetec Inc.

Genetec Advantage ID
02-1134-8752

Security Center subscription expiration
2017-05-03 00:00:00

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

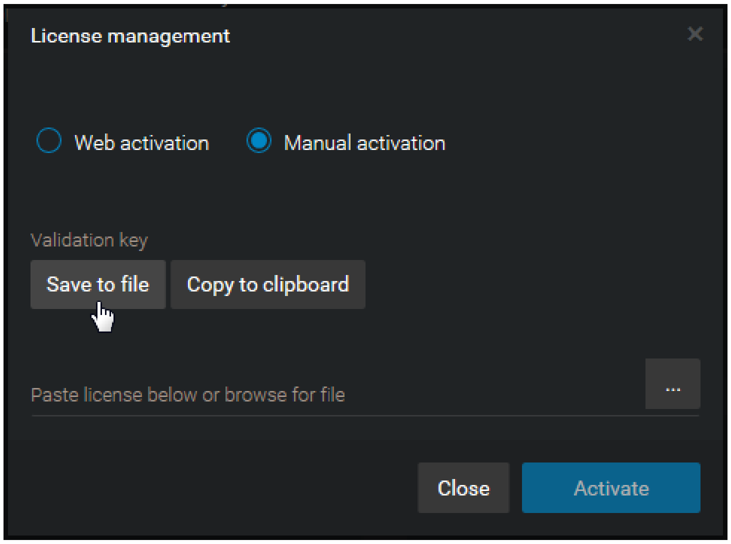
- **Web activation:** (Recommended) Activate your license from the Internet.

  In the dialog box that appears, enter your *System ID* and *Password* and click **Activate**. The process is complete.

- **Manual activation:** Update your Security Center license manually using a license file, then continue with the next step.

5 If your main server is still the same computer, go to step 7.

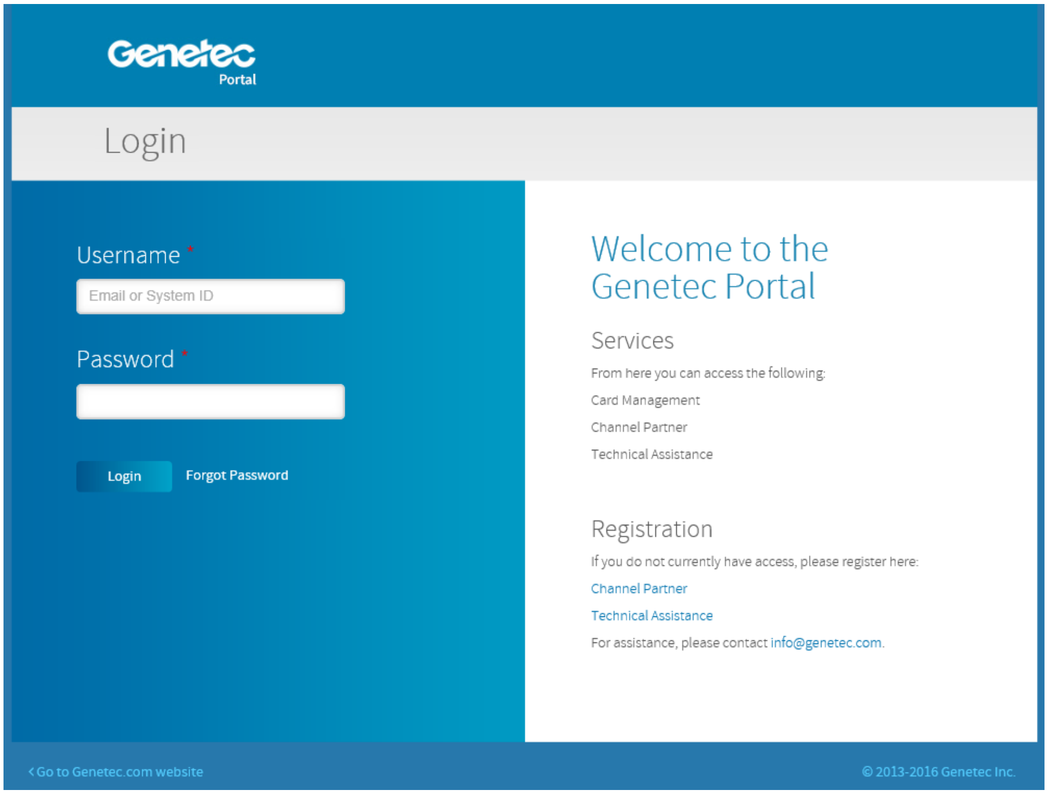
6 In the *License management* dialog box, click **Manual activation**, and then under *Validation key*, click **Save to file**.



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

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

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



Welcome to the Genetec Portal

Services

From here you can access the following:

Card Management

Channel Partner

Technical Assistance

Registration

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

Channel Partner

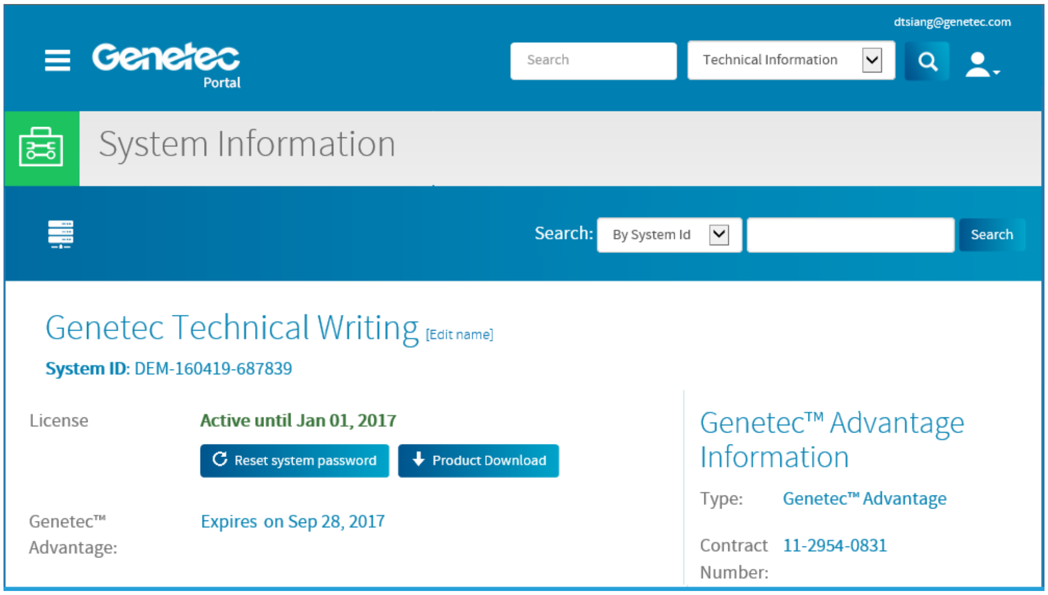
Technical Assistance

For assistance, please contact info@genetec.com.

8 On the GTAP login page, do one of the following:

- Enter the System ID and the Password specified in the *Security Center License Information* document, and click **Login**.
- Enter your GTAP user account (your email address) and Password, and click **Login**.
    1. On the *Genetec Portal - Home* page, click **Activate new system**.
    2. From the **System ID** drop-down list, select your system, and click **Submit**.

The browser opens to the *System Information* page.



Genetec Technical Writing

System ID: DEM-160419-687839

License: Active until Jan 01, 2017

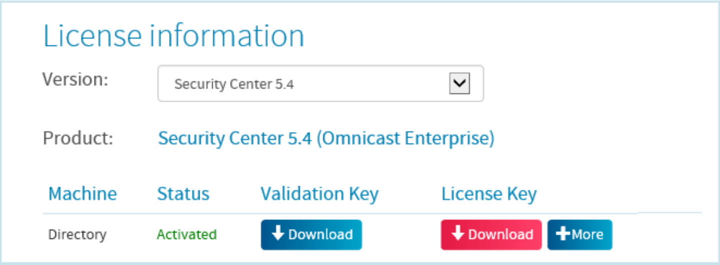
Genetec™ Advantage: Expires on Sep 28, 2017

Genetec™ Advantage Information

Type: Genetec™ Advantage

Contract Number: 11-2954-0831

9 Scroll down to the *License information* section, and do one of the following:



License information

Version: Security Center 5.4

Product: Security Center 5.4 (Omnicast Enterprise)

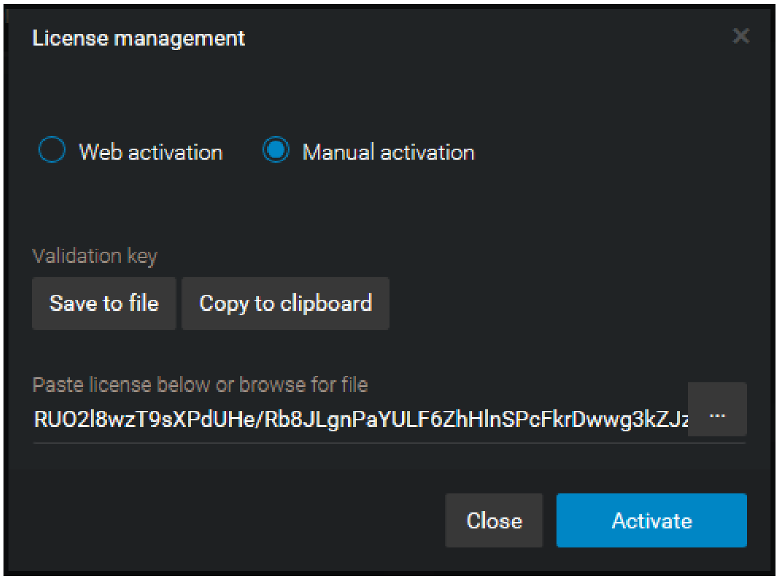
Machine	Status	Validation Key	License Key
Directory	Activated	Download	Download +More

- Below **License Key**, click **Download**, and save the license key to a file.
- Click +**More** > **Send by email**, enter your email address, and click **OK** to have the license key (.lic file) sent to you through email.

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

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

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



License management

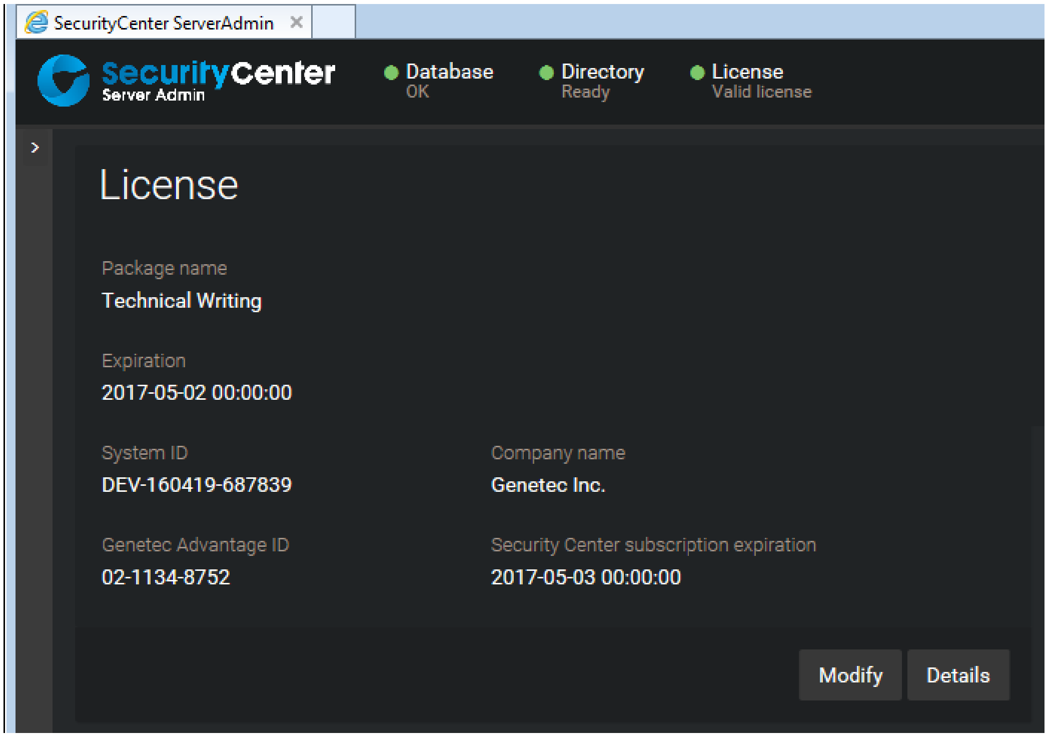
○ Web activation ● Manual activation

Validation key

Paste license below or browse for file: RUO2l8wzT9sXPdUHe/Rb8JLgnPaYULF6ZhHlnSPcFkrDwwg3kZJz

12 Click **Activate**.

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



License

Package name
Technical Writing

Expiration
2017-05-02 00:00:00

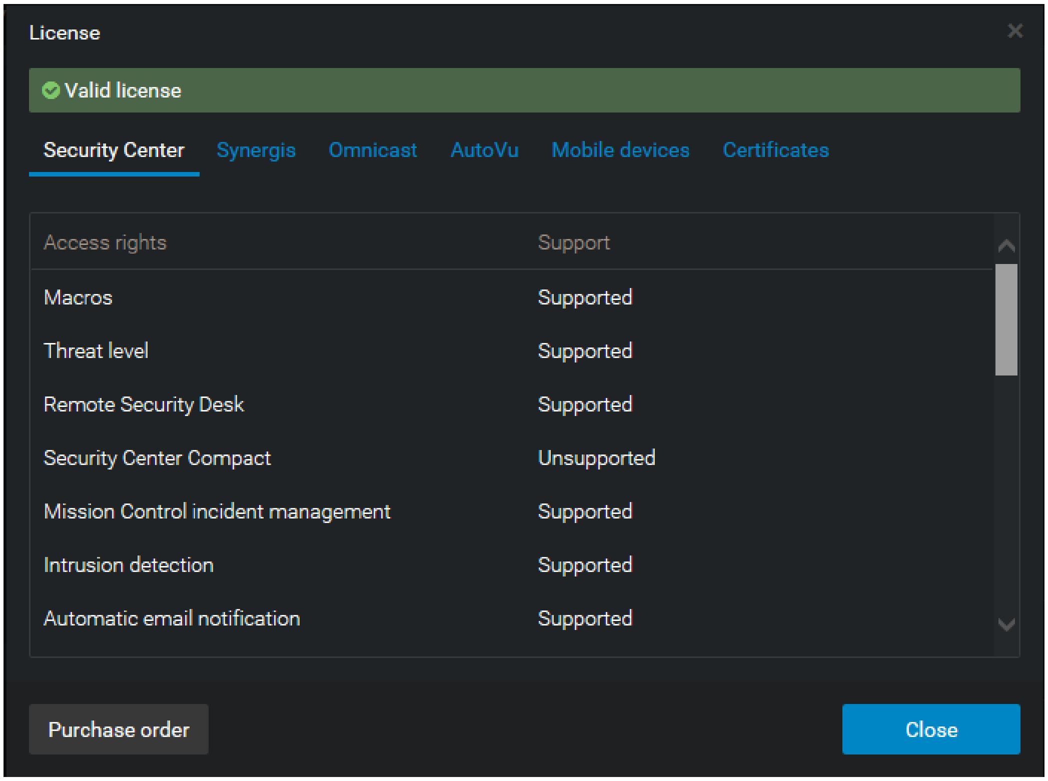
System ID
DEV-160419-687839

Company name
Genetec Inc.

Genetec Advantage ID
02-1134-8752

Security Center subscription expiration
2017-05-03 00:00:00

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



Access rights	Support
Macros	Supported
Threat level	Supported
Remote Security Desk	Supported
Security Center Compact	Unsupported
Mission Control incident management	Supported
Intrusion detection	Supported
Automatic email notification	Supported

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

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

About roles

A role is a software module that performs a specific job within Security Center. Roles must be assigned to one or more servers for their execution. You can assign roles for archiving video, for controlling a group of units, for synchronizing Security Center users with your corporate directory service, and so on.

In Security Center, role entities are defined by the following:

- **Role type:** Determines the specific set of functions that should be performed by the role, such managing *video units* and associated *video archives*.
- **Role settings:** Define the specific set of parameters the role should operate within, such as the retention period for the video archives, or which *database* the system should use.
- **Servers:** The *servers* that should be hosting (running) this role. You can assign one or more roles to a single server, or assign multiple servers to the same role to provide load balancing and failover.

After a role is configured, you can move it to any server on your system (for example, one with a faster processor or more disk space) without having to install any additional software on that server. Moving a role to another server might cause a short pause in the role's operations. In addition, some roles can spawn subprocesses (called *agents*) and execute them simultaneously on multiple servers for greater scalability.

Moving roles to other servers

You can move a role to another server without installing any additional software, for example, if the server that the role is installed on is slow or has limited disk space.

Before you begin

Make sure you have another server configured and ready to accept a new role.

What you should know

Moving a role to another server might cause a short pause in the role's operations.

NOTE: This procedure does not apply to Archiver roles. For moving Archiver roles, see Moving the Archiver role to another server on page 372.

To move a role to another server:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the role you want to modify, and then click the **Resources** tab.
3. If the role requires a database, do one of the following:
   - If the database resides on a third computer, you have nothing to change.
   - If the database is empty, you can create it anywhere you want.
   - If the database contains data and is residing on the current server, move the database to the new server or to a third computer.
4. Under the **Servers** list, click **Add an item** (➕).

   A dialog box appears with all available servers on your system.
5. Select the substitute server and click **Add**.
6. Select the current server in the **Servers** list and click **Delete** (✖).
7. Click **Apply**.

Related Topics
Adding expansion servers on page 91

Deactivating and activating roles

For maintenance or troubleshooting purposes, you can deactivate a role without affecting any of its settings and then re-activate it later

What you should know

If you are experiencing issues with your system, sometimes it is helpful to restart a role. Roles are also deactivated so their properties can be modified. .

You must be a system administrator to deactivate or activate a role.

To deactivate a role:

1 From the home page, open the **System status** task.

2 From the **Monitor** drop-down list, select **Roles**.

The roles that are part of your system are listed in the report pane.

3 Select a role you want to deactivate, and click **Deactivate role** (🚦).

The role turns red (inactive) in the report pane.

4 To reactivate the role, select the role, and click **Activate role** (🚦).

About the Directory role

Directory is the main role that identifies your system. It manages all entity configurations and system wide settings in Security Center.

How the Directory role works

Only a single instance of this role is permitted on your system. The server hosting the Directory role is called the *main server*, and must be set up first. All other servers you add in Security Center are called *expansion servers*, and must connect to the main server to be part of the same system.

The main functions of the Directory role are:

- Client application connection authentication
- Software license enforcement
- Central configuration management
- Event management and routing
- Audit trail and activity trail management
- Alarm management and routing
- Incident management
- Scheduled task execution
- Macro execution

Directory role configuration

Because the Directory role is responsible for the authentication of all client connections, it cannot be configured in the Config Tool client application. To configure the Directory role, you must log on to *Server Admin* from a web browser.

Using Server Admin, you can perform the following administrative tasks:

- Start/stop the Directory role
- Manage the Directory database and change the data retention periods
- View and modify your Security Center license
- View and modify the main server's password and communication ports
- Convert the main server into an expansion server

In a multiple Directory server configuration, Directory *failover* and *load balancing* is managed by the *Directory Manager* role.

Related Topics

Directory failover and load balancing on page 142

About Web-based SDK

The Web-based SDK role exposes the Security Center SDK methods and objects as web services to support cross-platform development.

It allows developers on platforms other than Windows (for example, Linux) to write custom programs that can interact with Security Center.

This role mainly exists for clients who need custom development. Genetec™ Professional Services can help you develop the custom solution you need. To find out more, contact your sales representative, or call us at one of our regional offices around the world. To contact us, visit our website at www.genetec.com.

7

Databases and networks

This section includes the following topics:

Databases

A database is a collection of data that is organized so that its contents can easily be accessed, managed, and updated.

How database hosting works in Security Center

By default, a role's database is hosted on the same server that hosts the role. This is shown in the role's **Resources** tab by the value`(local)\SQLEXPRESS` in the **Database server** field, where "(local)" is the server where the role is running.

If you plan to change the server hosting the role or add secondary servers for failover, the database must be hosted on a different computer.

In addition, the computer hosting the database server does not have to be a Security Center server (meaning a computer where *Genetec Server* service is installed), unless you are configuring Directory database failover using the backup and restore method.

How SQL Server uses memory

If you are using a licensed edition of SQL Server (like SQL Server Standard, SQL Server Business Intelligence, or SQL Server Enterprise) please keep in mind that all databases are managed by Microsoft SQL Server in Security Center. By default, SQL Server is configured to use as much memory as it is available on the system. This could lead to memory issues if you are hosting SQL Server and many roles on the same server, especially on a virtual machine with little memory resources. If you are running out of memory on one of your servers, you can fix the problem by setting a maximum limit to the amount of memory SQL Server is allowed to use.

Related Topics

Moving databases to other computers on page 118
Connecting roles to remote database servers on page 119
Restricting the memory allocated to database servers on page 122

Moving databases to other computers

If you want to change the server hosting a role or add secondary servers for failover, you must host the role's database on a different computer.

What you should know

This procedure is not necessary for the Archiver role. For Archiver roles, it is recommended to host the database locally.

To move a database to another computer:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the role whose database you want to move, and then click **Maintenance** > **Deactivate role** (🚦) in the toolbar at the bottom of the workspace.
3. Click the **Resources** tab.
4. Back up the current database.

   TIP: Since the backup folder is relative to the current server, it might be a good idea to select a network location that can be reached by any server on your system.
5. (Optional) Delete the current database.
6. Create the database on the new machine .
7. Restore the content that you have backed up to the new database.
8. Click **Apply**.
9. In the toolbar at the bottom of the workspace, click **Activate** (🚦).

Connecting roles to remote database servers

If a role’s database is hosted on a different computer than the role, you must configure the remote database server (SQL Server) to accept connection requests from the role.

Before you begin

On the computer hosting SQL Server, open TCP ports 1433 and 1434 on Windows Firewall.

To connect a role to a remote database server:

1 Allow remote connection on your SQL Server instance.

   a) On the server hosting the database, open *Microsoft SQL Server Management Studio* and connect to the *database server* used by Security Center.

   b) In the **Microsoft SQL Server Management Studio** window, right-click the database server name ( ) in the **Object Explorer**, and select **Properties**.

   c) In the **Server Properties** window, select the **Connections** page.

   d) Under the section **Remote server connections**, select the option **Allow remote connections to this server**.

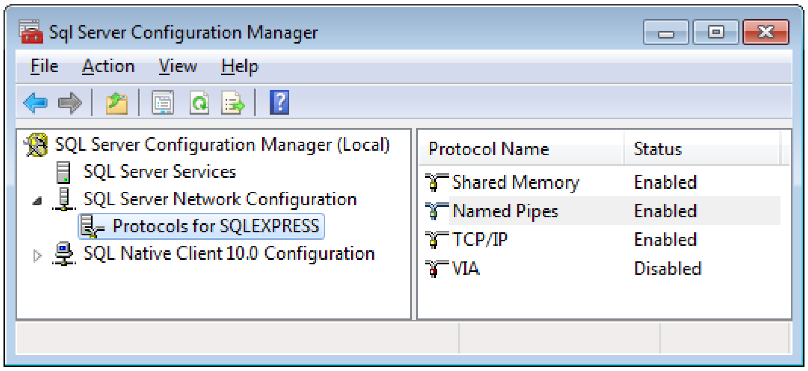
   e) Click **OK** and close *Microsoft SQL Server Management Studio*.

2 Enable **Named Pipes** and **TCP/IP** protocols on your SQL Server instance.

   a) On the server hosting the database, open *SQL Server Configuration Manager*.

   b) Expand the **SQL Server Network Configuration** section, and select the protocols for your database server instance (for example, **Protocols for SQLEXPRESS**).

   c) Right-click the **Named Pipes** and **TCP/IP** protocols, and set their status to **Enabled**.


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled
VIA	Disabled

   d) Close *SQL Server Configuration Manager*.

3 Make sure your SQL Server instance is visible from other computers on your network.

   a) On the server hosting the database, open *Microsoft Management Console Services* (`services.msc`).

   b) Start the service named **SQL Server Browser**.

   c) Right click the SQL Server Broswer service, and click **Properties**.

   d) In the **General** tab, from the **Startup type** drop-down list, select **Automatic**.

   The SQL Server instance is now available from the **Database server** drop-down list of any role’s **Resources** tab in Config Tool.

4 Restart your SQL Server instance to enable the settings you have changed.

   a) On the server hosting the database, open *Microsoft Management Console Services* (`services.msc`).

   b) Right-click the SQL Server instance service (for example `SQL Server (SQLEXPRESS)`), and click **Restart**.

5 On every server that hosts your Security Center roles, change the logon user of the **Genetec Server** service to a Windows administrator account that also has the permissions to access the SQL Server instance you just modified.

The Windows administrator account is usually a domain account used to connect to all servers.

a) On the server hosting the role, open *Microsoft Management Console Services* (`services.msc`).
b) Right-click the **Genetec Server** service, and click **Properties**.
c) In the **Log on** tab, select the **This account** option, and type an administrator **Account name** and **Password**.
d) Click **Apply** > **OK**.
e) Repeat these steps on every server that is hosting a Security Center role that will connect to the remote database server.

Granting SQL Server permissions

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

What you should know

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

For more information about server roles and their capabilities, see your Microsoft documentation.

NOTE: The following procedure is for SQL Server 2014 Express. If you are using a different version of SQL Server, see your Microsoft documentation for information about granting permissions.

To grant SQL Server permissions:

- In SQL Server Management Studio, do one of the following:
  - Execute the following query: `GRANT VIEW SERVER STATE TO [login name]`.
  - Manually modify the user permissions as follows:
    1. Right-click on the appropriate SQL server instance and select **Properties**.
    2. Click the *Permissions* page.
    3. Under **Logins or roles**, select the user or role you want to modify.
    4. In the **Permissions** section, click the **Explicit** tab and select the **Grant** check box beside the **View server state** permission.
    5. Click **OK**.

After you finish

For users that are granted the permission locally on the Security Center server, you must add them as users on the SQL Server.

Restricting the memory allocated to database servers

The database server (SQL Server) is configured to use as much memory as it is available on the system. If you are experiencing issues with insufficient memory, you can fix the problem by setting a maximum limit to the amount of memory SQL Server is allowed to use.

To restrict the memory used by SQL Server:

1. On the server hosting the database, open *Microsoft SQL Server Management Studio*.
2. In the **Microsoft SQL Server Management Studio** window, right-click the database server name () in the **Object Explorer**, and select **Properties**.
3. In the **Server Properties** window, select the **Memory** page.
4. In the field **Maximum server memory (in MB)**, enter the maximum memory SQL Server is allowed to use.

   Microsoft recommends the following guidelines:

   - RAM = 2 GB, Maximum server memory = 1000 MB
   - RAM = 4 GB, Maximum server memory = 2200 MB
   - RAM = 6 GB, Maximum server memory = 3800 MB
   - RAM = 8 GB, Maximum server memory = 5400 MB
   - RAM = 12 GB, Maximum server memory = 8000 MB
   - RAM = 16 GB, Maximum server memory = 13500 MB
   - RAM = 24 GB, Maximum server memory = 21500 MB

5. Click **OK**, and close *Microsoft SQL Server Management Studio*.

The SQL Server service automatically adjusts its memory footprint.

Creating databases

Under certain circumstances, you might need to create a new database, overwrite the default database assigned to a role, or assign a different database that is prepared by your IT Department if you plan on using a dedicated database server.

Before you begin

If you plan on overwriting the existing database with the new one, you should backup the existing database.

What you should know

All role databases are created from Config Tool, except the Directory database, which must be created from the Server Admin - Main Server page. The procedures are very similar in both cases. Therefore, only creating from Config Tool is described here.

To create a database:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select a role, and click the **Resources** tab
3. From the **Database server** drop-down list, type or select the name of the database server.

   The value `(local)\SQLEXPRESS` corresponds to *Microsoft SQL Server 2014 Express Edition* that was installed by default with *Genetec Security Center Server*.To specify a database server on a different server than the one hosting the role, enter the name of that remote server.
4. From the **Database** drop-down list, type or select the name of the database.

   The same database server can manage multiple database instances.
5. Click **Create a database**.
6. Specify the database creation options.

   CAUTION: If you select the **Overwrite existing database** option, all current content of the selected database is lost.
7. Click **OK.**

   The database creation starts. A window appears, showing the progress of this action. You can close this window, and review the history of all database actions later on by clicking **Database actions** in the notification tray.
8. Wait until you see **Database status** indicating **Connected**.

Related Topics

Backing up databases on page 127

Receiving notifications when databases are almost full on page 126

Deleting databases

To free up disk space, you can delete databases you no longer use.

What you should know

All role databases are deleted from Config Tool, except the Directory database, which must be deleted from the Server Admin - Main Server page. The procedures are very similar in both cases. Therefore, only deleting from Config Tool is described here.

To delete a database:

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

2 Select a role, and click the **Resources** tab

3 From the **Database** drop-down list in the **Resources** tab of a role, select the database you want to delete.

   NOTE: This does not need to be your current database.

4 Click **Delete the database** (✖).

   CAUTION: A confirmation dialog box appears. If you continue, the database is permanently deleted.

5 Click **Delete** in the confirmation dialog box.

   The database deletion starts. A window appears, showing the progress of this action. You can close this window, and review the history of all database actions later on by clicking **Database actions** in the notification tray.

6 Create a new database for the role.

After you finish

Connect the role to an existing database or create a new database.

Related Topics

Creating databases on page 123

Viewing database information

You can view the information about a role's database, such as the database server and database versions, how much disk space is available, and a summary of the data it holds.

What you should know

The database information provided varies depending on the role. You might be asked to provide information on a role’s database when you contact Technical support.

All roles' database information are viewed from Config Tool, with the exception of the Directory database, which must be viewed from the Server Admin - Main Server page. The procedures are very similar in both cases. Therefore, only viewing from Config Tool is described here.

To view a role's database information:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select a role, and click the **Resources** tab.
3. Click **Database info** (ⓘ).

   The following information can be displayed, depending on the role:

   - **Database server version:** Software version of the database server.
   - **Database version:** Schema version of the role’s database.
   - **Approximate number of events:** (Also called *Approximate number of archived events* and *Event count*) Number of events that are stored in the role’s database.
   - **Source count (Archiver and Auxiliary Archiver only):** Number of video sources (cameras) that have archives.
   - **Video file count (Archiver and Auxiliary Archiver only):** Number of video files.
   - **Size on disk:** Size of the Database files.
   - **Approximate number of entities (Directory only):** Number of entities (areas, cameras, doors, schedules, and so on) in the system.
   - **Approximate number of active alarms (Directory only):** Number of active alarms (not yet acknowledged) in the system.
   - **Approximate number of archived alarms (Directory only):** Number of past alarms available for reporting, excluding the active ones.

Receiving notifications when databases are almost full

You can configure different roles to send you an email notification when their database space is running low.

Before you begin

To make sure that the email notification is sent, configure the **SMTP** and **Watchdog** settings on the server hosting the role.

What you should know

All role database notifications are configured from Config Tool, except for the Directory database, which must be configured from the Server Admin - Main Server page. The procedures are very similar in both cases. Therefore, only the configuration from Config Tool is described here.

To receive a notification when a role's database is almost full:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select a role, and click the **Resources** tab.
3. Click **Notifications** ().
4. In the dialog box that opens, set the following options:
   - **Disk space:** Sends a notification when the remaining free space on the disk falls below a certain threshold (in GB).
   - **Database usage:** Sends a notification when the space used by the role's database reaches a certain percentage. This option is only for the Express edition of SQL Server, whose database size is limited to 10 GB. If you are using a full edition of SQL Server, this option has no effect.
5. Click **OK**.

Related Topics
Server Admin - Main server page on page 86

Backing up databases

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

What you should know

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

NOTE: The following cases are exceptions:

- To back up the Archiver and Auxiliary Archiver role databases with their associated video files, see Transferring video archives manually on page 448.
- To back up the Directory database while the *Backup and restore* failover mode is enabled, see Generating full Directory database backup on page 157.
- There are restrictions regarding the backup and restore of the Directory database when the *Mirroring* failover mode is enabled. For more information, refer to the Microsoft SQL Server Database Mirroring documentation.

To back up a role's database:

1 From the Config Tool home page, open the *System* task, and click the **Roles** view.
2 Select a role, and click the **Resources** tab.
3 Click **Backup/Restore** (▭).
4 In the *Backup/Restore* dialog box, beside the **Backup folder** field, click **Select folder** (📁), and select the folder where you want to save the backup file.

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

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

   If you select this option, you'll need to unzip the backup file before you can restore it.
6 Click **Backup now**.

A backup file is created in the backup folder with the file extension BAK. The name of the file is the database name, followed by "_ManualBackup_", and the current date (mm-dd-yyyy).

Backing up databases on a schedule

For extra protection for your data, you can configure database backups to be performed periodically.

To back up a role's database on a schedule:

1 From the Config Tool home page, open the *System* task, and click the **Roles** view.
2 Select a role, and click the **Resources** tab.
3 Click **Backup/restore** (▭).
4 In the **Backup/Restore** dialog box, switch the **Enable automatic backup** option to **ON**.
5 Select the day and time to perform the backup (every day or once a week).

   TIP: It is a good idea to stagger the backup operations if several different databases need to be backed up on the same machine.

6 Specify how many backup files you want to keep.

NOTE: The backup files you create manually are not counted in that number.

7 Click **OK** > **Apply**.

The automatic backup starts at the next scheduled date and time.

Restoring databases

If you just restored a server, moved a server to another computer, reinstalled or upgraded SQL Server, or made some configuration mistakes that you want to undo, you can restore the old database.

Before you begin

Back up the current database before you restore an old database. If the **Compress backup** file option was selected during backup, you must first unzip the backup file before you can restore it.

What you should know

All role databases are restored from Config Tool, except the Directory database, which must be restored from the Server Admin - Main Server page. The procedures are very similar in both cases. Therefore, only restoring databases from Config Tool is described here.

NOTE: The following cases are exceptions:

- To restore an Archiver or Auxiliary Archiver role database backed up using the *Archive transfer* task, see Restoring video archives on page 447.
- You cannot restore the Directory database from Server Admin when the *Mirroring* failover mode is enabled. For more information on the restrictions regarding backup and restore while the *database mirroring session* is active, refer to the Microsoft SQL Server Database Mirroring documentation.

To restore a role's database:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select a role, and click the **Resources** tab.
3. Click **Backup/restore** (▭).
4. In the **Backup/Restore** dialog box, beside the **Restore folder** field, click **Select folder** (📁), and select the backup file you want to restore.

   NOTE: The path is relative to the server hosting the role, not to the workstation where you are running Config Tool.

5. Click **Restore now**.

The current content of the database is replaced by the content restored from the backup file.

About networks

The network entity is used to capture the characteristics of the networks used by your system so that proper stream routing decisions can be made.

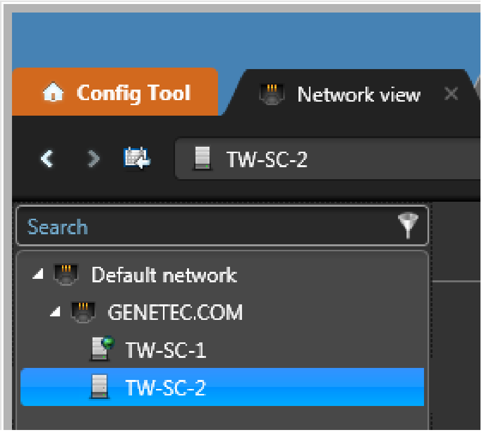
Unless your entire system runs from a single private network without communicating with the outside world, you must configure at least one network entity other than the *Default network* to describe your networking environment.

How network entities are created

Network entities are created automatically by the system.

After installing Security Center on your main server, you'll have the following two network entities on your system:

- The *Default network* is the root node on the network tree. Its video transmission capabilities are set to *Unicast TCP*, which is the characteristic shared by all IP networks. You cannot delete the *Default network* entity.
- A second network entity attached to the *Default network*, that corresponds to your company's network (where your main server is located).



After that, more network entities are added to your system when you add new servers belonging to different networks.

Network routes

Between every two networks on your system there is a route. The data transmission capabilities of the route are limited to the smallest capability set of the two end points.

For example, if one end is capable of multicast and the other end is only capable of unicast UDP, the capabilities of the route between these two end points cannot be more than unicast UDP.

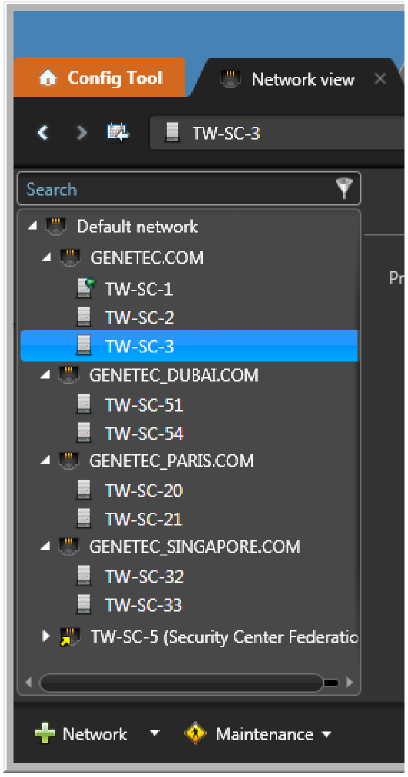
If the connection between the two end points (for example VPN) only supports unicast TCP, you might have to further limit the capabilities of a route.

Related Topics
Adding networks on page 132

About the Network view

The network view is a browser view that illustrates your network environment by showing each server under the network they belong to. You can manage this view through the *Network view* task. The hierarchy in the *Network view* task displays the *networks* () and the *servers* () found in your system, and lets you configure them. The *main server* hosting the *Directory* role is shown with a different icon ().

Having an accurate representation in the *Network view* helps you visualize the actual setup of your system.



A federated network () is created for every federated system. It allows you to control how media from that system is accessed from the local system, to force media redirection, and to set the route capabilities.

When a server with mulitple network interface cards (NIC) is added to the system, only the first address defined in the operating system is represented by default as a network entity. However, you can add the other network entities manually, if later, you need to have a better control of the routing capabilities.

Adding networks

If your system spreads across multiple networks or you allow your users to connect to the main server over the Internet, you must configure the network view and add additional networks.

To add a network:

1 Open the **Network view** task.

2 If you are creating a subnet, select the parent network in the network tree. Otherwise, select the *Default network*.

3 Click **Network** (➕), and enter the name of the network entity.

You are automatically placed in the network's **Properties** tab.

4 From the **Capabilities** drop-down list, select the data transmission type for streaming live video on the network.

TIP: Always select the largest set of capabilities that your network supports.

- **Unicast TCP:** Unicast (one-to-one) communication using TCP protocol is the most common mode of communication. It is supported by all IP networks, but it is also the least efficient method for transmitting video.

  IMPORTANT: Using TCP connection with secure communication (RTSP over TLS) has a significant impact on the performance of live video redirection (it doubles the CPU usage).

- **Unicast UDP:** Unicast (one-to-one) communication using UDP protocol. Because UDP is a connectionless protocol, it works better for live video transmission. When the network traffic is busy, UDP is much less likely to cause choppy video than TCP. A network that supports unicast UDP necessarily supports unicast TCP.

- **Multicast:** Multicast is the most efficient transmission method for live video. It allows a video stream to be transmitted once over the network to be received by as many destinations as necessary. The gain could be very significant if there are many destinations. A network supporting multicast necessarily supports unicast UDP and unicast TCP.

  NOTE: Multicast requires specialized routers and switches. Make sure you confirm this with your IT department before setting the capabilities to multicast.

5 Under the **Routes** section, verify that all the routes created by default are valid.

- You may have to change the default capabilities, or force the use of private address when public addresses cannot be used between servers within the same subnet. To edit a route, select it in the list and click **Edit the item** (✏).

- If there is no connection between this network and another network on the system, select the route, and click **Delete** (✖).

- You may want to add a direct route between this network and another child network, bypassing its parent network.

6 Click **Apply**.

Related Topics

Configuring the Media Router role on page 389

Network - Properties tab on page 831

Creating direct connections between networks

You can create a new route between two networks in your system if your network configuration allows it.

What you should know

Security Center creates by default a route between a network and its parent, and between two networks under the same parent.

To add a route between two networks:

1. Open the **Network view** task.
2. Select the network you want to establish the route from, and click the **Properties** tab.
3. Under the **Routes** sections, click **Add an item** (➕).

   The **Route properties** dialog box appears.
4. From the **End point 2** drop-down list, select another network you want to establish the route to.
5. From the **Capabilities** drop-down list, select the smallest set of capabilities.
6. If public addresses cannot be used between these two networks, switch the **Use private address** option to **ON**.
7. Click **OK**, and then click **Apply**.

Customizing network options

You can customize your network card, how your network is selected, and your port range to ensure the best communication to and from your workstation.

What you should know

The network settings apply to the local workstation, and affect Security Desk and Config Tool for all users.

To customize network options:

1. From the home page, click **Options** > **General**.
2. If your computer is equipped with more than one network card, select the one used to communicate with Security Center applications from the **Network card** drop-down list.
3. Choose how to select the **Network**:
   - **Auto-detect:** Security Center automatically detects the network your workstation is connected to.
   - **Specific:** Manually select the network you are on from the drop-down list. This option is helpful if you have trouble getting video feeds.
4. In the **Incoming UDP port range** option, select the port range used for transmitting video to your workstation using *multicast* or unicast *UDP*.
5. Click **Save**.

Example

Let’s consider the following use case. You have a network 10.1.x.x that has a route to 10.2.x.x. But for some reason, a specific workstation at address 10.1.2.3 cannot access 10.2.x.x. Specifying a network manually on that workstation allows the Media Router to know that it has to redirect the media from 10.2.x.x for that workstation instead of making it try to connect directly to 10.2.x.x and fail.

8

High availability

This section includes the following topics:

About the high availability features in Security Center

High availability is a design approach that enables a system to perform at a higher than normal operational level. This often involves failover and load balancing.

To ensure that there is uninterrupted access and data protection for your system, Security Center offers the following high availability features:

- **Directory failover:** Ensure that the Directory role remains available when its primary server fails. The Directory role handles failover for all other roles, so it is important that the Directory role remains available at all times.
- **Directory load balancing:** Additional benefit of Directory failover. Up to 5 servers can be assigned to the Directory role to share its workload. All servers that are set up for Directory failover are automatically used for load balancing.
- **Database failover (only for Directory role):** Protect the Directory database, using one of the following methods:
    - **Backup and restore:** Regularly backup your database, and restore it if a failover occurs.
    - **Microsoft SQL Server Database Mirroring:** The database instances are kept in synch by Microsoft SQL Server.
- **Archiver failover:** Ensure that the Archiver role and video archiving capability remains available when the Archiver's primary server fails.
- **Other role failover:** Ensure that other roles in your system remain available when their primary server fails. If the role database must be protected, you should consider one of the following third party solutions: *SQL Server Clustering* or *Database Mirroring*.
- **NEC ExpressCluster X LAN:** Third party solution for roles that do not support failover. For more information, see *Security Center Installation Guide for NEC Cluster*. Click here for the most recent version of this document.
- **Windows 2008 Server failover cluster:** Third party solution for roles that do not support failover. For more information, see *Security Center Installation Guide for Windows Cluster*. Click here for the most recent version of this document.

Other ways you can ensure high availability are to detect problems early, and prevent those problems from reoccurring.

Related Topics

About Heath monitoring on page 239

Role failover

Role failover is a backup operational mode where a role is transferred from its primary server to a standby server if the primary server becomes unavailable, either through failure or scheduled down time. Role failover is managed by the Directory role.

How role failover works in Security Center

For failover to work in Security Center, you need to define the following two types of servers:

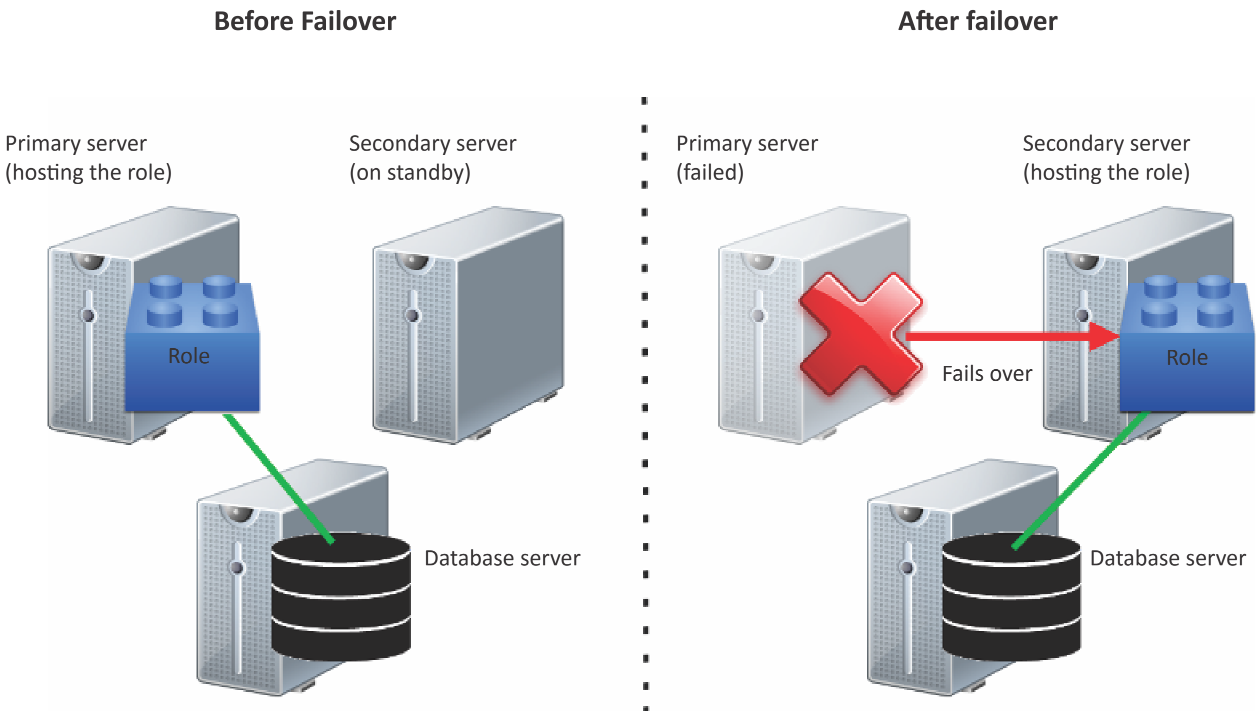
- **Primary server:** Server that normally hosts a role for it to work on the system.
- **Secondary server:** Standby servers that are assigned to a role to keep it running in case the primary server becomes unavailable.

There is no limit to the number of secondary servers you can assign to most roles. However, the more servers you add, the less cost-effective it might be for you.

The secondary server for one role can be the primary server for another role, provided that both servers have enough resources (CPU, memory, disk space, and network bandwidth) to handle the combined load of both roles in case of a failover.

IMPORTANT: Security Center does not handle database failover, except for the Directory role. Besides performing regular backups of your database, one solution you might consider to protect your data is to use *SQL Server Clustering* or *Database Mirroring*.

Before failover, a role is hosted on the *primary server* and connects to a *database server* hosted on a third computer. When the *primary server* fails, the role automatically fails over to the *secondary server* and reconnects to the **same** *database server*.



Roles supporting failover

Some roles in Security Center do not support failover, and others only support failover under certain conditions.

The following table lists which Security Center roles support failover, the failover approach they use, and any special conditions they might have.

Role	Supports failover	Exceptions
Access Manager	No	
Active Directory	Yes	
Archiver	Yes	Can have a secondary and tertiary standby server. Each server requires a separate database, hosted locally or on another computer.
Auxiliary Archiver	No. It ensures that video archives are still available if the main Archiver fails.	
Directory	Yes	Can run simultaneously on up to five servers. Also supports Directory database failover.
Directory Manager	No. It manages the Directory failover and load balancing.	
Global cardholder synchronizer	Yes	
Health Monitor	Yes	
Intrusion Manager	Yes	Only when the *intrusion panels* are connected using IP. Failover is not supported if the intrusion panels are connected using serial ports.
LPR Manager	Yes	Extra resources must be shared between the primary and secondary servers. The Root folder of the role must point to a UNC location that all servers have access to. File paths of hotlist and permit entities must be entered as a UNC location accessible to all servers. Also, the *WatermarkEncryptionParameters.xml* file located in the installation folder of the primary server must be copied to the secondary servers.
Map Manager	Yes	**BEST PRACTICE:** It is best to set the map cache to a location that can be reached by all servers assigned to the role.
Media Router	Yes	The primary and secondary servers can each have a separate database, hosted locally, or on another computer.

Role	Supports failover	Exceptions
Omnicast™ Federation™	Yes	
Plugin	Yes	
Point of sale	Yes	
Report Manager	Yes	
Security Center Federation™	Yes	
Web-based SDK	Yes	
Zone Manager	Yes	

Setting up role failover

To configure failover for roles on your system, you must select secondary servers to be on standby in case the primary server hosting the role becomes unavailable.

Before you begin

For roles that require a database (except for the Archiver), the database must be hosted on a different computer than the primary and secondary servers, and all the servers must be able to communicate with the database server.

What you should know

To set up failover for an Archiver role, see Archiver failover on page 160.

To set up role failover:

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

2 Select the role you want to configure failover for, and then click the **Resources** tab where the role's primary server is listed

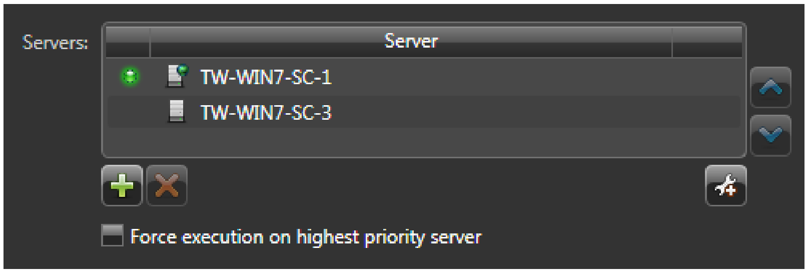
3 Under the **Servers** list, click **Add an item** (+).

A dialog box listing all remaining servers on your system not assigned to the role appears.

4 Select the server you want to add as a secondary server and click **Add**.

The secondary server is added below the primary server. The green LED indicates which server is currently hosting the role.

IMPORTANT: The order in which the servers appear in the list corresponds to the order they are picked if a failover occurs. When the primary server fails, the role automatically switches to the next server in the list.



5 After a failover occurs, if you want the primary server to take control of the role once it is restored, select the **Force execution on highest priority server** option.

NOTE: By default, the role remains on the secondary server after a failover occurs to minimize system disruptions.

6 Click **Apply**.

Changing the server priority for role failover

You can make secondary servers into primary servers, or ensure that a primary server takes back control of a role once the server is restored after a failover occurs.

What you should know

By default, the role remains on the secondary server after a failover occurs to minimize system disruptions. You can change the server priority, so that the original server can take control of the role again.

To change the server priority for failover:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the role and then click the **Resources** tab where the role's primary server is listed.
3. Select a server from the list, and click the ⌄ or ⌃ buttons to move it to the top or bottom of the list.
4. Select the **Force execution on highest priority server** option and click **Apply**.

   After a few seconds, the green LED moves to the new server, indicating that it is now the one hosting the role.

   IMPORTANT: Servers are displayed in the order they are picked if a failover occurs. When the primary server fails, the role automatically switches to the next server in the list.

Directory failover and load balancing

Since the Directory is the main role that manages all entity configuration in your system, you must ensure that the Directory service is always available, and does not become overloaded.

The Directory service is available as long as its two components are available:

- **Directory role:** Manages your system configuration, and handles failover for all other roles.
- **Directory database:** Stores your system configuration.

The *Directory Manager* role handles Directory *failover* and *load balancing* for your system. It manages failover for the Directory role and Directory database independently, allowing you to have separate lists of *servers* assigned to host the two components. These two lists of servers can overlap or be completely separate.

NOTE: There can only be one Directory Manager role in your system. It is created automatically when your software license supports multiple Directory servers.

Differences between Directory servers and the main server

To configure Directory failover and load balancing, you must know the difference between Directory servers and the main server.

- **Directory server:** Servers assigned to host the Directory role. The Directory role can run on five Directory servers simultaneously for *load balancing*. They distribute the workload for credential authentication, software license enforcement, Directory database report queries, and so on.

  Users can log on to Security Center through any of the Directory servers. By default, the Directory Manager redirects the connection requests across all Directory servers in a round robin fashion, but you can bypass load balancing on specific workstations as necessary.

- **Main server:** The primary Directory server in your system (). It has full read/write access to the Directory database. If your system is configured for Directory failover and load balancing, the additional Directory servers () only have read access to the database.

When a Directory server fails, only the client applications connected to Security Center through that server must reconnect. If the main server fails, then *all* clients on the system must reconnect, and the responsibility of being the *main server* is passed down to the next Directory server in the failover list.

Preparing Directory failover and load balancing

Before you can configure the Directory for failover and load balancing, there are some pre-configuration steps required.

Before setting up Directory failover and load balancing:

1 Make sure your Security Center license supports multiple *Directory servers*.

   NOTE: The *Directory Manager* () role is created automatically in Config Tool when your license supports multiple Directory servers.

   a) From the home page, click **About** > **Security Center**.
   b) In the **Number of additional Directory servers** option, note the number of supported servers.
      If you need to update your license, see the *Security Center Installation and Upgrade Guide*.

2 Have your *System ID* and *Password* on hand, found in the *Security Center License Information* document.

   Genetec™ Technical Assistance sends you this document when you purchase the product.

3 Make sure that all the *servers* you plan to use as Directory servers are up and running as expansion servers.

   For more information about installing expansion servers, see the *Security Center Installation and Upgrade Guide*.

4 For all the expansion servers you plan to use as Directory servers, make sure their general properties configured in Server Admin are the same as those of the main server.

   This ensures that your data, such as the alarm retention period and so on, is stored for the same amount of time.

5 Host the Directory database on a remote computer from the Directory servers.

6 Make sure the database server is accessible from all Directory servers.

Related Topics

Server Admin - Main server page on page 86

Setting up Directory failover and load balancing

To protect your information in case the main server fails, you can set up Directory failover and load balancing by assigning expansion servers as Directory servers.

Before you begin

Prepare for Directory failover and load balancing.

What you should know

- You can convert up to five expansion servers as *Directory servers* to be used for load balancing and failover. The order of appearance of the servers in the list corresponds to the order they are picked if a failover occurs. If the main server fails, the role switches to the next server in the list, and that server becomes the main server.

  IMPORTANT: Do not try to add a server to the Directory failover list by activating the Directory on that expansion server with Server Admin. This action disconnects the server from your current system and transforms it into the *main server* of a new system.
- If you want to exclude a Directory server from load balancing because either the server or the connection between the client and the server is slow, you can enable the **Disaster recovery** option. This removes the server from participating in load balancing, but the server will still be available to take over as the main server in the event of a Directory failover.

To set up Directory failover and load balancing:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the **Directory Manager** ( ) role, and click the **Directory servers** tab.
3. Click **Add an item** ( ).
4. In the dialog box that appears, select the server you want to add, its connection port (default=5500), and click **Add**.

   The server is added to the failover list.
5. Add more Directory servers if necessary.
6. Update your license to include the servers you've just promoted to Directory servers.
7. Click **Apply**.

The expansion servers are converted into Directory servers and the updated license is applied to all Directory servers in the list. Client applications and roles on expansion servers can connect to Security Center using any of the Directory servers.

Related Topics
Setting up a Directory server for disaster recovery on page 145

Forcing a Directory server to always be the main server

If one of the *Directory servers* is your preferred choice to be the *main server*, you can force it to always be the main server whenever it is available.

What you should know

The first server in the Directory servers list is your *default* main server. When a Directory failover occurs, the next server in line becomes the new main server ( ). When the first server is back online after a failover, the default behavior is to keep the current server as the main server and not switch back to the first server. This behavior minimizes system disruptions caused by applications having to disconnect and reconnect to the main server. If this is not the behavior you want for your system, you can change it in the **Directory servers** tab.

To change the priority of the servers in the Directory failover list:

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

2 Select the **Directory Manager** ( ) role, and click the **Directory servers** tab.

3 Select a server in the list, and click **Up** ( ) or **Down** ( ) to move the Directory servers up or down in the list.

4 To force the first server in the failover list to be the main server whenever it is available, select **Force the first server in the list to be the main server** option.

5 Click **Apply**.

Setting up a Directory server for disaster recovery

Configuring a Directory server to be a *disaster recovery* server excludes the server from load balancing. A disaster recovery server only activates if it takes over as the main server during a Directory failover.

Before you begin

Set up Directory failover and load balancing.

What you should know

- If the Directory failover server is located remotely or has a slow connection, you can enable the disaster recovery option so that the server does not slow down the system by participating in load balancing.
- A disaster recovery server does not accept client connections unless it becomes the main server during a Directory failover.
- Roles such as the Media Router, Health Monitor, and Report Manager are often associated with the Directory servers. If you are enabling disaster recovery, you must enable the option *force execution on highest priority server* for all roles that are hosted on the server, to ensure that the roles do not start on the disaster recovery server. For more information, see "Role failover on page 137".

To set up a disaster recovery server:

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

2 Select the **Directory Manager** ( ) role, and click the **Directory servers** tab.

3 At the bottom of the server list, click **Advanced** ( ).

An extra column, **Disaster recovery**, is displayed in the list.

4 Select **Disaster recovery** for one or more Directory servers.

NOTE: The **Disaster recovery** option only applies to Directory servers, not to Gateways.

5 Click **Apply**.

The server is excluded from load balancing and only accepts client connections if it becomes the main server during a Directory failover.

Related Topics

Setting up Directory failover and load balancing on page 144

Switching the main server

If necessary, you can assign any server in the Directory failover list to be the main server. For example, when maintenance work needs to be done on the current main server.

To switch the main server:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the **Directory Manager** (🌐) role, and click the **Directory servers** tab.
3. Select a server, and click **Activate Directory** (●).
4. Click **Continue**.

All client applications and roles are disconnected, the main server switches to the Directory server you selected, and all applications and roles reconnect.

Reactivating the Security Center license for Failover Directory systems

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

Before you begin

To update your license, you need the following:

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

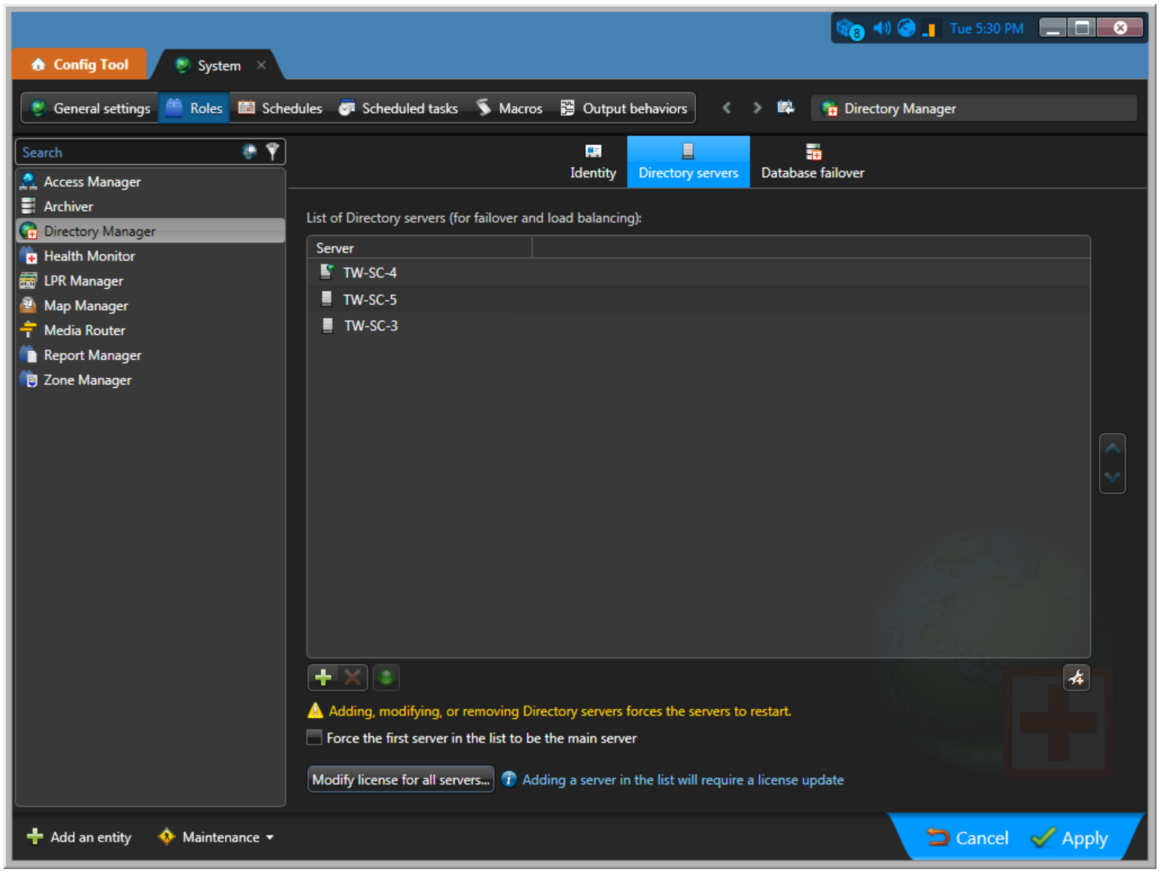
What you should know

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

To activate the Security Center license for a multiple Directory server system:

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

2 Select the **Directory Manager** () role, and click the **Directory servers** tab.



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

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

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

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

Adding a server in the list will require a license update

3 Click **Modify license for all servers**.

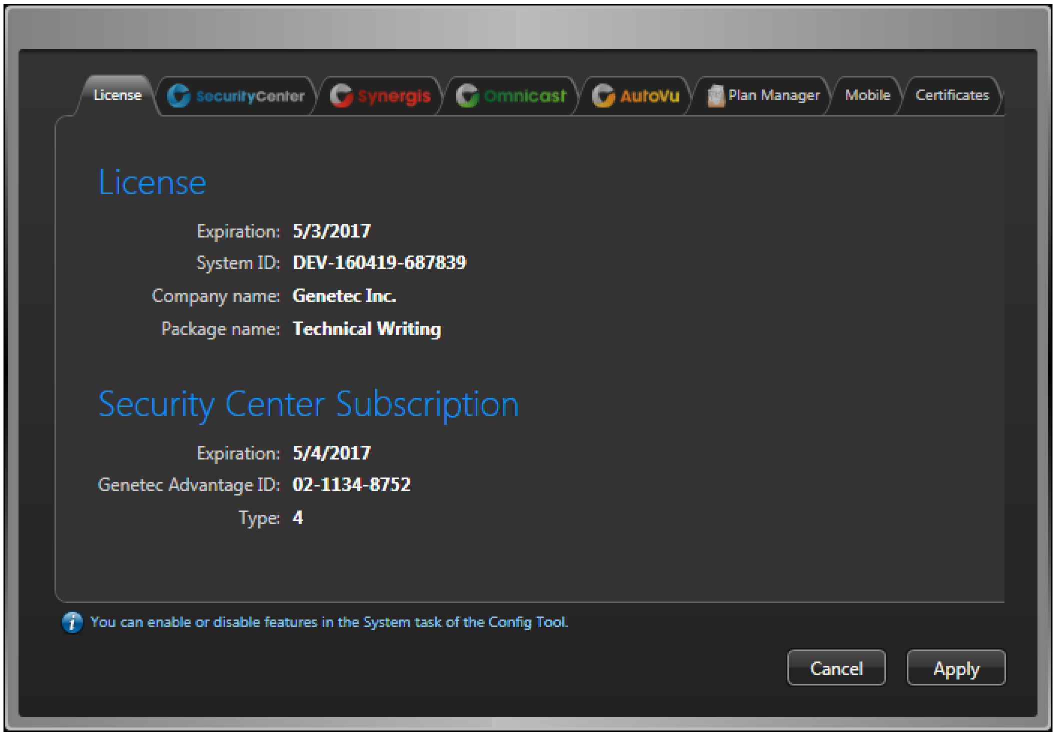
4 In the **License management** dialog box, activate your license in one of the following ways:

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

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

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

A dialog box showing your license information opens.



License

Expiration: 5/3/2017
System ID: DEV-160419-687839
Company name: Genetec Inc.
Package name: Technical Writing

Security Center Subscription

Expiration: 5/4/2017
Genetec Advantage ID: 02-1134-8752
Type: 4

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

Click the colored tabs to view your license options.

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

Reactivating your Security Center license using a license file

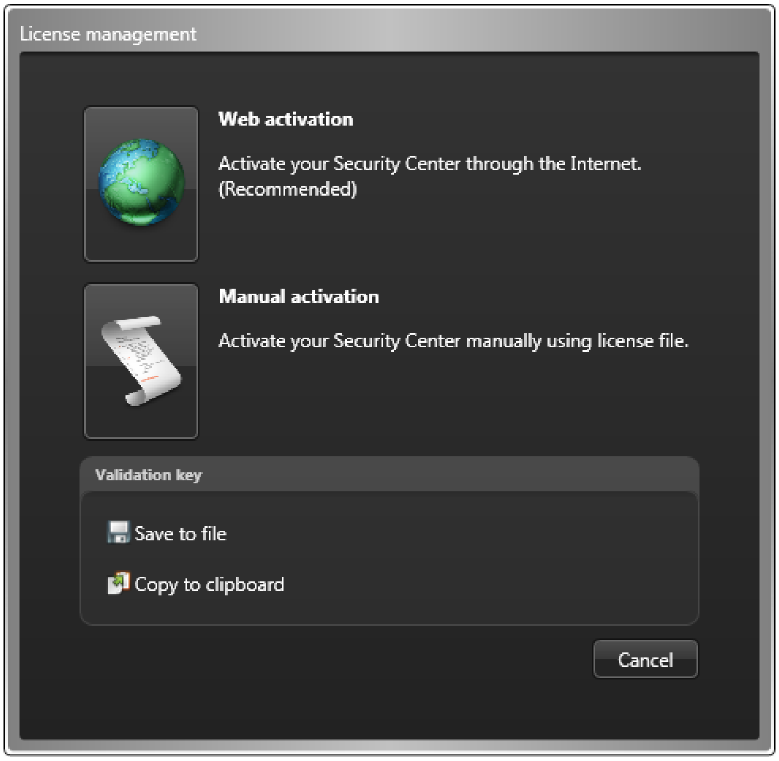
To reactivate your Security Center license for the changes you made to the list of Directory servers while the Config Tool workstation has no Internet access, you must use a second workstation to download your license file from GTAP, and then apply the license file using your first workstation.

What you should know

This procedure fits in the context of reactivating your Security Center license on a Failover Directory system.

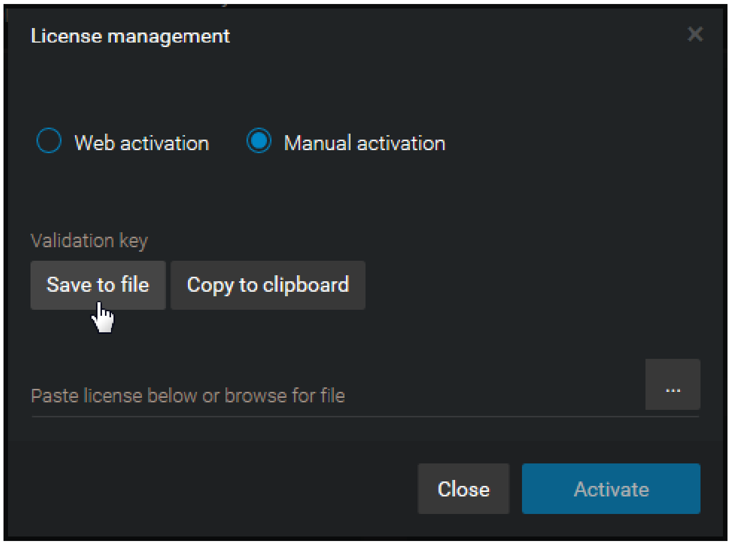
To update your license using a license file:

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


License management
Web activation
Activate your Security Center through the Internet. (Recommended)
Manual activation
Activate your Security Center manually using license file.
Validation key
Save to file
Copy to clipboard
Cancel

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

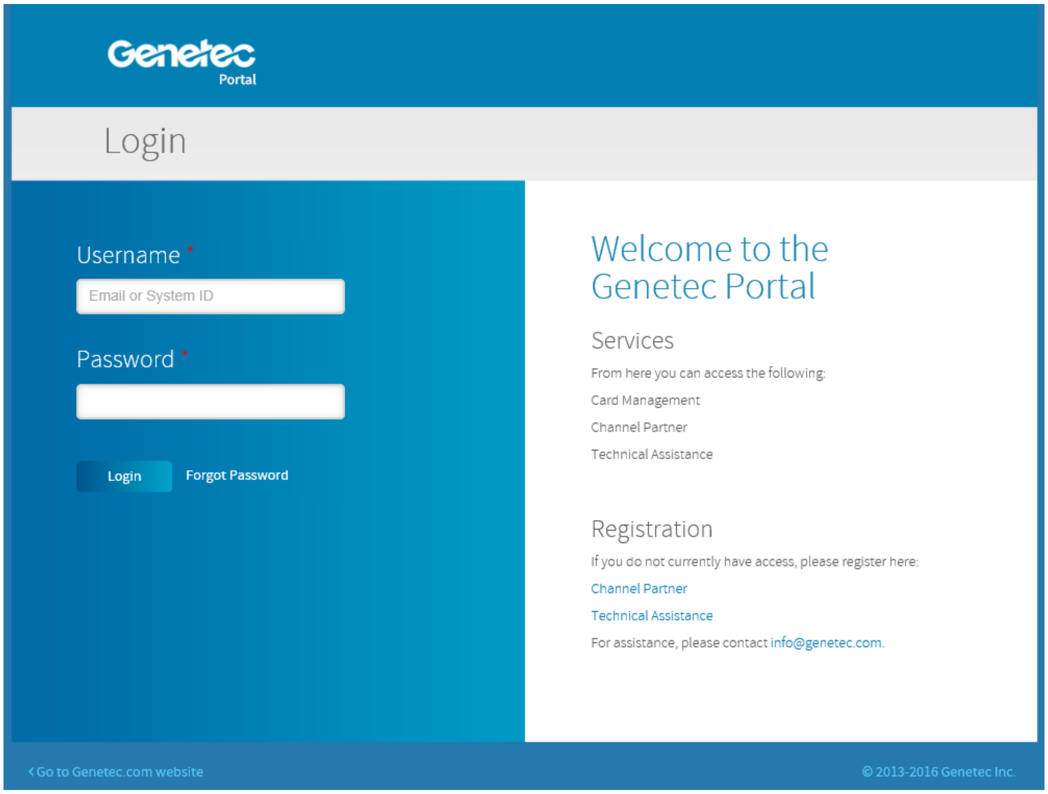
2 In the *License management* dialog box, click **Manual activation**, and then under *Validation key*, click **Save to file**.



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

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

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



Genetec Portal

Login

Username *

Email or System ID

Password *

Login Forgot Password

Welcome to the Genetec Portal

Services

From here you can access the following:

Card Management

Channel Partner

Technical Assistance

Registration

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

Channel Partner

Technical Assistance

For assistance, please contact info@genetec.com.

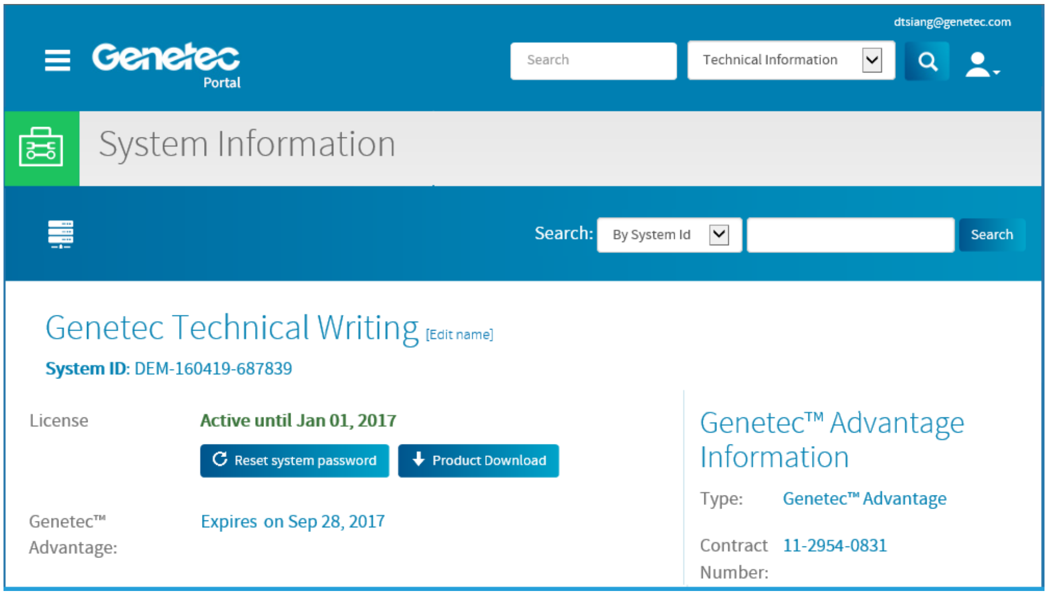
< Go to Genetec.com website

© 2013-2016 Genetec Inc.

4 On the GTAP login page, do one of the following:

- Enter the System ID and the Password specified in the *Security Center License Information* document, and click **Login**.
- Enter your GTAP user account (your email address) and Password, and click **Login**.
  1 On the *Genetec Portal - Home* page, click **Activate new system**.
  2 From the **System ID** drop-down list, select your system, and click **Submit**.

The browser opens to the *System Information* page.



dtsiang@genetec.com

Genetec Portal

Search | Technical Information

System Information

Search: By System Id | Search

Genetec Technical Writing [Edit name]

System ID: DEM-160419-687839

License: Active until Jan 01, 2017

Reset system password | Product Download

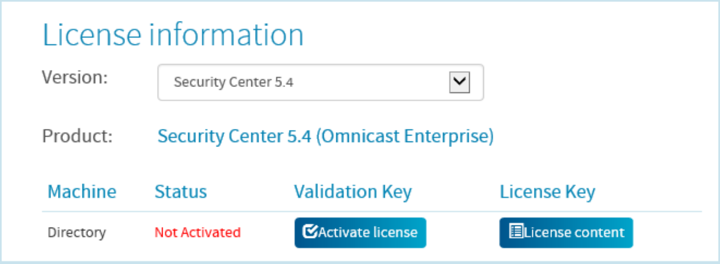
Genetec™ Advantage: Expires on Sep 28, 2017

Genetec™ Advantage Information

Type: Genetec™ Advantage

Contract Number: 11-2954-0831

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



License information

Version: Security Center 5.4

Product: Security Center 5.4 (Omnicast Enterprise)

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

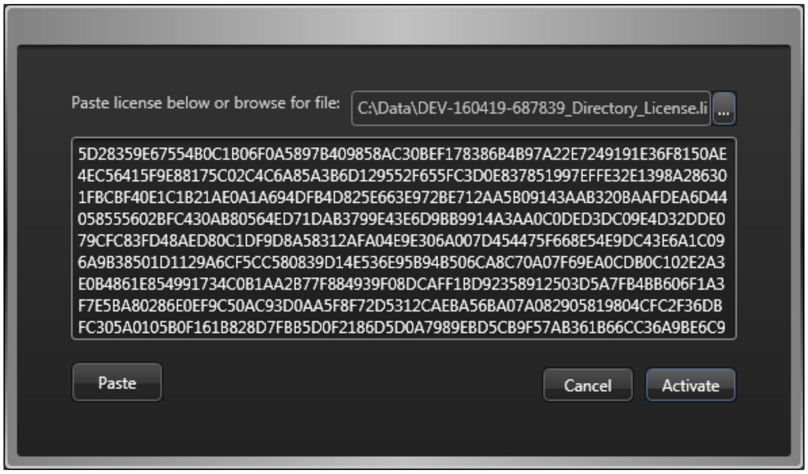
6 In the dialog box that opens, browse to your validation key (.vk file), and click **Submit**.
The message **License activation successful** appears.

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

8 Return to the Config Tool workstation.

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

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



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

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

11 Click **Activate**.

Removing servers from the Directory failover list

If you no longer need a server as a Directory server for Directory failover or load balancing, you can remove it from the Directory failover list.

What you should know

Do not try to remove a server from the Directory failover list by deactivating the Directory on that server from Server Admin. Your change will not be permanent because the Directory Manager will change it back to a Directory server.

To remove a server from the Directory failover list:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the **Directory Manager** (🌐) role, and then click **Directory servers** tab.
3. Select the servers you want to remove, and click **Remove the item** (✖).
4. Update your license to exclude the servers you've just removed.
5. Click **Apply**.

The removed servers become expansion servers, and the updated license is applied to all remaining Directory servers. Users can no longer connect to the system using the servers that have been removed. Clients connected to Security Center through these servers are disconnected, and reconnected to the remaining Directory servers.

Example

You just added a new computer to your system and want to use the server on that computer as a Directory server; however, you are already using five Directory servers. You can remove one of the existing servers from the Directory failover list to make room for the new server.

Bypassing load balancing on workstations

If you have more than one Directory server on your system, but you do not want users to be redirected to another server when they log on to Security Center, you can bypass the load balancing.

What you should know

When you have more than one Directory server on your system, load balancing is automatically in effect. This means that every time a user logs on to Security Center, the Directory Manager redirects their logon request to the next Directory server in the list, based on the server that the previous user connected to.

You can bypass the load balancing behavior on specific workstations (applied to Config Tool and Security Desk), which is helpful when a client is on a remote LAN.

To bypass load balancing on a workstation:

1. From the home page, click **Options** > **General**.
2. Select the **Prevent connection redirection to different Directory servers** option.
3. Click **Save**.

Directory database failover

You can fail over the Directory database using either the backup and restore failover mode or the mirroring failover mode.

Three database failover modes are supported for the Directory:

- **Backup and restore:** The Directory Manager protects the Directory database by regularly backing up the master database instance (source copy). During a failover, the latest backups are restored to the backup database that's next in line. Two schedules can be defined: one for full backups, and another for differential backups.
- **Mirroring:** Database failover is taken care of by Microsoft SQL Server and is transparent to Security Center. The *Principal* and *Mirror* instances of the Directory database are kept in synch at all times. There is no loss of data during failover.
- **SQL AlwaysOn:** Use this failover mode if you are using the Windows feature SQL AlwaysOn as your high availability and disaster recovery solution.

Limitations of the backup and restore failover mode

- To preserve the changes made to your system configuration while you were operating from the backup database, you must restore the latest contingency backup (created in the *ContingencyBackups* subfolder under the restore folder) to your master database before reactivating it.
- To avoid losing the configuration changes made while you were operating from the backup database, you can change the backup database as your master database. To do this, select it from the database failover list to move it to the top of the list. However, keep in mind that your backup database is only as up to date as the most recent backup before the failover took place.

Differences between the backup and restore mode and the mirroring mode

The following table compares the differences between the two database failover modes.

Backup and restore (Directory Manager)	Mirroring (Microsoft SQL Server)
Multiple backup instances of the Directory database are kept relatively in sync with its master instance through regular backups performed by the Directory Manager role.	A single copy (the mirror instance) of the Directory database is kept perfectly in sync with the master copy (or principal instance) using SQL Server database mirroring.
The failover database can only be as up to date as the most recent backup.	The failover database is an exact copy of the principal database.
Changes made while the Directory is connected to the backup database are lost when the Directory switches back to the master database.	Changes can be made to the Directory database at any time without ever losing data.
Both master and backup databases must be hosted on Security Center *servers*.	The principal and mirror database instances can be hosted on any computer.
Can work with SQL Server Express edition which is free.	Requires SQL Server 2008 Standard Edition or better, that supports mirroring.

Backup and restore (Directory Manager)	Mirroring (Microsoft SQL Server)
Recommended when the entity configurations are not frequently updated.	Recommended when entity configurations are frequently updated, such as for cardholder and visitor management.
Causes a temporary disconnection of all client applications and roles while the database failover is in progress.	No client application disconnection during failover.
Database failover is handled by the Directory Manager role.	Database failover is executed by a separate *Witness server* running on SQL Server Express (optional but highly recommended) or it has to be manually detected and executed by the database administrator.

Related Topics

Setting up Directory database failover through backup and restore on page 156
Setting up Directory database failover through mirroring on page 158
Setting up Directory database failover through SQL AlwaysOn on page 159

Setting up Directory database failover through backup and restore

To protect the Directory database by regularly backing up the master database instance, you can set up Directory database failover using the backup and restore method.

Before you begin

- Your Security Center license must support multiple *Directory servers*. If you need to update your license, see the *Security Center Installation and Upgrade Guide*.

  NOTE: The *Directory Manager* () role is created automatically in Config Tool when your license supports multiple Directory servers.

- All database servers must be accessible from all Directory servers. You must configure the remote database server (SQL Server) to accept connection requests from the roles.

- All database instances must be the same version, and an expansion server must be installed on each database server. For more information about installing expansion servers, see the *Security Center Installation and Upgrade Guide*.

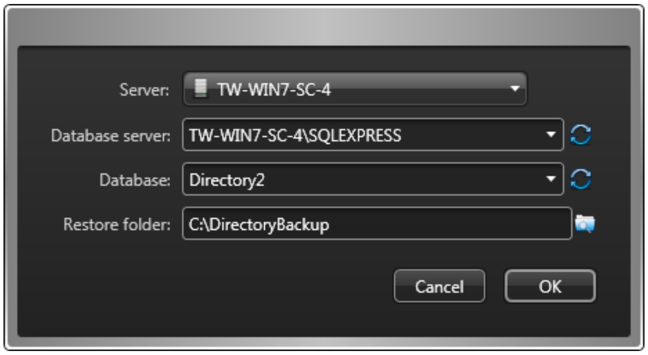
What you should know

Once *Backup and restore* failover mode is enabled, you no longer back up the Directory database from Server Admin, but from Config Tool.

Changes made to the system configuration while you were operating from the backup database are not automatically restored to the master database when it is restored to active service.

To use backup and restore as your Directory database failover solution:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the Directory Manager () role, and click the **Database failover** tab.
3. Switch the **Use database failover** option to **ON**.
4. Select **Backup and restore** for **Failover mode**.
5. Click **Add an item** (➕).
6. In the dialog box that appears, specify the Security Center *server*, the *database server*, the database instance, and the folder where the backup files should be copied.

   Server: TW-WIN7-SC-4

   Database server: TW-WIN7-SC-4\SQLEXPRESS

   Database: Directory2

   Restore folder: C:\DirectoryBackup

   You can assign as many backup databases as you want. However, the more backup databases you have, the longer it takes to back up the Directory database content.

7. Click **OK**.

   The new backup database instance is added.

NOTE: The server flagged as **(Master)** is the one currently hosting the database. The green LED (●) indicates the database that is currently active (not necessarily the *master*).

8 To force all Directory servers to reconnect to the master database once it is back online after a failover, select the **Automatically reconnect to master database** option.

CAUTION: Switching the active database causes a short service disruption, and all changes made to the system configuration while the master database was offline are lost. Use this option only if you are ready to lose the changes made to the system configuration while you were operating from the backup database.

9 Under **Master backup**, specify the frequency at which the *full backup* and the *differential backup* should be generated.

A differential backup only contains the database transactions made since the previous backup, so it is much faster to generate than a full backup. Frequent differential backups ensure that your backup database is most up to date when you fail over, but might take longer to restore.

10 Click **Apply**.

After you finish

CAUTION: Once the *Backup and restore* failover mode is enabled, all subsequent changes to the master database from Server Admin (restoring a previous backup for example) must immediately be followed by a full manual backup executed from Config Tool. Failing to do so causes your master and backup databases to become out of sync and the database failover mechanism to no longer work.

Related Topics
Directory database failover on page 154

Generating full Directory database backup

Once the *Backup and restore* failover mode is enabled, all manual backups of the Directory database must be performed from the Directory Manager's **Database failover** tab in Config Tool.

What you should know

If the *Backup and restore* failover mode is not enabled, back up the Directory database from Server Admin.

To generate a full backup of the Directory database:

1 From the Config Tool home page, open the *System* task, and click the **Roles** view.
2 Select the Directory Manager () role, and click the **Database failover** tab.
3 In the *Master backup* section, click **Generate full backup**.

A full Directory backup is generated in the Security Center backup folder (default=*C:|SecurityCenterBackup|Backups*). All configuration files (*config*, *gconfig*, and *xml* files) are backed up as well.

Setting up Directory database failover through mirroring

To protect the Directory database so you do not lose any data if a failover occurs, you can set up Directory database failover to use Microsoft SQL Server Database Mirroring.

Before you begin

- Microsoft Database Mirroring is being phased out. For new installations, it is recommended to use SQL AlwaysOn.
- The *Principal* database server, the *Mirror* database server, and the *Witness* server (the *Witness* server is optional, but highly recommended) must be configured. For the configuration of SQL Server for mirroring, please refer to Microsoft SQL Server Database Mirroring documentation.
- Your Security Center license must support multiple *Directory servers*. If you need to update your license, see the *Security Center Installation and Upgrade Guide*.

  NOTE: The *Directory Manager* () role is created automatically in Config Tool when your license supports multiple Directory servers.
- The database servers must be running on remote computers from the Directory servers. Move the databases to other computers.
- All database servers must be accessible from all Directory servers. You must configure the remote database server (SQL Server) to accept connection requests from the roles.
- The *Principal* and the *Mirror* databases must be of the same version. For more information on database mirroring, such as how to perform manual backup and restore, refer to the Microsoft SQL Server Database Mirroring documentation.

What you should know

With Database Mirroring, the database failover is handled by Microsoft SQL Server. The *Principal* and *Mirror* instances of the Directory database are kept in sync at all times. There is no loss of data during failover.

NOTE: Following a database failover, the first database query performed by Security Center client applications are likely to fail. When a query fails, the message "Database transaction has failed" appears on screen. Close the message box and try again to resume normal operation.

To use Database Mirroring as your Directory database failover solution:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the Directory Manager () role, and click the **Database failover** tab.
3. Switch the **Use database failover** option to **ON**, and select the **Mirroring** option.

   The database you’re currently connected to is the *Principal* database.
4. Under **Mirror database**, enter the database server name of the *Mirror* database.
5. Click **Apply**.

Related Topics
Directory database failover on page 154

Setting up Directory database failover through SQL AlwaysOn

If you are using the Windows feature *SQL AlwaysOn* as your Directory database failover solution, you must configure the Directory Manager to use SQL AlwaysOn in Config Tool.

Before you begin

All database servers must be accessible from all Directory servers. You must configure the remote database server (SQL Server) to accept connection requests from the roles.

To use SQL AlwaysOn as your Directory database failover solution:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the Directory Manager (🌐) role, and click the **Database failover** tab.
3. Switch the **Use database failover** option to **ON**, and select the **SQL AlwaysOn** option.
4. Click **Apply**.

Related Topics
Directory database failover on page 154

Archiver failover

Adding a standby server to your *Archiver* role minimizes the downtime of your live video if a hardware failure occurs.

How Archiver failover works

If the server hosting the Archiver role fails, you lose access to live video and archived video. Live video is disabled because the Archiver controls the *video units*. Access to archived video is disabled because your archives can only be accessed through the Archiver that created them (even if your *database server* is not the computer that failed).

For Archiver failover, the following conditions apply:

- You can assign a primary server, a secondary server, and a tertiary server to an Archiver role. This is especially useful in multi-site systems, as you can protect the primary and secondary servers at a local site with a tertiary server located at a remote site.
- The primary, secondary, and tertiary servers must each have their own database, hosted locally, or on another computer.
- To make sure that the video archived by the *primary server* is still available if it fails to a secondary or tertiary server, you must turn on redundant archiving. This ensures that all servers can archive video at the same time, and that they each manage their own copy of the video archive. You can set up redundant archiving on all cameras managed by the Archiver role, or protect just a few important cameras

Careful load planning for failover

If failover occurs, the performance of a standby server might be affected by the additional archiving load (number of cameras, video quality, and so on) from the new Archiver role. If the standby server hosts other roles, this also affects archiving capability.

When selecting a server as a standby server for an Archiver role, consider the following:

- If the server has other functions, it might not be able to absorb the full load of another server.

  TIP: To lessen the failover load on a server, create multiple Archiver roles with fewer video units each. Also, configure all the Archivers to share the same primary server, but to fail over to different secondary or tertiary servers.
- How long is a typical failover expected to last? The longer a failover lasts, the more additional disk space you need to reserve for archiving.
- A server can handle more video units when only command and control functionality is needed. If video archiving is not important on all cameras, you can associate all important cameras to one Archiver role and give it a higher *archiving priority* than the rest. That way, if multiple Archiver roles fail over to the same server at the same time, archiving will be maintained for the important cameras.

Limitations of Archiver failover

The failover process can take 15-30 seconds. During that time, video cannot be recorded but viewing live video is not affected. You cannot add a bookmark during the failover process.

If an Achiver role (A) is configured with a secondary and tertiary server, and the secondary server is shared with another Archiver role (B) which has higher archiving priority, then if both main Archiver servers fail at the same time, the secondary server starts archiving for the highest priority Archiver (B). However, this configuration prevents Archiver Role (A) from archiving on the secondary or tertiary servers. As a workaround, if you have a tertiary server configuration for archiver failover, do not assign the same server to multiple Archiver roles.

Related Topics

Creating Auxiliary Archivers on page 385
About video archives on page 432

Setting up Archiver role failover

You can set up the Archiver role to fail over to a secondary server if the primary server fails, and a tertiary server if both the primary and secondary server fail. This enables you to maintain control of video units, access live video, and minimize potential downtime.

Before you begin

A license is required to assign a tertiary server for Archiver role failover. See License options in Security Center on page 936 for more details.

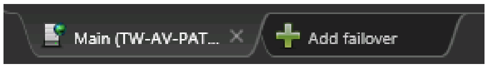
What you should know

The servers assigned to the Archiver must be configured separately, and must have their own database and storage system for the video archive.

To set up Archiver role failover:

1 Open the **Video** task, and select the Archiver role to configure.

2 Click the **Resources** tab, and then click **Add failover** (+).



3 In the dialog box that opens, select a server and click **Add**.

   The server you added for failover becomes the secondary server tab.

4 From the secondary server tab, configure archive database and archive storage settings.

5 (Optional) If the secondary server is also on standby for other Archiver roles, then you might have to adjust the archiving priorities for standby servers.

6 (Optional) Add a tertiary server in the event that both the primary and secondary server fail:

   a) Click the **Add failover** tab.

   b) Select a tertiary server and click **Add**.

      The server you added for failover becomes the tertiary server tab.

   c) From the tertiary server tab, configure archive database and archive storage settings.

   d) (Optional) If the tertiary server is also on standby for other Archiver roles, then you might have to adjust the archiving priorities for standby servers.

7 Click **Apply**.

8 To have the primary and standby servers archive video at the same time, click the **Camera default settings** tab, click **Show advanced settings**, and switch the **Redundant archiving** option to **ON**.

   This ensures that the recorded video is stored in three places, for additional protection.

Related Topics

Archiver failover on page 160
Databases on page 117
About video archives on page 432

Changing the server priority for Archiver failover

You can decide which Archiver is the primary server, which one is the secondary, and which one is the tertiary server for failover.

Before you begin

You must have at least two servers assigned to the Archiver role.

What you should know

CAUTION: To avoid losing video, you should change the server priority for Archiver failover at a time when the Archiver is not archiving.

To change the server priority for Archiver failover:

1 Click **Failover** (⊞) at the bottom of the **Resources** tab.

A dialog box appears, showing the servers assigned to this Archiver role.

2 Select one of the servers in the list and click ▲ or ▼ to move it up or down the list.

3 Click **OK** to close the **Failover** dialog box.

The server tabs switch places.

4 When a standby server hosts other Archiver roles, you might have to adjust the archiving priorities for the standby server.

5 Click **Apply**.

Assigning archiving priorities for standby servers

If all the Archiver roles fail over to the same standby server at the same time, you can assign archiving priorities to the roles to avoid overloading the server.

What you should know

The same server can be designated as the standby server for multiple Archiver roles. If all Archiver roles fail over to the same server at the same time, their combined load might be too much for the server to handle. One way to avoid overloading a server is to assign a lower archiving priority to the roles of lesser importance so they are not competing for computer resources.

NOTE: At any point in time on a given server, only the Archiver roles with the highest archiving priority will be able to archive. The archiving priority only affects archiving. Having a lower archiving priority does not prevent a failed over Archiver role from performing its command and control functions.

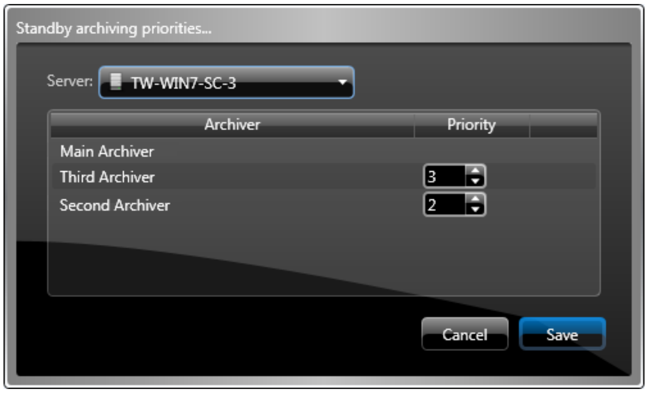
To assign archiving priorities for standby servers:

1 Open the **Video** task, and select the Archiver role to configure.

2 Click the **Resources** tab, and click **Failover** (⊞).

3 In the **Failover** dialog box, click **Standby archiving priorities**.

4 Select a server from the **Server** drop-down list.



Server: TW-WIN7-SC-3

Archiver	Priority
Main Archiver	
Third Archiver	3
Second Archiver	2

All Archiver roles that rely on this server as their primary or *secondary server* are listed. The archiving priority can only be set when the server is used as a standby. For roles that rely on the server as their *primary server*, the archiving priority is implicitly locked at 1 (the highest).

5 Set the priority of the roles, and click **Save**.

NOTE: The archiving priority is specific to each Archiver role on each server. When the archiving priority has never been set, its default value is 1.

6 Repeat these steps to configure all servers hosting Archiver roles on your system.

Troubleshooting failover

If you encounter problems when configuring failover for your system, there are a few things you can check to resolve the issues.

To troubleshoot failover:

1. Make sure the correct ports are open on your network (see Common communication ports on page 941).
2. Make sure your database connections are configured properly, and that the servers being used for failover can communicate with the database server (see Connecting roles to remote database servers on page 119).
3. Make sure the database path is correct in the Server Admin - Main Server page.
4. Make sure the Genetec™ Server and SQL Server services are running under a local Windows administrator user account (see Connecting roles to remote database servers on page 119).
5. (Directory database failover using Backup/Restore method only) Make sure that the user account has access read/write access to the backup folder.
6. (Directory database failover using Backup/Restore method only) Make sure that Security Center Server is installed on the remote database server.

   For more information about installing expansion servers, see the *Security Center Installation and Upgrade Guide*.

9

System automation

This section includes the following topics:

About schedules

A schedule is a type of entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).

Each time constraint is characterized by a date coverage (date pattern or specific dates covered by the schedule) and a time coverage (time periods that apply during a 24-hour day).

When the Security Center Directory is installed, the *Always* schedule is created by default. This schedule has a 24/7 coverage. It cannot be renamed, modified, or deleted, and has the lowest priority in terms of schedule conflict resolution.

Time zones for schedules

The time of day for a schedule is based on the local time zone set in each individual context where it is applied. For example, if the schedule is used to set continuous video recording from 9 a.m. to 5 p.m., whether the *video unit* is in Tokyo or London, the recording occurs on schedule according to the local time. This is because every video unit has a time zone setting to control video settings and recordings relative to the unit's local time.

When a schedule is applied to an entity that has no time zone settings, such as the logon schedule for a user, the local time is taken from the *server* hosting the Directory role.

Schedule conflicts

You might have a scheduling conflict when two overlapping schedules are applied to the same function. For example, if two schedules are applied to the recording of the same *camera*.

Security Center can resolve some of these conflicts by giving priority to the most specific (or restrictive) schedule. The specificity of a schedule is determined by its date coverage option.

The following lists the date coverage options in decreasing order of priority:

1. Specific (Runs only once. Highest priority)
2. Ordinal (Repeats on a monthly or yearly basis)
3. Weekly (Repeats every week)
4. Daily (Repeats every day)
5. Always (The default schedule. Has the lowest priority)

IMPORTANT: When two overlapping schedules with the same priority level are applied to the same function, you have an unresolved conflict. If the two schedule were applied to an entity, an *Entity warning* occurs, and the entity with the conflicting configuration is displayed in yellow in the entity browser.

Related Topics
Customizing time zone settings on page 42

About twilight schedules

A twilight schedule is a type of schedule entity that supports both daytime and nighttime coverages. A twilight schedule cannot be used in all situations. Its primary function is to control video related behaviors.

Benefits of twilight schedules

Twilight schedules are designed for situations where the sunlight has an impact on the system's operation, such as video settings and recording. Some typical uses of the twilight schedules are the following:

- To record video only during daytime.
- To boost the *video encoder*'s sensitivity after sunset.
- To disable *motion detection* during twilight.

Limitations of twilight schedules

Twilight schedules have the following limitations:

- They cannot be used in any situation involving access control entities.
- The entity the schedule applies to must have a geographical location setting, such as video units and *LPR units*.
- The *Weekly* option for date coverage is not available.
- The *All day* and *Range* options for time coverage are not available.
- They are not visible in contexts where they are not applicable.

Related Topics
Setting geographical locations of entities on page 57

Creating schedules

To define a set of time constraints for a multitude of situations, such as when a user can log on to the system or when video from a surveillance camera can be recorded, you can create schedules and then apply them to specific entities.

What you should know

When the Security Center Directory is installed, the *Always* schedule is created by default. This schedule has a 24/7 coverage. It cannot be renamed, modified, or deleted, and has the lowest priority in terms of schedule conflict resolution.

If you want to use schedules for any of your settings in Security Center, you must create the schedules in advance.

To create a schedule:

1. Open the **System** task, and click the **Schedules** view.
2. Click **Schedule** (+), type a name for the schedule, and then press **ENTER**.
3. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply.**
4. Click the **Properties** tab.
5. From the **Date coverage** drop-down list, choose one of the following:
   - **Daily:** Defines a pattern that repeats every day.
   - **Weekly:** Defines a pattern that repeats every week. Each day of the week can have a different time coverage. This option is not available for twilight schedules.
   - **Ordinal:** Defines a series of patterns that repeat on a monthly or yearly basis. Each date pattern can have a different time coverage. For example, on July 1st every year, on the first Sunday of every month, or on the last Friday of October every year.
   - **Specific:** Defines a list of specific dates in the future. Each date can have a different time coverage. This option is ideal for special events that occur only once.

   NOTE: The *Daily*, *Ordinal*, and *Specific* schedules allow you to define twilight settings.
6. Click **Apply**.

Defining daily schedules

To define a set of time constraints for situations that occur daily, you can define daily schedules and then apply them to entities.

What you should know

Time ranges are shown as colored blocks on a time grid. Each block represents either 15 minutes or one minute, depending on the selected time resolution.

To define a daily schedule:

1. Open the **System** task, and click the **Schedules** view.
2. Click **Schedule** (+), type a name for the schedule, and then press **ENTER**.
3. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply.**
4. Click the **Properties** tab.
5. From the **Date coverage** drop-down list, select **Daily**.
6. From the **Time coverage** drop-down list, select **All day** or **Range**.
7. Using the time grid, set the time coverage as follows:

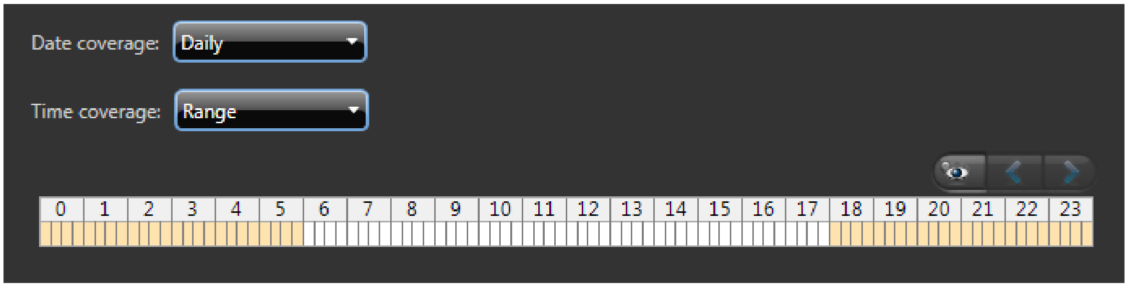
- To select blocks of time, left-click your mouse.
- To remove blocks of time, right-click your mouse.
- To select or remove a successive block of time, click and drag your mouse.

NOTE: To zoom in and out on the time grid, click **Toggle to high time resolution** (👁).

8 Click **Apply**.

Example

The following example shows a daily schedule from 6 p.m. to 6 a.m. The time grid shows a 24-hour day in blocks of 15 minutes.



Date coverage: Daily

Time coverage: Range

Defining weekly schedules

To define a set of time constraints for situations that occur weekly, you can define weekly schedules and then apply them to entities.

What you should know

Time ranges are shown as colored blocks on a time grid. Each block represents either 15 minutes or one minute, depending on the selected time resolution.

To define a weekly schedule:

1 Open the **System** task, and click the **Schedules** view.

2 Click **Schedule** (✚), type a name for the schedule, and then press **ENTER**.

3 In the **Identity** tab, enter basic properties of the schedule, and then click **Apply.**

4 Click the **Properties** tab.

5 From the **Date coverage** drop-down list, select **Weekly**.

6 Using the time grid, set the time coverage as follows:

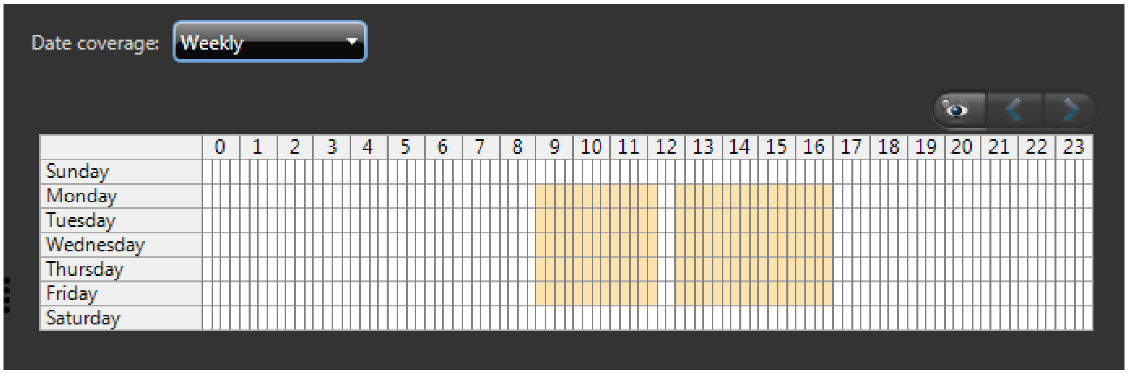
- To select blocks of time, left-click your mouse.
- To remove blocks of time, right-click your mouse.
- To select or remove a successive block of time, click and drag your mouse.

NOTE: To zoom in and out on the time grid, click **Toggle to high time resolution** (👁).

7 Click **Apply**.

Example

The following example shows a weekly schedule from 9 a.m. to 5 p.m., from Monday to Friday, with a half-hour break between 12:15 p.m. and 12:45 p.m.



Date coverage: Weekly

Defining ordinal schedules

To define a set of time constraints for situations that include a series of repetitive patterns, each with a different time coverage, you can define ordinal schedules and then apply them to entities.

What you should know

Ordinal schedules are ideal for events that repeat. You can define as many dates as necessary within a single schedule entity.

To define an ordinal schedule:

1 Open the **System** task, and click the **Schedules** view.

2 Click **Schedule** (+), type a name for the schedule, and then press **ENTER**.

3 In the **Identity** tab, enter basic properties of the schedule, and then click **Apply.**

4 Click the **Properties** tab.

5 From the **Date coverage** drop-down list, select **Ordinal**, and then click **Add an item** (+).

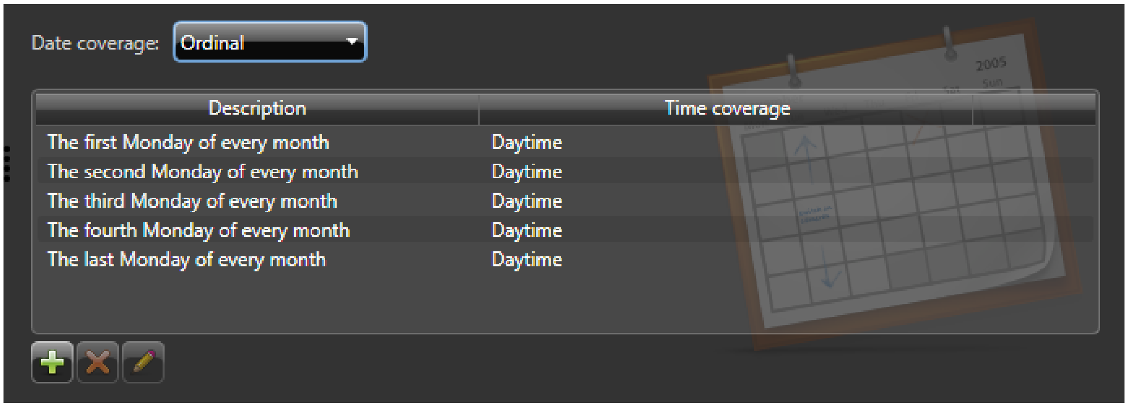
6 Select a day and a month.

7 From the **Time coverage** drop-down list, select **All day**, **Range, Daytime**, or **Nighttime** (see Defining twilight schedules for information on daytime and nighttime time coverages).

8 Click **OK** and then click **Apply**.

Example

You can configure something similar to the *Weekly* pattern using the *Ordinal* pattern. The following example shows a schedule that cover the daytime of every Monday of the year.



Date coverage: Ordinal

Description	Time coverage
The first Monday of every month	Daytime
The second Monday of every month	Daytime
The third Monday of every month	Daytime
The fourth Monday of every month	Daytime
The last Monday of every month	Daytime

Defining schedules with specific dates

To define a set of time constraints for situations that will occur on specific dates, where each date can have a different time coverage, you can define schedules with specific dates and then apply them to entities.

What you should know

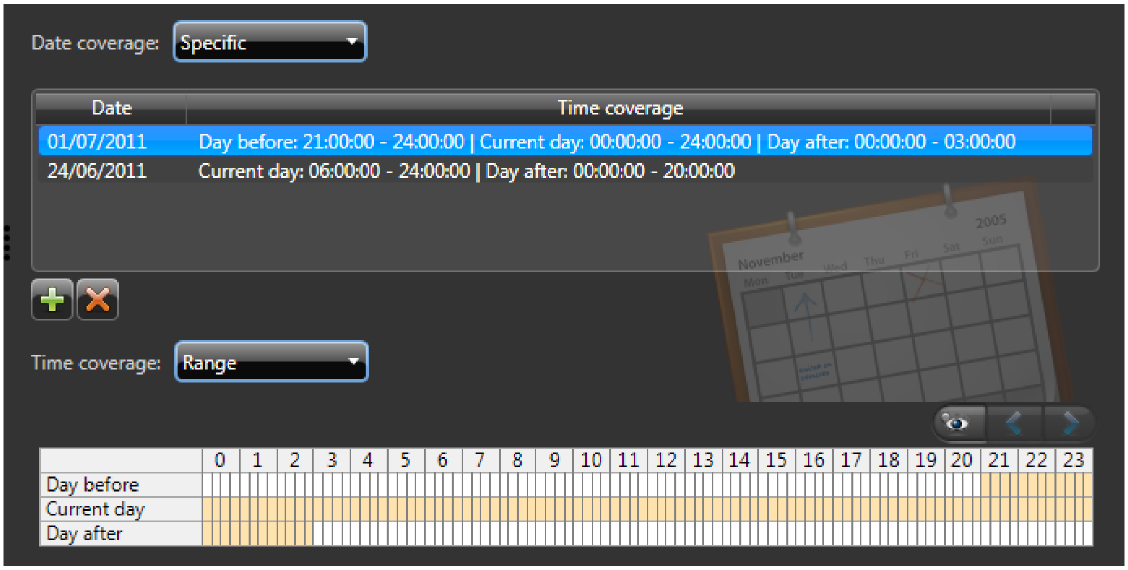
You can set a different time range for each date in the schedule.

To define a schedule with specific dates:

1. Open the **System** task, and click the **Schedules** view.
2. Click **Schedule** (+), type a name for the schedule, and then press **ENTER**.
3. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply.**
4. Click the **Properties** tab.
5. From the **Date coverage** drop-down list, select **Specific**, and then click **Add an item** (+).
6. Select dates on the calendar and click **Close**.
7. Select an entry and, from the **Time coverage** drop-down list, do one of the following:
   - Select **All day**.
   - Select **Range** and then select specific times on the grid for the *Day before*, the *Current day*, or the *Day after*.
   - Select **Daytime** or **Nighttime** (see Defining twilight schedules for information on daytime and nighttime time coverages).
8. Click **Apply**.

Example

The following example shows a specific schedule covering July 1st 2011 from 9 p.m. the day before to 3 a.m. the day after.



Date coverage: Specific

Date	Time coverage
01/07/2011	Day before: 21:00:00 - 24:00:00 | Current day: 00:00:00 - 24:00:00 | Day after: 00:00:00 - 03:00:00
24/06/2011	Current day: 06:00:00 - 24:00:00 | Day after: 00:00:00 - 20:00:00

Time coverage: Range

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Day before																						▨	▨	▨
Current day	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Day after	▨	▨	▨																					

Defining twilight schedules

To define a set of time constraints for situations that cover either daytime or nighttime, where the calculation of exactly when the sun rises and sets is based on a geographical location (latitude and longitude), you can define twilight schedules.

What you should know

Twilight schedules are designed for situations where the sunlight has an impact on the system's operation, such as with video settings and video recording.

To define a twilight schedule:

1 Open the **System** task, and click the **Schedules** view.

2 Click **Schedule** (+), type a name for the schedule, and then press **ENTER**.

3 In the **Identity** tab, enter basic properties of the schedule, and then click **Apply.**

4 Click the **Properties** tab.

5 From the **Date coverage** drop-down list, select **Daily**, **Specific**, or **Ordinal**.

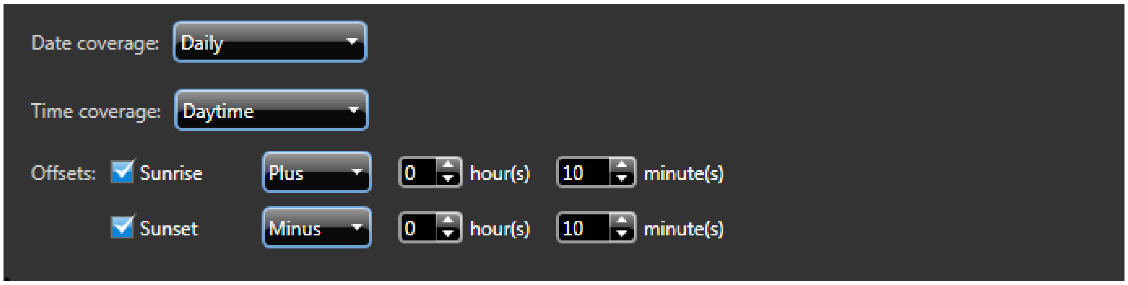
6 If you selected **Specific** or **Ordinal**, set up the date coverage (see Defining ordinal schedules or Defining schedules with specific dates)

7 From the **Time coverage** drop-down list, select **Daytime** or **Nighttime**.

8 Select the **Sunrise** or **Sunset** options, and then select the amount of time to offset the sunrise time or sunset time (up to 3 hours before or after).

Example

The following example shows a daily schedule using a *Daytime* coverage. The time coverage starts 10 minutes after the sun rises and ends 10 minutes before the sun sets.



Date coverage: Daily

Time coverage: Daytime

Offsets: ☑ Sunrise Plus 0 hour(s) 10 minute(s)

☑ Sunset Minus 0 hour(s) 10 minute(s)

About events

An event indicates the occurrence of an activity or incident, such as access denied to a cardholder or motion detected on a camera. Events are automatically logged in Security Center, and can be programmed to trigger actions. Every event mainly focuses on one entity, called the event source.

Events can arise from many sources, such as recording started by a user on a camera, a door being left open for too long, or an attempt to use a stolen credential. The types of events generated by Security Center vary depending on the entity. For example, *Access denied* events relate to *cardholders*, *Signal lost* events relate to cameras, *License plate hit* events relate to *hotlists*, and so on.

Some of the ways you can make use of *system events* are the following:

- View them in *Security Desk* in real-time.
- Have the system record them in event logs for viewing and analysis at a later time.
- Configure the system to take action automatically by associating *actions* to various types of events, such as triggering an *alarm*, or sending a message. This is called an *event-to-action*. This is the most powerful method for handling events.

Custom events

In addition to the predefined event types, you can also define custom events to represent each of the various combinations of input signals received from different units on your system.

Related Topics

Event types on page 908
Creating event-to-actions on page 177
Creating custom events on page 176

Assigning colors to events

For users to quickly assess and respond to events when they are received in Security Desk, you can assign different colors to Security Center events.

What you should know

Event colors are used as visual cues in the Security Desk. When a *system event* is generated, the event color is indicated in the event list and in the canvas tile.

If you have a large system, this helps you focus on events that are more important. For example, you can use red to indicate a critical event (someone attempted to use a stolen credential), and blue to indicate a less critical event (*Access granted*).

To assign a color to an event:

1. Open the **System** task, click the **General settings** view, and click the **Events** page.
2. Next to an event in the **Event colors** tab, select a color from the **Color** drop-down list.
3. Click **Apply**.

Creating custom events

You can create your own custom Security Center events that you can use for event-to-actions.

What you should know

Custom events allow you to give descriptive names to standard events generated by input signals from zones, intrusion panels, and so on. They are used to configure custom event-to-actions.

For example, you can associate an input state (normal, active, trouble) of a zone entity to a custom event that describes what is happening, such as *Illegal entry* or *Door open too long for this zone*. When this custom event is received in Security Desk, it can trigger an action, using event-to-actions.

To create a custom event:

1. Open the **System** task, click the **General settings** view, and click the **Events** page.
2. Click **Add an item** (✚).
3. In the **Create custom event** dialog box, type a **Name** for the new event.
4. From the **Entity type** drop-down list, select the entity type that triggers this event.
5. In the **Value** field, type a unique number to identify the custom event from other custom events.

   These values are not related to the logical IDs of entities.
6. Click **Save** > **Close**.

Creating event-to-actions

If you want certain events that occur in your system to automatically trigger an action, such as sounding an alarm or recording a camera, you can create event-to-actions.

What you should know

An event-to-action links an *action* to a particular *event*. For example, you can configure Security Center to trigger an alarm when a door is forced open.

To create an event-to-action:

1. Open the **System** task, and click **General settings** view.
2. Click the **Actions** page, and click **Add an item** (➕).
3. From the **When** drop-down list in the **Event-to-action** dialog box, select an event type.

   (Optional) If you select **License plate read**, you can specify a condition.
4. In the **From** option, click **Any entity**, and then select an entity that triggers the event.

   By default, the event-to-action occurs when any entity triggers the event type you select. If you select a specific entity, then you might have to set other parameters (for example, if you select a door, then you must also select a door side).
5. From the **Action** drop-down list, select an action type and configure its parameters.

   For example, if you select the *Send an email* action, then you must also select the email recipients.
6. In the **Effective** option, click **Always**, and select a schedule when this event-to-action is active.

   If the event occurs outside of the defined schedule, then the action is not triggered. For example, you might want to sound an alarm only when a window is opened during the weekend. By default, **Always** is selected.
7. Click **Save**.

   The **Save** button is only available when all the arguments required by the event-to-action type are specified.

The new event-to-action is added to the list of system actions.

Related Topics
Event types on page 908
Action types on page 924

Adding conditions when creating event-to-actions for license plate reads

When creating event-to-actions for license plate reads, you can specify additional conditions based on Sharp analytics to trigger an action. For example, you can specify that an action occur only when the plate number contains “123”, or the vehicle is traveling at a certain speed.

Before you begin

- Enable and configure analytics for your Sharps. For more information, see the *Sharp Administrator Guide*, and the *Patroller Administrator Guide*.

What you should know

- Conditions must be typed as an expression that contains an identifier, operator, and a value (not case sensitive). For example, **[PlateNumber] = "ABC123"**. To know more about the operators and identifiers that can be used, see Elements used in event-to-action conditions for license plate reads on page 180.
- Identifiers must be typed in square brackets: **[PlateNumber]**.
- Text values must be typed in quotation marks: **"ABC123"**.
- You can use AND and OR to combine multiple expressions. When doing this, it's preferable to use parentheses to force the order of the evaluation. For example, if you type (**[Speed] > 20 AND [Speed.unit] = "mph") OR ([Speed] > 50 AND [Speed.Unit] = "km/h"** the AND operator takes precedence.
- You can use the exclamation point (!) to exclude an expression. For example, if you type **[PlateNumber] contains "123" AND !([PlateState] = "QC")**, any plate reads with a plate number that contains the value "123" and a plate state other than "QC" will trigger an action.
- Sharp analytics are not generated 100% of the time. An event-to-action may not be executed if the Sharp is not able to generate the analytic specified in the condition. For example, if the condition is **[Speed] > 50** and the Sharp cannot produce a value for speed, Security Center will evaluate the condition as being false and the action will not be executed.
- When the outputs of an LPR Processing Unit are used to control building access through event-to-actions in Security Center, rebooting the LPR Processing Unit causes the outputs to activate which could lead to the opening of the access point. This output behavior is not ideal for access control, but is required in order to power the in-vehicle computer on vehicle startup. Create an event-to-action in Security Center that will send a "Normal" state to the outputs following a "Unit Connected" event. The access points will still open, but will close shortly afterward.

To add a condition when creating an event-to-action for a license plate read:

1 Open the **System** task, and click **General settings** view.

2 Click the **Actions** page, and click **Add an item** (✚).

3 From the **When** drop-down list in the **Event-to-action** dialog box, select **License plate read**.

4 Click **Specify a condition**, and type the expression.

TIP: Hover your mouse over the field for examples of valid expressions. The field will appear in red if the expression you enter is invalid.

5 In the **From** drop-down list, select the LPR unit that triggers the event.

6 In the **For** drop-down list, select the desired entity.

7 From the **Action** drop-down list, select an action type and configure its parameters.

For example, if you select *Send an email*, then you must also select the email recipients.

8 In the **Effective** option, click **Always**, and select a schedule when the event-to-action is active.

If the event occurs outside of the defined schedule, then the action is not triggered.

9 Click **Save**.

The **Save** button is only available when all the arguments required by the event-to-action type are specified.

Elements used in event-to-action conditions for license plate reads

If you add a condition when creating an event-to-action for a license plate read, the condition must contain an identifier, an operator, and a value (text or numeric).

Operators

The following table lists operators that can be used and the corresponding value types, as well as descriptions and examples.

Operator	Description	Type of value	Example
>	Greater than the specified value.	Numeric	[Confidence Score] > 80
<	Less than the specified value.	Numeric	[Confidence Score] < 75
=	Equal to the specified value.	Numeric	[Confidence Score] = 80
		Text	[Vehicle Make] = "Toyota"
Contains	Contains the specified value.	Text	[PlateNumber] contains "123"
StartsWith	Starts with the specified value.	Text	[PlateNumber] starts with "X"
EndsWith	Ends with the specified value.	Text	[State Name] ends with "C"
Matches	Respects the regular expression.	Text	[PlateNumber] matches "[02468]$"

Identifiers

The following table lists the common identifiers that can be used and the corresponding value type, as well as descriptions and examples.

Identifier	Description	Type of value	Example
PlateNumber	Plate Number read by the Sharp.	Numeric	[PlateNumber] Contains "123"
State Name	State Name read by the Sharp.	Text	[State Name] = "QC"
Vehicle Type	Certain license plates include character symbols that identify specific vehicle types (for example, taxi, transport, and so on). The Sharp can read these symbols, and display the vehicle type.	Text	[Vehicle Type] = "Taxi"
Relative Motion	The Sharp can detect if the vehicle is getting closer or moving away from the Sharp.	Text	[Relative Motion] = "Closer"

Identifier	Description	Type of value	Example
Context	Type of LPR context for a specific region.	Text	[Context] = "Brazil"
Characters Height	Height in pixels of the context characters.	Numeric	[Characters Height] = 26
Vehicle Make	Sharp cameras can recognize the make of certain vehicles.	Text	[Vehicle Make] = "Toyota"
Confidence Score	The Sharp assigns a numerical value (from 0 to 100) to each license plate read. This value tells you how confident the Sharp is in the accuracy of the read.	Numeric	[Confidence Score] = 80
Speed	Sharp cameras are able to estimate a vehicle’s approximate speed.	Numeric	[Speed] > 50
Speed.Unit	Depending on the Sharp context used, the unit of speed is measured in "km/h" or "mph". For the US context speed is measured in "mph".	Text	[Speed.Unit] = "mph"
Prefix	Leftmost and topmost digits that appear on a United Arab Emirates plate.	Text	[Prefix] = 10

For more information about specifying conditions when creating event-to-actions for license plate reads, see Adding conditions when creating event-to-actions for license plate reads on page 178

Modifying event-to-actions

If you need to modify an event-to-action, but you have a long list of them in Security Center, you can search for them using a combination of source entity (name and type), event type, and action type.

To modify an event-to-action:

1 Open the **System** task, and click **General settings** view.

2 Click the **Actions** page, and **Advanced search** (⊕) to show the search filters, and filter out the event-to-actions as follows:

- **Entity name:** Search for source entity names starting with the search string.
- **Entity type:** Select a specific source entity type (default=All).
- **Event:** Select a specific event type (default=All).
- **Action:** Select a specific action type (default=All).

3 Select an event-to-action, and click **Edit the item** (✎).

4 From the **When** drop-down list in the **Event-to-action** dialog box, select an event type.

(Optional) If you select **License plate read**, you can specify a condition.

5 In the **From** option, click **Any entity**, and then select an entity that triggers the event.

By default, the event-to-action occurs when any entity triggers the event type you select. If you select a specific entity, then you might have to set other parameters (for example, if you select a door, then you must also select a door side).

6 From the **Action** drop-down list, select an action type and configure its parameters.

For example, if you select the *Send an email* action, then you must also select the email recipients.

7 In the **Effective** option, click **Always**, and select a schedule when this event-to-action is active.

If the event occurs outside of the defined schedule, then the action is not triggered. For example, you might want to sound an alarm only when a window is opened during the weekend. By default, **Always** is selected.

8 Click **Save**.

The **Save** button is only available when all the arguments required by the event-to-action type are specified.

9 To delete an event-to-action, select the item, and click **Delete** (✖).

10 Click **Apply**.

Scheduled tasks

A scheduled task is a type of entity that defines an action that executes automatically on a specific date and time, or according to a recurring schedule.

Similarities between scheduled tasks and event-to-actions

The similarities between the two concepts are:

- Both have access to the same set of actions.
- Both use recurring schedules.

Differences between scheduled tasks and event-to-actions

The differences between the two concepts are:

- A scheduled task is saved as an *entity*, an event-to-action is not.
- A scheduled task is triggered on schedule, not on event.
- A scheduled task can be turned on and off.
- The scheduling options are different:
    - **Once:** Executed once at a specific date and time.
    - **Every minute:** Executed every minute.
    - **Hourly:** Executed at a specific minute of every hour.
    - **Daily:** Executed at a specific time every day.
    - **Weekly:** Executed at a specific time on selected days of the week
    - **On startup:** Executed on system startup.
    - **Interval:** Executed at regular intervals that can be days, hours, minutes, or seconds.

Scheduling a task

You can configure an action to execute automatically on system startup or according to a schedule by creating a *scheduled task*.

To set up an action to trigger on a schedule:

1 From the Config Tool home page, open the *System* task, and click the **Scheduled tasks** view.

2 Click **Scheduled task** (➕).

A new scheduled task entity appears in the entity list.

3 Type a name for the scheduled task, and press **ENTER**.

4 Click the **Properties** tab, and switch the **Status** option to **Active**.

5 In the **Recurrence** option, select how often you want the task to occur:

- **Once:** Executed once at a specific date and time.
- **Every minute:** Executed every minute.
- **Hourly:** Executed at a specific minute of every hour.
- **Daily:** Executed at a specific time every day.
- **Weekly:** Executed at a specific time on selected days of the week.
- **On startup:** Executed on system startup.
- **Interval:** Executed at regular intervals that can be days, hours, minutes, or seconds.

6 Select the type of action to be executed.

7 If required, set the additional parameters for the selected action.

For example, if you select *Synchronize role* as the action, you must select which role is synchronized.

8 Click **Apply**.

Related Topics

Action types on page 924

Adding audio files

You can add new audio files that can be played when users receive an alarm in Security Desk, or used with the *Play a sound* action.

What you should know

Security Center supports .mid, .rmi, .midi, .wav, .snd, .au, .aif, .aifc, .aiff, .mp3, and .ogg file types.

As a best practice, do not add audio files that are larger than 100 KB.

To add an audio file:

1. Open the **System** task, click the **General settings** view, and click the **Audio** page.
2. Click **Add an item** (➕).
3. In the Windows browser, select an audio file, and click **Open**.

   The audio file is added to the list.
4. To change the name of the audio file, click **Edit the item** (✏), type a name, and click **OK**.
5. To listen to the audio file, click **Play** (▶).
6. Click **Apply**.

About macros

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

Macros can be executed either manually or automatically. When automated, it is loaded as a background process and executes when a set of conditions are met.

You create macros by writing a program in C# using Security Center *SDK*, and then loading the program into Security Center. If you need help developing custom macros, contact Genetec™ Professional Services through your sales representative for a quote, or call us at one of our regional offices around the world. To contact us, visit our website at www.genetec.com.

Marco execution context

You can provide input parameters to your macro by declaring mutators. Such mutators must be public. Their type must be one of the following:

- System.Boolean
- System.String
- System.Int32
- System.Guid

By declaring mutators, your macro will have an execution context that can be configured in the *Default execution context* tab. If a macro is run without specifying an execution context, the default execution context is used. This is always the case when a macro is launched from the toolbar at the bottom of Config Tool.

The default execution context can be overridden by specifying your own context.

Creating macros

To create a macro that you can run in Security Center, you must write a C# program using an external text editor or the text editor in Config Tool, and then load the program in Security Center.

What you should know

Security Center prevents a macro that has errors from being saved. If a macro has errors, and you change tabs, it is rolled back to its last error free version.

To create a macro:

1. From the Config Tool home page, pen the *System* task, and click the **Macros** view.
2. Click **Macro** (➕), and enter the macro name.
3. Click the **Properties** tab, and do one of the following:
   - To import the source code from a file, click **Import from file**, select the file containing the C# code, and then click **Open**.
   - Write your own program in the **Properties** tab.
4. Click **Apply**.
5. If you added input parameters to the program, click the **Default execution context** tab, and configure the settings.
6. Click **Apply**.

10

Federation

This section includes the following topics:

About Federation™

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

Security Center can join (or federate) other Security Center systems and Omnicast™ systems into a large Federation™ of Genetec™ IP security systems. The system that joins other systems together is called the *Federation™ host*. Security Center does this by creating a specific Federation™ role for each system it needs to unify.

For a list of Security Center and Omnicast™ versions you can federate in this release, see the *Security Center Release Notes*.

Security Center Federation™

The Security Center Federation™ role connects a remote, independent Security Center system to your local Security Center. That way, the remote system's entities and events can be used in your local system.

The Security Center Federation™ role acts as a proxy between your local clients and the remote Security Center system they need to connect to.

Multiple instances of the Security Center Federation™ role can be created on the system.

For a detailed list of available federated events, see Federated Security Center events on the Technical Information site.

Omnicast™ Federation™

The Omnicast™ Federation™ role connects an Omnicast™ 4.x system to Security Center. That way, the Omnicast™ entities and events can be used in your Security Center system.

The Omnicast™ Federation™ role acts as a proxy between your local clients and the remote Omnicast™ system they need to connect to.

Multiple instances of the Omnicast™ Federation™ role can be created on the system.

Limitations with Omnicast™ Federation™

Federating an Omnicast™ system has the following limitations:

- Some playback capabilities are not supported on federated cameras. Smooth reverse playback is not available and the rewind speed is limited to -10x, -20x, -40x, and -100x.
- Camera sequences are federated, but they behave as a single camera on the Federation™ host. This means that the users on the Federation™ host cannot unpack nor stop the camera cycling on camera sequences () federated from Omnicast™.
- Sites () are federated as areas () in Security Center.
- Sites with a Map (URL) property () are federated as areas () with a web page tile plugin attached.

About federated entities

Federated entities are entities imported from remote independent Security Center or Omnicast™ systems.

Federated entities do not belong to your local system. You can view and manipulate them in your local system, but you cannot change their native settings. You can easily identify federated entities by the yellow arrow that is superimposed on their entity icon (for example, here is a federated alarm entity —).

The following federated entities only apply to one Federation™ type:

- – Federated door entity (Security Center Federation™ only)
- – Federated elevator entity (Security Center Federation™ only)
- – Federated cardholder entity (Security Center Federation™ only)
- – Federated credential entity (Security Center Federation™ only)
- – Federated virtual camera entity (Omnicast™ Federation™ only)

What entities are federated in Security Center

The following entities can be federated from a remote Security Center system:

Component	Entities
Video	Cameras and camera sequences
Access control	Access control units, doors, elevators, cardholders, cardholder groups, credentials, intrusion detection units, and intrusion detection areas
LPR	LPR units and patrollers
General	Alarms, cash registers, networks, areas, zones, output behaviors, and custom events

Roles, servers, partitions, and other entities not listed above will not be federated.

NOTE: Visitors and visitor groups are different from cardholders and cardholder groups and are not federated.

What you can do with federated entities in Security Desk

You can perform the following operations on federated entities in Security Desk:

- View live or playback video from federated cameras.
- Add *bookmarks*, start/stop recording, and export video from federated cameras.
- Control federated PTZ cameras (except PTZ locking).
- Switch cameras on CCTV matrices using *virtual cameras* federated from Omnicast™ 4.x.
- View, start/stop cycling, pack/unpack federated *camera sequences*.
- Receive, acknowledge, snooze, forward, start/stop cycling, pack/unpack federated alarms.
- View and control federated *tile plugins*.
- Lock/unlock federated *doors*.
- Arm/disarm federated *intrusion detection areas*.

- Arm/disarm federated *zones*.

What you can configure with federated entities

You can make the following changes to federated entities on your local system:

- You can assign a logical ID to each federated entity. The logical ID is a local attribute associated with the federated entity to uniquely identify it within the Federation.
- You can update custom fields associated to federated entities as local attributes.
- You can choose what events you want to receive from the federated system. Based on these events, you can define *event-to-actions* for the federated entities. The actions can either be executed on the Federation™ host or on the federated system.
- You can view their activity and audit trail reports in the Reporting tab.
- You can control the visibility of the federated entities to your local users using *partitions*.
- You can configure the *visual tracking* for cameras federated from Omnicast™ systems.
- You can use them in the configuration of local entities, such as attaching federated cameras to local entities, or use them to define local alarms and camera sequences.

Limitations of federated entities

You cannot do the following with federated entities:

- You cannot change their name and description on your local system.
- You cannot change any attributes that inherently defines the entity. This includes most properties defined in the entity configuration tabs, although you can view them.
- You cannot view the custom fields defined on the federated system. Custom fields are not federated.

Exceptions for federated alarms

Not all alarm properties are federated. Most properties pertaining to the alarm display in Security Desk must be configured locally on the Federation™ host.

The exceptions for federated alarms are the following:

- The alarm *schedule* follows the original configuration of the remote system. Since schedule entities are not federated, the default schedule *Always* is shown instead.
- Alarm priority:
  - Omnicast: Original value is not federated. You can configure it (default=1) locally on the Federation™ host.
  - Security Center: Original value is federated and cannot be modified.
- Reactivation threshold is an inherent property of the alarm and cannot be modified.
- Entity cycling is a local property to the Federation™ host. You can change its setting and it will not affect the federated system.
- Automatic acknowledgement is an inherent property of the alarm and cannot be modified.
- Create an *incident* on acknowledgement is a local property to the Federation™ host. You can change its setting and it will not affect the federated system.
- Automatic video recording is an inherent property of the alarm and cannot be modified.
- Protect recorded video is an inherent property of the alarm and cannot be modified.
- Video display is a local property to the Federation™ host. You can change its setting and it will not affect the federated system.

- Alarm procedure (*URL*):
  - Omnicast: Original value is not federated. You can configure it locally on the Federation™ host.
  - Security Center: Original value is federated and cannot be modified.
- Entities that are attached to the federated alarm (cameras, doors, and so on) are inherent properties of the alarm and cannot be modified.
- Alarm recipients must always be configured locally for the Federation™ host.

Related Topics

Custom card formats on page 567
Importing security groups from an Active Directory on page 323

Setting up Security Center Federation™

To set up Security Center Federation™, you must create an Security Center Federation™ role, connect it to the Security Center system, and decide which events you want to federate.

To set up a Security Center Federation™:

1 Open the **System** task, and click the **Roles** view.

2 Click **Add an entity** (✚), and click **Security Center Federation™**.

3 In the **Directory** field, enter the Directory server name of the remote Security Center system.

4 In the next two fields, enter the username and password that the Federation™ role is going to use to log on to the remote Security Center system, and click **Next**.

The rights and privileges of that user determine what your local users will be able to see and do on the federated remote system.

5 In the **Basic information** page, enter a name and description for the role.

6 Select a **Partition** this role is a member of, and click **Next**.

All federated entities are created in the partition you select. Only users that are part of the partition can view or modify those entities.

7 Click **Next** > **Create** > **Close**.

The new Federation™ role (●) is created.

8 If you plan to host more than 100 Security Center Federation™ roles on the same server, you need to assign a different *role group* to every 100 roles you create.

9 Click the **Properties** tab.

The connection status should say **Synchronizing entities**, or **Connected**.

10 From the **Default live stream** drop-down list, select the default video stream used for viewing live video from federated Security Center cameras.

11 To disable users from viewing playback video from federated cameras, then switch the **Enable playback requests** option to **OFF**.

12 If you do not want to receive alarms from the federated system, then switch the **Federate alarms** option to **OFF**.

13 In the **Federated events** section, select the events that you want to receive from the federated system, and click **Apply**.

Events are necessary if you plan to monitor the federated entities in Security Desk, or to configure event-to-actions for the federated entities.

14 Open the **Area view** task.

15 Expand the new Security Center Federation™ role (●) in the area view, and make sure all the federated entities were imported by the role.

The entity hierarchy corresponds to the area view on the federated remote system.

Related Topics

Requirements for large federations on page 196

Setting up Omnicast™ federation

To set up Omnicast™ Federation™, you must create an Omnicast™ Federation™ role, connect it to the Omnicast™ system, and decide which events you want to federate.

Before you begin

Install the Omnicast™ Compatibility Pack corresponding to the version of the Omnicast™ system you plan to federate on the following servers and workstations:

- On the server where the Federation™ role is to be hosted.
- On the client workstation where Config Tool is running.
- On all secondary servers you plan to assign to the Federation™ role.
- On all Security Desk workstations viewing the federated cameras.

To set up Omnicast™ federation:

1. Open the **System** task, and click the **Roles** view.
2. Click **Add an entity** (➕), and click **Omnicast™ Federation™**.
3. In the **Directory** field, enter the name of the Omnicast™ Gateway connecting you to the remote Omnicast™ system.
4. In the next two fields, enter the username and password that the Federation™ role is going to use to log on to the remote Omnicast™ system.

   The rights and privileges of that user determine what your local users will be able to see and do on the federated remote system.
5. From the **Version** drop-down list, select the version of the remote Omnicast™ system, and click **Next**.

   This drop-down list only shows the Omnicast™ versions for which a compatibility pack is installed.
6. In the **Federated events** section, select the events that you want to receive from the federated system, and click **Next**.

   Events are necessary if you plan to monitor the federated entities in Security Desk, or to configure event-to-actions for the federated entities.
7. In the **Basic information** page, enter a name and description for the role.
8. Select a **Partition** this role is a member of, and click **Next**.

   All federated entities are created in the partition you select. Only users that are part of the partition can view or modify those entities.
9. Click **Next** > **Create** > **Close**.

   The new Federation™ role (🌐) is created.
10. If you plan to host more than 40 Omnicast™ Federation™ roles on the same server, you need to assign a different *role group* to every 40 roles you create.
11. Click the **Properties** tab.

    The connection status should say **Synchronizing entities**, or **Connected**.
12. From the **Default live stream** drop-down list, select the default video stream used for viewing live video from federated Omnicast™ cameras.
13. To disable users from viewing playback video from federated cameras, then switch the **Enable playback requests** option to **OFF**.
14. If you do not want to receive alarms from the federated system, then switch the **Federate alarms** option to **OFF**.
15. Open the **Area view** task.
16. Expand the new Omnicast™ Federation™ role (🌐) in the area view, and make sure all the federated entities were imported by the role.

    The entity hierarchy corresponds to the area view on the federated remote system.

Related Topics

Requirements for large federations on page 196

Requirements for large federations

On a large scale deployment, Security Center can federate thousands of independent remote systems. However, there are hardware and software limitations you must consider.

The number of Federation™ roles you can host on a single server depends on the following:

- Type of Federation™ roles you are hosting.
- Number of Federation™ roles you are hosting.
- Type of computer running the Genetec™ Server service.
  - Low capacity: Intel Core 2 Duo 3.0 GHz, 2 GB RAM
  - Medium capacity: Dual Core Intel Xeon 2.66 GHz, 4 GB RAM
  - High capacity: Quad Core Intel® Xeon®, 2.00 GHz, 4 GB of RAM

Federation role groups

When a large number of Federation™ roles are hosted on the same server, they must be divided into multiple *role groups*. All roles belonging to the same role group are executed by the same process on the same machine. There is a limit to the number of roles a single process can handle.

The following table helps determine how many role groups you need on your server.

NOTE: These calculations assume that each federated system (Omnicast or Security Center system) has 150 cameras.

Role type	Number of Federation™ roles supported on a single server		
	Single role group (Any hardware profile)	**Multiple role groups(Low and Medium capacity hardware profiles)**	**Multiple role groups (High capacity hardware profile)**
Omnicast™ Federation™	40	Contact Genetec™ Technical Assistance.	100
Security Center Federation™	100	Contact Genetec™ Technical Assistance.	500

If a single role group can have up to 40 Omnicast™ Federation™ roles, a high capacity computer hosting 100 Omnicast™ Federation™ roles requires three separate role groups. A high capacity computer hosting 500 Security Center Federation™ roles requires five separate role groups.

Example

You want to federate 250 Omnicast™ sites, using one Omnicast™ Federation™ role per site. You can divide your sites as follows:

- **Server A:** 40 Omnicast™ sites (*role group 1*) + 40 Omnicast™ sites (*role group 2*) + 20 Omnicast™ sites (*role group 3*) = 100 Omnicast™ sites.
- **Server B:** 40 Omnicast™ sites (*role group 1*) + 40 Omnicast™ sites (*role group 2*) + 20 Omnicast™ sites (*role group 3*) = 100 Omnicast™ sites.
- **Server C:** 40 Omnicast™ sites (*role group 1*) + 10 Omnicast™ sites (*role group 2*) = 50 Omnicast™ sites.

Adding Federation™ role groups

If you need to host a large number of Federation™ roles on the same server, you must configure a Federation™ role group.

Before you begin

Determine how many role groups you require for your deployment.

To add a Federation™ role group:

1. Open the **System** task, and click the **Role view**.
2. Select the Federation™ role entity to configure (Security Center or Omnicast™), and click the **Identity** tab.
3. In the **Name** field, type **Ctrl+SHIFT+A**.

   The **Advanced settings** section appears at the bottom of the tab.
4. Change the **Role group** name if necessary.
5. Click **Apply**.

11

Maps

This section includes the following topics:

About Plan Manager

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

Greatly enhancing situational awareness and security management, Plan Manager allows you to dynamically navigate throughout facilities and intuitively manage your cameras, doors, intrusion devices, and other security systems.

With Plan Manager, you can:

- Gain situational awareness by monitoring your security equipment (cameras, doors, zones, intrusion panels, input pins, LPR cameras), managed by Security Center, on a map.
- Receive real-time notifications of alarms and events on maps.
- Represent both local and federated entities on maps.
- Quickly locate devices on maps, as a way to find out what other devices are in their proximity.
- Mark and locate points of interest (fire exits, first aid kits, and so on) on maps.
- View live and playback video and control cameras directly on maps.
- Monitor door status (open, closed, locked, unlocked) directly on maps.
- View license plate reads and hits from fixed LPR cameras.
- Monitor the state of input pins (active, inactive) directly on maps.
- Control PTZ cameras by dragging the cameras' field of view (FOV) on maps.
- Point all PTZ cameras to the same location on a map with a simple click.
- Lock and unlock doors, shunt readers, directly on maps.
- Arm and disarm zones directly on maps.
- Arm and disarm intrusion detection areas directly on maps.
- Control the behavior of output relays directly on maps.
- Run macros directly on maps.
- Monitor and respond to alarms directly from the maps.
- Move around and zoom in and out on maps.
- Easily navigate through different maps.
- Span a single map over multiple monitors.

Configuring the Map Manager role

Map Manager is the central role that manages all mapping resources in Security Center, including imported map files, external map providers, and KML objects. It acts as the map server to all client applications that require maps. You must configure this role before you can start using maps on your system.

What you should know

The Map Manager role is created by default at software installation, and assigned to the main server.

To configure the Map Manager role:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the Map Manager role, and click the **Properties** tab.
3. Under the **Map providers** section, connect the Map Manager to third-party map providers.

   Map providers are *GIS* systems. Most of them require a license to use. Once configured, they appear in the list of available choices when you create geographic maps.
4. (Optional) Under the **Map layers** section, import the KML objects you want to show on your maps.
5. Set the **Cache location** for your maps.

   The cache is a folder where the map tiles are stored. When you create maps from images files, the role generates a set of small images, called *map tiles*, for each zoom level at which you need to view the map. The larger the map scale, the more map tiles the role needs to generate. The default folder is *C:\ProgramData\Genetec Security Center 5.5\Maps*.

   BEST PRACTICE: If you are setting up role failover, set the cache to a location that can be reached by all servers assigned to the role. If the role cannot reach the configured cache location, it will regenerate the map tiles from the source files stored in the Directory database, and save them to the default cache location.
6. Click **Default map**, and select the default map for your system.

   The system default map, also known as the *global default map*, is used when a user does not have a personalized default map configured. You can only set the global default map after you have created your first map.
7. Click **Apply**.

Creating maps

A map in Security Center is a two-dimensional diagram that helps you visualize the physical locations of your security equipment in a geographical area or a building space. You create maps using the *Map designer* task.

Before you begin

All maps must be attached to an area in Security Center. The area and the attached map form a single entity. It is best practice to define your area hierarchy before attaching the maps.

What you should know

A map is composed of a static background image with information layered on top, called *map objects*. Security Desk users can choose to show or hide any of these layers, thus, showing more or less information on the map.

To create a map:

1. From the Config Tool home page, open the *Area view* task.
2. In the entity tree, click the area you wish to attach the map to.
3. Click the **Identity** tab, and click **Create map**.
   A new Map designer task opens.
4. Select one of the following methods to create your map background.
   - Import the map background from an image file.
   - Connect to a map provider.
5. Configure the default section and zoom level to display when someone opens this map.
6. Configure the default information to display when someone opens this map.
7. Click **Apply**.

After you finish

Add map objects to your map.

Related Topics
Overview of the Map designer task on page 209

Configuring the default map view

You can set the default values for zoom level and the displayed portion of the map, These defaults are used when someone opens the map.

What you should know

A map view is a defined display position and zoom level for a given map. The *default view* is the map view that is displayed by default when someone opens the map.

To configure the default view for a map:

1. In the *Map designer* menu, click **Edit** > **Edit default view**.
   A semi-transparent blue banner appears at the top your map.
2. Position your map to the desired default view.
   - Drag to move the map around.

- Roll the mouse wheel to zoom in or out.

3 In the blue banner, click **Save**.

Configuring default information to display on maps

You can set default information to display on your maps. This information is always displayed when someone opens the maps.

What you should know

Security Desk users can always set the layers (map objects) they want to see on their maps, regardless of what layers are displayed by default.

To configure the layers to show by default on a map:

1. In the *Map designer* menu, click **Arrange** > **Layers**.

   A dialog box listing all available layers for your map appears.
2. Select the layers you want to show by default. You can choose to show or hide any objects that appear on the map, including map objects (cameras, doors, and so on), KML objects, custom objects, LPR hits and reads, and so on.
3. To sort the layers, select a layer, and then use the up (▲) and down (▼) arrows.
4. Click **Apply**.

Creating maps from image files

You can create personalized maps of your site and floor plans of your buildings, by importing their background image from image files.

What you should know

All maps must be attached to an area.

To create a map from an image file:

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

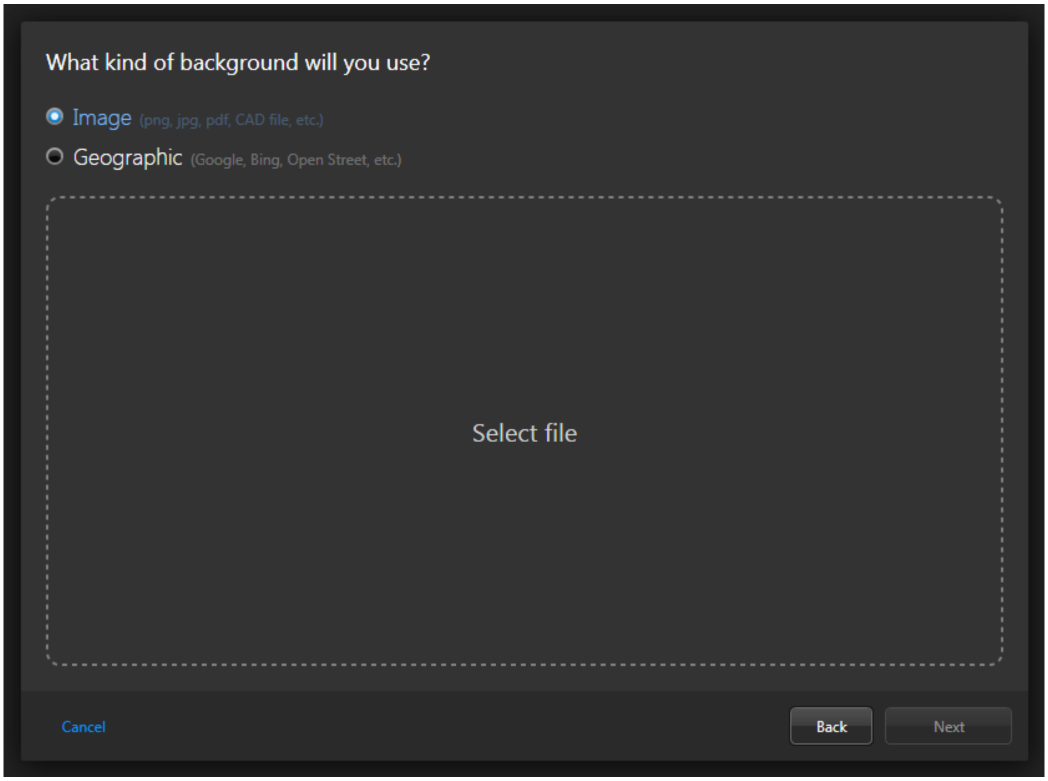
2 Click **Create** (✚).

3 From the area tree, select the area you want to attach your map to, or click **New area** (✚) to create a new one.

4 (Optional) Select the icon to represent your area with a map (Default = 🏢).

5 Click **Next**.

6 For the type of map background, select the **Image** option, and click **Select file**.



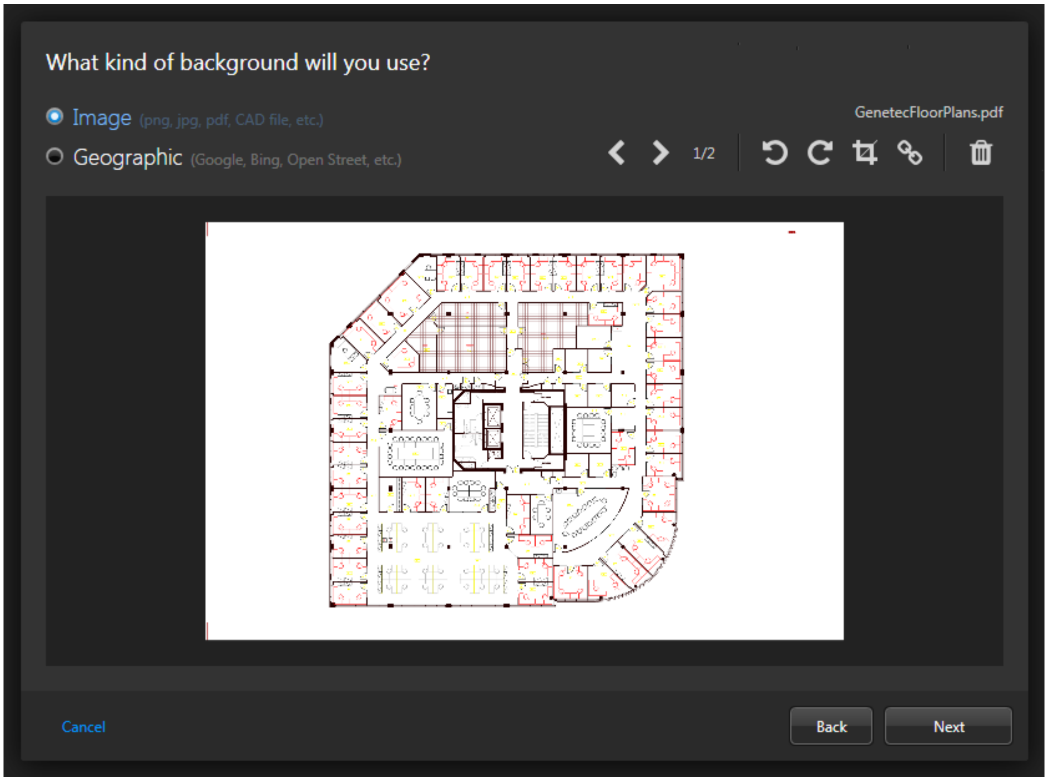
What kind of background will you use?

● Image (png, jpg, pdf, CAD file, etc.)

○ Geographic (Google, Bing, Open Street, etc.)

7 In the file browser that appears, select an image file (.png, .jpg, .pdf, and son on), and click **Open**.

The selected image appears in the preview window.



What kind of background will you use?

● Image (png, jpg, pdf, CAD file, etc.)

○ Geographic (Google, Bing, Open Street, etc.)

GenetecFloorPlans.pdf

8 If necessary, move to the desired page, and then rotate and crop the image.

9 Click **Advanced settings**, and set the following options:

- **Resolution:** The resolution of the image.
- **Projection:** The projection type of the map.
- **Background:** The background color of the image.

10 Click **Next**.

11 Set your map scale using one of the following options.

- **Room:** Floor plan for a small area such as a cafeteria or an auditorium.
- **Building:** Floor plan for a large area such as a building floor, a stadium, or a warehouse.
- **Campus:** Site map for an airport, a mall, or a university campus.
- **City:** City map. For example: Montreal, New York, Paris, London, Tokyo.
- **Specific scale:** Draw a line on the map and specify its exact length.

12 Click **Create** to generate the map.
The created map is displayed in the Map designer workspace.

13 Configure the default section and zoom level to display when someone opens this map.

14 Configure the default information to display when someone opens this map.

15 Click **Apply**.

After you finish

Add map objects to your map.

Related Topics

Setting the scale of an imported map image on page 206

Georeferencing a map image

To ensure that all imported maps respect the same scale, you can georeference each map by adding at least three markers with geographic coordinates to the map.

Before you begin

Import a map image file. For more information, see Creating maps from image files on page 203.

What you should know

IMPORTANT: Georeferencing a map removes all objects that were previously added to the map. Objects need to be added again after you georeference the map.

To georeference a map image:

1 Open the *Map Designer* task and select the map that you want to georeference.

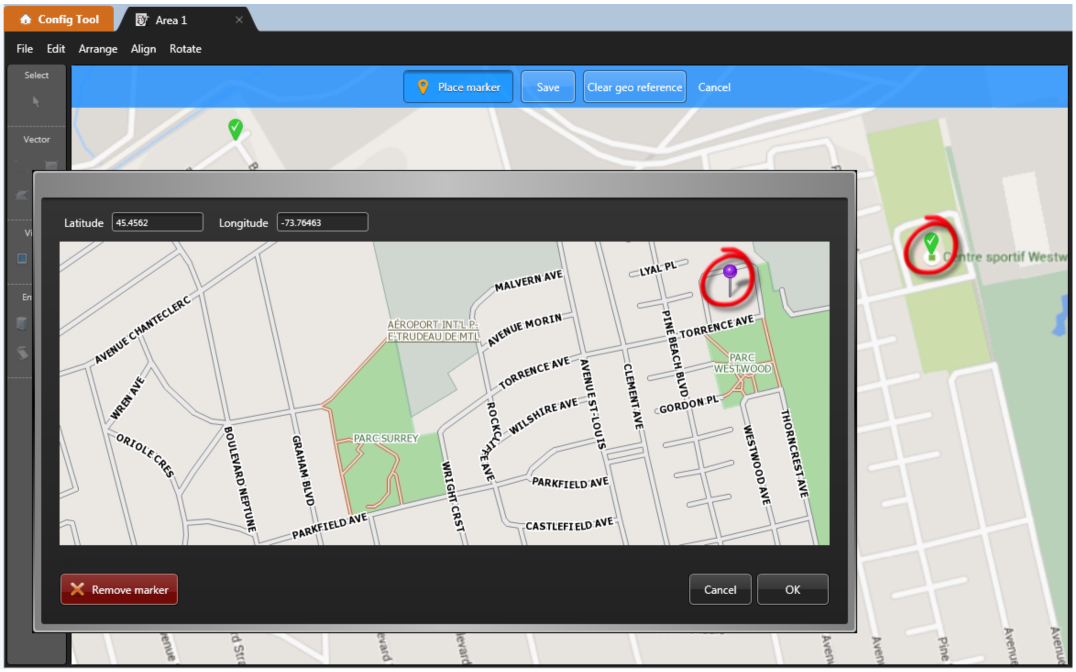
2 Click **Edit** > **Set georeference**.

3 Click **Place marker** and click a location on the map.

A window opens with a second map.

4 Zoom in and click the same location as the marker you set in the previous step.

NOTE: If you already know the exact coordinates of the location, you can enter the latitude and longitude in the provided fields.



Latitude 45.4562

Longitude -73.76463

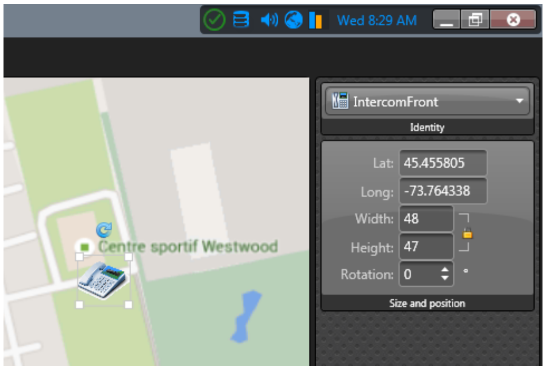
5 Click **OK** to accept the pin position.

6 Repeat the same process until you have georeferenced at least three positions.

TIP: Adding additional markers increases the georeferencing accuracy.

7 Click **Save**.

8 To verify that georeferencing is enabled on the map, add an object to the map. If the *Size and position* widget shows the latitude and longitude of the object, the map is georeferenced.



IntercomFront

Lat: 45.455805

Long: -73.764338

Width: 48

Height: 47

Rotation: 0 °

Related Topics

Setting the scale of an imported map image on page 206
Adding cameras to your maps on page 220

Setting the scale of an imported map image

To ensure that the map scale matches the field of view distance that is defined for cameras on the map, you can set the scale of the imported map image.

Before you begin

- Import a map image file.
- Add a camera to the map.
- Know the exact distance between two points that appear on the map.

What you should know

As an alternative to setting the scale of the map, you can georeference the map.

NOTE: Map scaling and georeferencing cannot be set at the same time.

To set the scale of an imported map image:

1. Open the *Map Designer* task and select the map that you want to scale.
2. Click **Edit** > **Set scale**.
3. From the drop-down list at the top of the screen, select the units to use for the measurement (for example, meters or feet) and define the number of units to match your known measurement.
4. Click **Draw line**.
5. Click and drag your mouse across the map to draw the line.
6. Move the endpoints of the line until they match the two known points of your measurement.
7. Click **Save**.

   The camera's field of view is automatically adjusted to the scale you have defined.

Related Topics

Creating maps from image files on page 203
Adding cameras to your maps on page 220
Georeferencing a map image on page 205

Creating maps by connecting to a GIS

You can create detailed road maps and large area maps by connecting to a third-party *GIS* vendor, also known as a map provider.

Before you begin

You must connect your Map Manager to at least one external map provider.

What you should know

All maps must be attached to an area.

To create a map by connecting to a map provider:

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

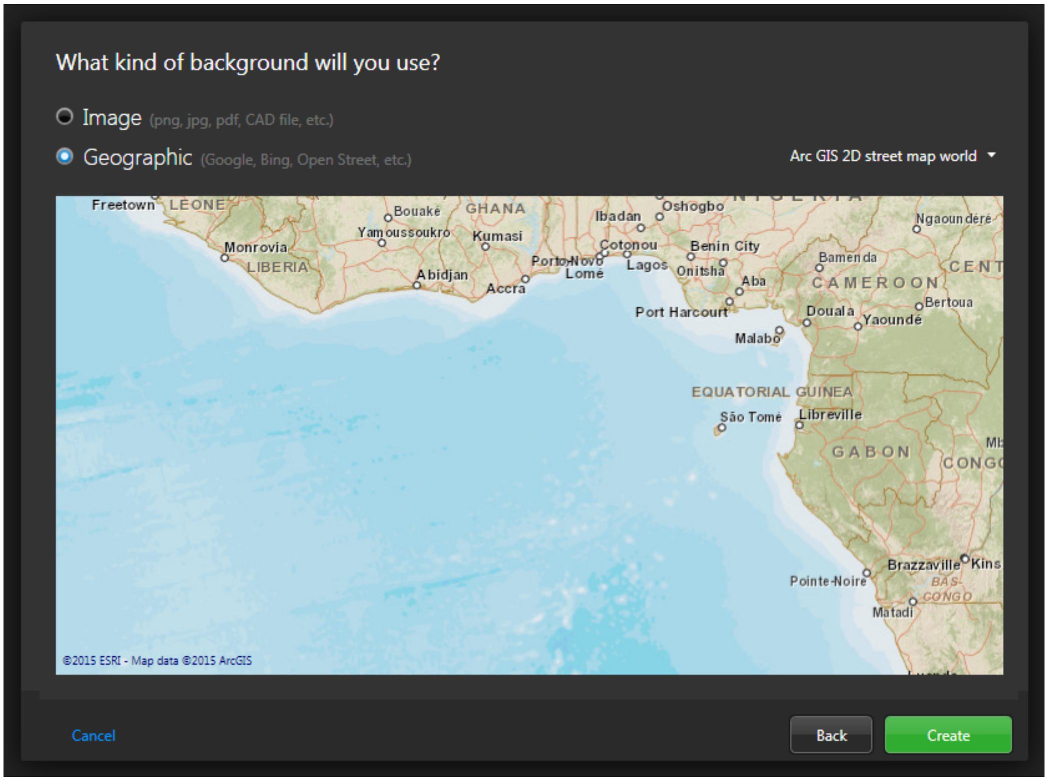
2 Click **Create** (➕).

3 From the area tree, select the area you want to attach your map to, or click **New area** (➕) to create a new one.

4 (Optional) Select the icon to represent your area with a map (Default = ▦).

5 Click **Next**.

6 For the type of map background, select the **Geographic** option.



What kind of background will you use?

○ Image (png, jpg, pdf, CAD file, etc.)

● Geographic (Google, Bing, Open Street, etc.)

Arc GIS 2D street map world ▾

©2015 ESRI - Map data ©2015 ArcGIS

Cancel

Back

Create

7 Click the drop-down list to the right, select the desired map provider, and then click **Create**.

The created map is displayed in the Map designer workspace.

8 Configure the default section and zoom level to display when someone opens this map.

9 Configure the default information to display when someone opens this map.

10 Click **Apply**.

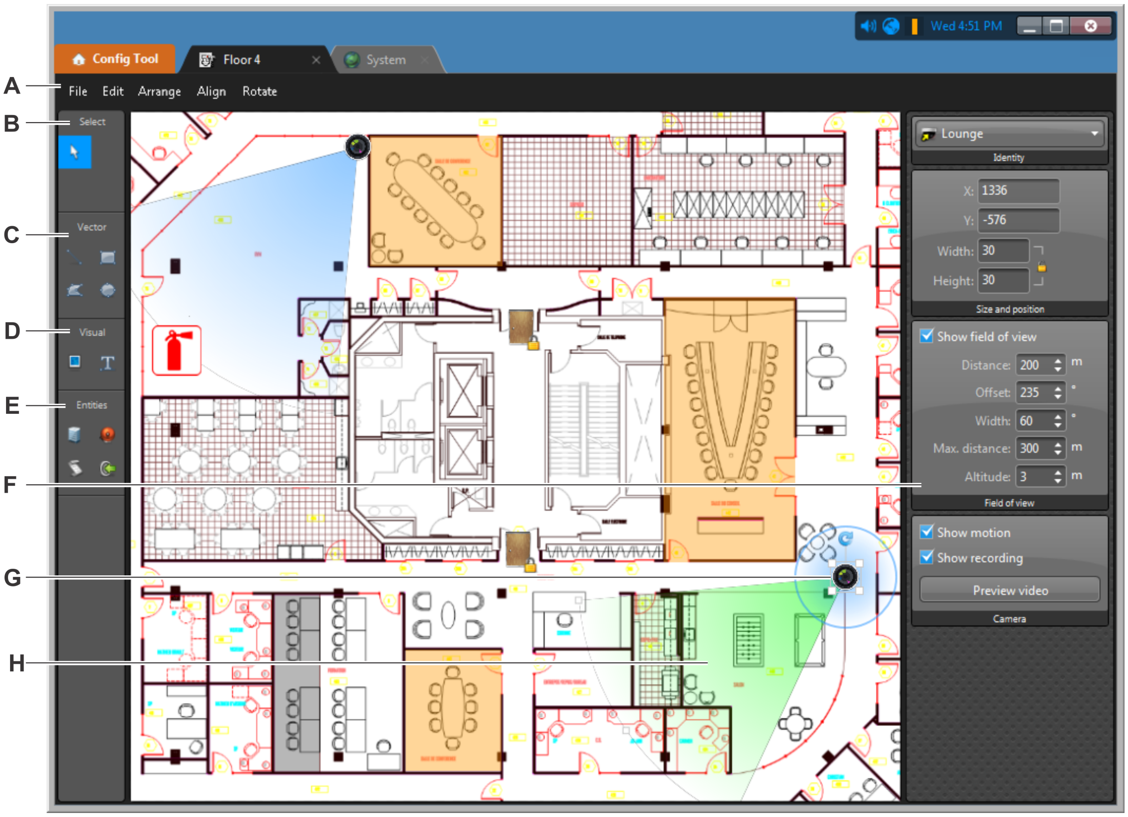
After you finish

Add map objects to your map.

Overview of the Map designer task

Use the Map designer task to create and edit maps that represent physical locations of your equipment to Security Desk users.

A map in Security Center is a two-dimensional diagram that helps you visualize the physical locations of your security equipment in a geographical area or a building space. The following figure shows a Map designer task editing a map named "Floor 4" in an access control and video monitoring system.



X: 1336
Y: -576
Width: 30
Height: 30

☑ Show field of view
Distance: 200 m
Offset: 235 °
Width: 60 °
Max. distance: 300 m
Altitude: 3 m

☑ Show motion
☑ Show recording

A Use the Map designer menu to create, edit, and delete the maps in your system, as well as arrange the *map objects* on your map.

B **Selection tool** (): Click a map object to select it. Click and hold the map background to move it. To select multiple map objects with a rectangle, hold the Alt key, and then click and drag.

C Draw vector objects:

- **Draw line:** Click and drag to draw a single line segment to represent a wall.
- **Draw rectangle:** Click and drag to draw a rectangle. Drag a handle to change its size. Note that you cannot change a rectangle into a different type of polygon.
- **Draw polygon:** Click once for each endpoint, and click the first endpoint to close the polygon. Use Alt+Click to add a point between two points, and Alt+Right-Click to remove a point.
- **Draw ellipse:** Click and drag to draw an ellipse. Drag a handle to change its size.

D	Insert images and text: • **Insert image:** Opens a browser for you to select an image file, and click to place it on the map. • **Insert text:** Click to place a text box on the map. Double-click the text box to enter the text. Use the widgets to adjust the appearance of the text.
E	Create map objects representing entities: • **Area view:** Click the area view to create map objects representing areas, intrusion detection areas, cameras, camera sequences, doors, LPR cameras, and zones. • **Alarms:** Click, select, and drag an alarm to the map. • **Macros:** Click, select, and drag a macro to the map. • **I/Os:** Click, select, and drag an input pin or an output relay to the map. **NOTE:** It is possible to select I/Os federated and local cameras.
F	Use the widgets to configure the selected map object. When multiple map objects are selected, only the common widgets are displayed.
G	The selected map object is circled in blue.
H	Click and drag the FOV to position it on the map.

Supported map objects

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

Map objects are displayed on your map as dynamic icons or as colored shapes that you can point and click. The following standard actions can be performed on most map objects:

- Point to show the name of the entity it represents.
- (When applicable) Click to display the entity in a tile bubble and its corresponding widgets in the dashboard.
- (When applicable) Double-click to display the entity in the Monitoring task.
- Right-click to display the contextual menu.
- Right-click the entity, and jump to its configuration page.

The following map objects are supported.

Map object	Appearance on maps	Application and specific actions
Access control unit	• - Access control unit • The color indicates the access control unit state: *Online*, *Offline*, or *Warning*.	• Monitor the access control unit state.
Area	• Map thumbnail (always linked to the map that is represented by the thumbnail). • Colored semi-transparent polygon (may or may not be linked to a map).	• Point to show people count or people presence (if enabled). • Click to switch to the linked map if it is defined, or else, display the area (or map) in a tile bubble.
Door	• - Door open • - Door closed (no lock is configured) • - Door closed and locked • - Door closed and unlocked • - Door forced open • - Door unlocked and in maintenance mode • Events are displayed in event notification bubbles. The color of the bubble corresponds to the color assigned to the event.	• Monitor alarms, and door states and events. • Point to the bubble to show more details. • Click the notification bubble to change it into a tile bubble. • Unlock the door, override the unlock schedule, and shunt the reader from the door widget, or by right-clicking the door on the map.

Map object	Appearance on maps	Application and specific actions
Camera	• - Camera is not recording • - Camera is recording • - Camera detected motion (with green ripple effect) • -Camea is in maintenance mode • Fixed cameras are shown with a blue FOV (field of view). • PTZ cameras are shown with a green FOV.	• Monitor alarms and camera events. • Click to view live or playback video in a tile bubble. • Click and drag the FOV to pan and tilt (only if the camera supports position feedback). • Use the PTZ widget to zoom in and zoom out. • Click a location on the map while holding the CTRL key to point all available cameras to that location.
Camera sequence	• - Camera sequence	• Display multiple cameras at once. • Point a number of PTZ cameras to a specific location. • Double-click the camera sequence to display the all cameras in separate tiles in the Monitoring task. If the map is displayed in a tile, it is not replaced if tiles are full. **NOTE:** When using the **Locate me** map control, you will get results for individual cameras that are part of the sequence. The camera sequence is not found by the **Locate me** control.
LPR camera	• - Fixed LPR camera • - LPR camera is in maintenance mode • Reads and hits are shown in notification bubbles.	• Monitor reads and hits from LPR cameras. • Click to view live video from the associated context camera.
Alarm	• - Alarm is inactive • - Alarm is active • Colored semi-transparent polygon or ellipse that turns red and flashes if the alarm is active. • A map object that is linked to an active alarm is flagged with an alarm notification bubble.	• Show alarms on maps (useful when no entities attached to the alarm are represented on maps). • Point to the bubble to show more details. • Click the notification bubble to change it into a tile bubble. • (Inactive) Click to trigger the alarm manually. • (Active) Click to display the alarm in a tile bubble.

Map object	Appearance on maps	Application and specific actions
Intrusion detection area	• Intrusion detection areas are represented as colored semi-transparent polygons. • The color indicates the intrusion detection area state: *Perimeter armed*, *Master armed*, *Disarmed*, or *Unknown*.	• Monitor alarms and intrusion detection area state. • Arm and disarm the intrusion detection area from the widget.
Zone	• Hardware and virtual zones are represented as colored semi-transparent polygons. • The color indicates the zone state: *Armed*, *Disarmed*, or *Unknown*.	• Monitor alarms and zone state. • Arm and disarm the zone from the widget.
Input pin	• 🟢 - Input is active • 🔴 - Input is inactive	• Monitor the input state.
Output relay	• - Output relay (Normal) • - Output relay (Active)	• Trigger output behaviors on output relays directly from maps. • Click to show a list of output behaviors you can trigger.
KML object	• Can be anything displayed as transparent layer over a georeferenced map.	• Overlay useful information on maps, such as city boundaries, roads, and hydrographic features.
Macro	• - Macro	• Execute macros directly from maps. • Override the default execution context on maps. • Click on a macro to run it.
Map link	A map link is a map object that brings you to another map with a single click. Map links can be represented as map thumbnails, or any texts, icons, images, or colored geometrical shapes.	• Map navigation without using the Maps toolbar. • Particularly useful when the map is displayed in the Monitoring task. • Click to switch to the linked map.
Text, images and geometrical shapes	Text, icons, images, and colored geometrical shapes (polygons and ellipses) can be added to maps to provide additional information, indicate the location of points of interest, or serve as map links or alarms.	A sample application could be to indicate the location of wall mounted scanners on a department store floor plan.

Map object	Appearance on maps	Application and specific actions
Custom object	Custom objects can be added to the map as icons or polygons to add custom behavior to the map.	Examples of custom objects include: custom intercom solution, GPS tracker for mobile units. Contact your representative of Genetec Inc. for information on Genetec™ Custom Solutions.
Cluster bubble	A group of three or more map objects that are located close together are represented by a blue cluster bubble.	Click to zoom in on the map to view the individual map objects.

Adding map objects to your maps

You must add *map objects* to your maps for your maps to be interactive.

Before you begin

Create the map where you want to add the map objects.

What you should know

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

To add a map object to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.
   The selected map fills the Map designer workspace.
3. Do one of the following:
   - Add an access control unit.
   - Add an area.
   - Add a door.
   - Add a camera.
   - Add a camera sequence.
   - Add a fixed LPR camera.
   - Add an alarm.
   - Add an intrusion detection area.
   - Add a zone.
   - Add an input pin.
   - Add an output relay.
   - Add a KML object.
   - Add a macro.
   - Add a point of interest.

After you finish

View and test your map objects in Security Desk with the *Maps* task.

Related Topics
Overview of the Map designer task on page 209

Adding areas to your maps

You can add areas to your maps to allow Security Desk operators to use them as *map links*, monitor people counts, show people presence, or all the above.

Before you begin

Create the map where you want to add your areas.

What you should know

- Areas that have a map attached are represented as map thumbnails by default. The map thumbnails are meant to be used as *map links*.
- Area that do not have a map attached are represented as tetragons by default. You can change them later into any type of polygon.
- You can also use any icon, image, or geometrical shape to represent areas on the map.

To add an area to your map:

1. Do one of the following:
   - Add an area as a map thumbnail.
   - Add an area for monitoring people counts.
   - Add an area as a custom shape or image.
2. Click **Apply**.

Related Topics
Overview of the Map designer task on page 209

Adding areas as map thumbnails to your maps

You can add areas with a map attached, as map thumbnails to a map, and use them as *map links*.

Before you begin

- Create the map where you want to add your map thumbnails.
- Make sure you have other maps you want to link to from your current map.

To add an area as a map thumbnail to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.
   The selected map fills the Map designer workspace.
3. In the toolbar, click **Area view** ( ), select the map ( ) you want to link to, and drag it to where you want its thumbnail to be on the current map.
   A large thumbnail of the target map appears on your current map.
4. Resize and position the thumbnail to the location you want using the mouse.
5. Click **Apply**.

Adding areas for people counting to your maps

You can add secured areas to your maps to view people counts on maps.

Before you begin

- Create the map where you want to add your areas to.
- Make sure you have secured areas configured for people counting in your system.

To add an area for people counting to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

   The selected map fills the Map designer workspace.
3. In the toolbar, click **Area view** ( ), select the secured area ( ) you want to add, and drag it to where you want it to be on the map.

   A tetragon appears on the map.
4. Drag the corners of the tetragon to cover the physical space the secured area represents on the map.

   Use Alt+Click to add a point between two points, and Alt+Right-Click to remove a point.
5. Use the **Color and border** widget to change the display attributes of the map object.

   Select **Block field of view** if the perimeter of the secured area corresponds to actual walls.
6. (Optional) Click **Unassigned** in the **Links** widget to make the map object into a *map link*.

   NOTE: If you add multiple links to the map object, the operator would have to click three times to get to a link. The first click displays the entity that identifies the map object. The second click displays the choices of links. The third click selects a link.
7. Click **Apply**.

Adding text, images, and shapes to your maps

You can add text, images, and shapes to your maps to indicate points of interest, or to represent entities on the map with something else than the standard look. These map objects can also be doubled as *map links*.

Before you begin

Create the map where you want to add your graphical objects.

What you should know

Entities that are normally represented by polygons, such as areas, intrusion detection areas, and zones, can be assigned to custom graphical objects. Alarms can also be assigned to custom graphical objects.

To add a text or an image to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

   The selected map fills the Map designer workspace.
3. In the toolbar, click one of the following tools to insert a graphical object:
   - **Draw rectangle:** Click and drag to draw a rectangle. Drag a handle to change its size. Note that you cannot change a rectangle into a different type of polygon.
   - **Draw polygon:** Click once for each endpoint, and click the first endpoint to close the polygon. Use Alt+Click to add a point between two points, and Alt+Right-Click to remove a point.
   - **Draw ellipse:** Click and drag to draw an ellipse. Drag a handle to change its size.
   - **Insert image:** Opens a browser for you to select an image file, and click to place it on the map.
   - T **Insert text:** Click to place a text box on the map. Double-click the text box to enter the text. Use the widgets to adjust the appearance of the text.
4. (Optional) In the **Color and border widget**, select **Block field of view** to use the object to block camera FOVs on the map.

   NOTE: The **Block field of view** option is not available for ellipses.
5. (Optional) Click **Unassigned** in the **Identity** widget to assign an entity to your map object.

   Map objects inherit their identity from the entity they represent. You do not need to assign an entity to the map object if you are only using it to indicate a point of interest. Map objects that are not assigned to an entity have no name.
6. (Optional) Click **Unassigned** in the **Links** widget to make the map object into a *map link*.

   NOTE: If you add multiple links to the map object, the operator would have to click three times to get to a link. The first click displays the entity that identifies the map object. The second click displays the choices of links. The third click selects a link.
7. Click **Apply**.

Adding doors to your maps

You can add doors to your maps to allow Security Desk operators to monitor door events, manage alarms, and control door locks and readers from maps.

Before you begin

- Create the map where you want to add your doors.
- Make sure you have door in your Security Center system.

To add a door to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

   The selected map fills the Map designer workspace.
3. In the toolbar, click **Area view** ( ), select the door you want to add, and drag it to where you want it to be on the map.

   The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity it represents.
4. Click **Apply**.

Related Topics

Overview of the Map designer task on page 209

Adding cameras to your maps

You can add cameras to your maps to allow Security Desk operators to monitor live video and camera events, manage alarms, and control PTZ cameras and recording from maps.

Before you begin

- Create the map where you want to add your cameras.
- Make sure you have cameras in your Security Center system.

What you should know

You can draw walls and other obstacles on your map to block the field of view of your cameras. This creates a more realistic effect. Know, however, that the blocking effect is only visible when the map is displayed in the Maps or the Monitoring task.

To add a camera to your map:

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

2 Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

The selected map fills the Map designer workspace.

3 In the toolbar, click **Area view** ( ), select the camera you want to add, and drag it to where you want it to be on the map.

The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity it represents.

4 Select **Show field of view**, and set the FOV properties.

IMPORTANT: You must set the FOV properties even if you do not intend to show the FOV on the map. The orientation, width, and maximum distance of the FOV are necessary for the *Smart click* feature to work properly.

NOTE: If the map that you are adding the camera to is an imported image file, you must set the scale of the map to give meaning to the distances in the field of view properties. You can do this by georeferencing the map, or by setting the scale of the map.

- **Distance:** Length of the FOV as it appears on the map.
- **Orientation:** Direction the camera is pointing.
- **Width:** Width of the FOV as it appears on the map.
- **Max. distance:** How far the camera can see. Mainly for *Smart click* calculations.
- **Elevation:** Distance of the camera from the ground.

TIP: Alternatively, you can adjust the orientation and the length of the FOV with the mouse.

5 Select the camera events you wish to monitor on the map.

- **Show motion:** Shows the camera icon with a green ripple effect ( ) on *Motion on* event.
- **Show recording:** Shows the camera icon with a red button ( ) when recording is on.

6 Click **Apply**.

Related Topics

Setting the scale of an imported map image on page 206
Georeferencing a map image on page 205
Overview of the Map designer task on page 209

Drawing walls to block the field of view of your cameras

You can draw walls and other obstacles on your map to block the field of view of your cameras. This creates a more realistic effect.

What you should know

Only lines, rectangles, and polygons, can be used to block the field of view (FOV) of cameras. Text, images, and elliptical shapes cannot be used for blocking.

To draw an object to block the FOV of cameras:

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

2 Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

The selected map fills the Map designer workspace.

3 In the toolbar, click one of the following tools to insert a graphical object:

- **Draw line:** Click and drag to draw a single line segment to represent a wall.
- **Draw rectangle:** Click and drag to draw a rectangle. Drag a handle to change its size. Note that you cannot change a rectangle into a different type of polygon.
- **Draw polygon:** Click once for each endpoint, and click the first endpoint to close the polygon. Use Alt+Click to add a point between two points, and Alt+Right-Click to remove a point.

4 In the **Color and border widget**, select **Block field of view**.

Be sure to set the border thickness to zero if you do not want the lines to show on your map.

5 Click **Apply**.

Adding camera sequences to your maps

To allow Security Desk operators to focus on a point of interest, you can add camera sequences to your maps so that multiple cameras are displayed when you click a single map object.

Before you begin

- Create the map where you want to add your camera sequences.
- Make sure you have camera sequences in your Security Center system.

What you should know

A camera sequence marks a location on the map that requires special attention or close monitoring. You can configure a camera sequence so that when it is displayed, it turns all PTZ cameras that are part of it to a specific location (preset position).

To add a camera sequence to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

   The selected map fills the Map designer workspace.
3. In the toolbar, click **Area view** (▤), select the camera sequence you want to add, and drag it to where you want it to be on the map.

   The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity it represents.
4. Click **Apply**.

Related Topics

Overview of the Map designer task on page 209

Adding LPR cameras to your maps

You can add fixed LPR cameras to your maps to allow Security Desk operators to monitor reads and hits from maps.

Before you begin

- Create the map where you want to add your fixed LPR cameras.
- Make sure you have fixed LPR cameras in your Security Center system.

What you should know

To add a fixed LPR camera to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

   The selected map fills the Map designer workspace.
3. In the toolbar, click **Area view** ( ), select the context camera ( ) attached to the fixed LPR camera you want to add, and drag it to where you want it to be on the map.

   NOTE: Do not drag the LPR unit ( ) or the LPR camera ( ) itself.

   The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity it represents.
4. In the **LPR rules** widget, select a hotlist.
5. Click **Apply**.

Related Topics

Overview of the Map designer task on page 209

Adding access control units to your maps

You can add access control units to your maps to allow Security Desk operators to monitor access control unit states from maps.

Before you begin

- Create the map to which you want to add your access control unit.
- Make sure you have access control units in your system.

To add an access control unit to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

   The selected map fills the Map designer workspace.
3. In the toolbar, click **IOs** (), select the access control unit () you want to add, and drag it to where you want it to be on the map.

   The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity it represents.
4. Click **Apply**.

Adding alarms to your maps

You can add alarms to your maps to allow Security Desk operators to monitor and manage alarms from maps.

Before you begin

- Create the map where you want to add your alarms.
- Make sure you have alarms in your Security Center system.

What you should know

Alarm notification bubbles are displayed above all map objects that represent an entity attached to an active alarm. If no entities attached to an active alarm is represented on a map, then no alarm notifications is displayed on that map, unless the active alarm itself is represented on that map.

You can also link an alarm to a custom shape.

To add an alarm to your map:

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

2 Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

The selected map fills the Map designer workspace.

3 In the toolbar, click **Alarms** (🚨), select the alarm you want to add, and drag it to where you want it to be on the map.

The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity it represents.

4 Click **Apply**.

Related Topics
Overview of the Map designer task on page 209

Adding intrusion detection areas to your maps

You can add intrusion detection areas to your maps to allow Security Desk operators to monitor and control intrusion detection areas from maps.

Before you begin

- Create the map where you want to add your intrusion detection areas.
- Make sure you have intrusion detection areas in your system.

To add an intrusion detection area to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

   The selected map fills the Map designer workspace.
3. In the toolbar, click **Area view** ( ), select the intrusion detection area ( ) you want to add, and drag it to where you want it to be on the map.

   A tetragon appears on the map.
4. Drag the corners of the tetragon to cover the physical space the intrusion detection area represents on the map.

   Use Alt+Click to add a point between two points, and Alt+Right-Click to remove a point.
5. Use the **Color and border** widget to change the display attributes of the map object.

   Select **Block field of view** if the perimeter of the intrusion detection area corresponds to actual walls.
6. (Optional) Click **Unassigned** in the **Links** widget to make the map object into a *map link*.

   NOTE: If you add multiple links to the map object, the operator would have to click three times to get to a link. The first click displays the entity that identifies the map object. The second click displays the choices of links. The third click selects a link.
7. Click **Apply**.

Related Topics

Overview of the Map designer task on page 209

Adding zones to your maps

You can add hardware zones and virtual zones to your maps to allow Security Desk operators to monitor and control zones from maps.

Before you begin

- Create the map where you want to add your zones.
- Make sure you have zones in your system.

To add an zone to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

   The selected map fills the Map designer workspace.
3. In the toolbar, click **Area view** ( ), select the hardware zone ( ) or the virtual zone ( ) you want to add, and drag it to where you want it to be on the map.

   A tetragon appears on the map.
4. Drag the corners of the tetragon to cover the physical space the zone represents on the map.

   Use Alt+Click to add a point between two points, and Alt+Right-Click to remove a point.
5. Use the **Color and border** widget to change the display attributes of the map object.

   Select **Block field of view** if the perimeter of the zone corresponds to actual walls.
6. (Optional) Click **Unassigned** in the **Links** widget to make the map object into a *map link*.

   NOTE: If you add multiple links to the map object, the operator would have to click three times to get to a link. The first click displays the entity that identifies the map object. The second click displays the choices of links. The third click selects a link.
7. Click **Apply**.

Related Topics

Overview of the Map designer task on page 209

Adding input pins to your maps

You can add input pins to your maps to allow Security Desk operators to monitor the states of input pins from maps.

Before you begin

- Create the map where you want to add your input pins.
- Make sure you have input pin in your Security Center system.

To add a input pin to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

   The selected map fills the Map designer workspace.
3. In the toolbar, click **IOs** (), select the input pin () you want to add, and drag it to where you want it to be on the map.

   The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity it represents.
4. Click **Apply**.

Related Topics

Overview of the Map designer task on page 209

Adding output relays to your maps

You can add output relays to your maps to allow Security Desk operators to trigger output behaviors on output relays from maps.

Before you begin

- Create the map where you want to add your output relays.
- Make sure you have output relay in your Security Center system.

To add a output relay to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

   The selected map fills the Map designer workspace.
3. In the toolbar, click **IOs** (), select the output relay () you want to add, and drag it to where you want it to be on the map.

   The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity it represents.
4. In the **Ouptut behaviors** widget, click **Add action** (✚), select an output behavior and give it a name.

   You can configure multiple output behaviors. When an operator clicks an output relay on the map, the available output behaviors appear in a menu bubble.
5. Click **Apply**.

Related Topics

Overview of the Map designer task on page 209

Adding macros to your maps

You can add macros to your maps to allow Security Desk operators to run macros from maps.

Before you begin

- Create the map where you want to add your macros.
- Make sure you have macro in your Security Center system.

To add a macro to your map:

1. From the Config Tool home page, open the *Map designer* task.
2. Select one of the **Recent maps** or click **Browse all maps** to open an existing map.

   The selected map fills the Map designer workspace.
3. In the toolbar, click **Macros** (📜), select the macro (📜) you want to add, and drag it to where you want it to be on the map.

   The widgets for configuring the map object appear in the right panel. The map object always takes on the identity of the entity it represents.
4. (Optional) In the **Macro properties** widget, click **Override default context** to set an execution context that is different from the default.

   Click **Clear** to revert to the default execution context. the For more information on macro execution context, see About macros on page 186.
5. Click **Apply**.

Related Topics

Overview of the Map designer task on page 209

Adding KML objects to your maps

You can add features, such as roads, parks, buildings, and so on, to your maps by importing Keyhole Markup Language (KML) objects from KML files through the Map Manager role.

Before you begin

You must create at least one georeferenced map.

What you should know

Keyhole Markup Language (KML) is a file format used to display geographic data in an Earth browser such as Google Earth and Google Maps. KML objects are typically used to represent static objects such as roads, rivers, parks, buildings, and so on. They can only be used with georeferenced maps.

To add KML objects to your map:

1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the Map Manager role, and click the **Properties** tab.
3. Under the **Map layers** section, click **Add an item** (➕).
4. In the **Select layers to import** dialog box, enter the path to your `.kml` file.
   A preview of the KML object appears in the dialog box.
5. Click **Import**, and then click **Apply**.

After you finish

The newly imported KML objects will appear by default on all existing maps you have created. If you do not want to show them in some maps, you must change those maps and remove this KML layer from their default layers.

Configuring map clustering options in Security Center

By default, groups of three or more map objects that are located close together are represented by blue cluster bubbles on a map. If you have a small number of cameras or other map objects on your map, you can reconfigure or disable this feature from the *LnkMaps.config* file.

To configure map clustering options in Security Center:

1. Open the *LnkMaps.config* file, located in the *ConfigurationFiles* folder of your Security Center installation folder.
2. To disable clustering, add the following code to the <Maps> line:

   ```
   EnableClustering="False"
   ```

3. To disable clustering only if there are less than *x* number of map objects on your map, add the following code to the <Maps> line, and specify the desired number of map objects:

   ```
   ClusterMinObjectCount="500"
   ```

4. To change the default number of map objects that must be close together in order for cluster bubbles to appear, add the following code to the <Maps> line, and change the number from 3 to the desired number:

   ```
   ClusterDensity="3"
   ```

5. Save the *LnkMaps.config* file, and then restart Config Tool and Security Desk.

The next time you open Config Tool or Security Desk, the map clustering changes are made.

12

Plugins

This section includes the following topics:

About the Plugin role

Plugin is a type of role that hosts a specific plugin. Each Plugin role instance hosts exactly one plugin of the type you select.

You need to install the plugin package on your client and server computers before you can create the corresponding Plugin role, and you must make sure your Security Center license has a valid *certificate* for the plugin you want to use. For more information, see the individual *Plugin Guide* for the plugin you are using. The Plugin Guides are available for download from the GTAP Documents page. Note, you'll need a username and password to log on to GTAP.

About tile plugins

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

The *tile plugin* entity represents either a website (🌐) or an interactive *.dll* or *.xaml* file (🧩).

When a tile plugin is displayed in Security Desk, you can view and interact with the website or the interactive plugin file. When a tile plugin is attached to (is a member of) an area entity, it is automatically displayed in Security Desk instead of the area icon when the area is dragged to a tile.

Creating tile plugins that link to a website

You can create a tile plugin that links to a web site that contains a map, which you can interact with when the tile plugin is displayed in Security Desk.

What you should know

Make sure that URL you link the tile plugin to can be reached from all Security Desk workstations, or some users might not be able to view the map or other content from the URL.

To create a tile plugin that links to a website:

1 Open the **Area view** task.
2 Click **Add an entity** (➕) > **Tile plugin**.
3 In the **Creating a tile plugin** wizard, enter the entity name and description.
4 If there are partitions in your system, select the partition the tile plugin is a member of, and click **Next**.

   Partitions determine which Security Center users have access to this entity. Only accepted users of the partition can view and modify the tile plugin.

5 In the *Tile plugin information* page, select **Website**.
6 Click **Next** > **Close**.

   The tile plugin appears in the area view with a website icon (●).

7 Select the tile plugin, and click the **Properties** tab.
8 In the **Web page** option, type a web address.
9 Click **Apply**.

Related Topics
About tile plugins on page 235

Creating tile plugins that link to an executable file

You can create a tile plugin that links to a .dll or .xmal file that contains an executable that you can interact with when the tile plugin is displayed in Security Desk.

Before you begin

The executable file must be created and located on your local computer.

To create a tile plugin that links to an executable file:

1 Open the **Area view** task.

2 Click **Add an entity** (➕) > **Tile plugin**.

3 In the **Creating a tile plugin** wizard, enter the entity name and description.

4 If there are partitions in your system, select the partition the tile plugin is a member of, and click **Next**.

   Partitions determine which Security Center users have access to this entity. Only accepted users of the partition can view and modify the tile plugin.

5 In the *Tile plugin information* page, select **Tile plugin**.

6 In Windows, select the .dll file that the tile plugin will link to, and click **Open**.

7 Click **Next** > **Close**.

   The tile plugin appears in the area view with the default tile plugin icon (🧩).

8 Select the tile plugin, and click the **Properties** tab.

9 To select another executable file, click **Modify**, and select another .dll file.

10 Click **Apply**.

Related Topics

About tile plugins on page 235

13

Health monitoring

This section includes the following topics:

About Heath monitoring

Health monitoring refers to a set of tools to monitor your Security Center system's health. The goal is to detect health issues early enough to avoid more serious problems in the future. Health monitoring also provides you with the information to identify the root cause of various health problems so that they can be prevented from occurring again.

Health events

The table below lists the health events by their error number and indicates their severity level, information (ℹ), warning (⚠), or error (❗).

Error number	Health event	Severity
64	Archive transfer failed	Error
63	Archive transfer succeeded	Information
61	Duplicating archives failed	Error
62	Duplicating archives partially failed	Error
60	Duplicating archives succeeded	Information
58	Retrieving archivevs from units failed	Error
59	Retrieving archives from units partially failed	Error
57	Retrieving archives from untis succeeded	Information
1	Archiving started	Information
2	Archiving stopped	Error
3	Application connected	Information
4	Application disconnected by user	Information
5	Application disconnected unexpectedly	Warning
6	Application started	Information
7	Application stopped by user	Information
8	Application stopped unexpectedly	Warning
9	Connection restored	Information
10	Connection failed	Error
11	Connection to unit established	Information
12	Connection to unit stopped unexpectedly	Error

Error number	Health event	Severity
13	Connection to unit stopped by user	Information
14	Database automatic backup restored	Information
15	Database automatic backup failed	Error
16	Database recovered	Information
17	Database lost	Error
18	CPU usage normal	Information
19	CPU usage high	Warning
20	Memory usage normal	Information
21	Memory usage high	Warning
22	Database space normal	Information
23	Database space low	Warning
24	Patroller offload restored	Information
25	Patroller offload failed	Error
26	Patroller online	Information
27	Patroller offline	Information
28	*Point of Sale* database recovered	Information
29	*Point of Sale* database lost	Error
30	Role started	Information
31	Role stopped unexpectedly	Error
32	Role stopped by user	Information
33	RTP packet loss normal	Information
34	RTP packet loss high	Warning
35	Server started	Information
36	Server stopped by user	Information
37	Server stopped unexpectedly	Error
38	Synchronization recovered	Information
39	Synchronization failed	Warning

Error number	Health event	Severity
40	Video signal recovered	Information
41	Video signal lost	Error
42	Disk access restored	Information
43	Disk access unauthorized	Warning
44	Alarm trigger rate normal	Information
45	Alarm trigger rate high	Warning
46	Directory started	Information
47	Directory stopped unexpectedly	Error
48	Directory stopped by user	Information
49	Remaining archive disk space normal	Information
50	Remaining archive disk space low	Warning
51	Live server monitoring restored	Information
52	Live server monitoring failed	Error
53	Directory failover: Main database recovered	Information
54	Directory failover: Main database lost	Error
55	Database restore succeeded	Information
56	Database restore failed	Error

About the Health Monitor role

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

Health events are recorded in a database for the purpose of reporting and statistical analysis. Current system errors are reported in real time in your application’s notification tray.

Only one instance of this role is permitted per system. It is created at system installation and cannot be deleted.

From the Heath Monitor role, you can choose which health events to monitor.

Resetting the Health Monitor database

After you initially set up your system, you should reset the health monitoring database to its original state.

What you should know

The process of setting up and configuring a system can generate many health events. It is normal that health errors and warnings are produced during this time. That is why it is important to restore the database to its original, clean state, so the health statistics of your system are reset.

To reset the Health Monitor database to its original state:

1. Open the **System** task, and click the **Roles** view.
2. Select the **Health Monitor** role, and click the **Resources** tab.
3. Click **Delete the database** (✖).
4. When prompted if you want to delete this database, click **Delete**.

   The **Database actions** window opens.
5. When you see confirmation that the database has been deleted, click **Clear finished**, and then click **Close**.
6. In the toolbar at the bottom of the workspace, click **Deactivate role** (🟠).
7. Click **Activate role** (🟢).

   After 15-30 seconds, a new *HealthMonitor* database should be created in the Health monitor role's **Resources** tab.

The health errors and warnings generated during the setup are deleted, and all health statistics are reset.

Selecting health events to monitor

You can configure the *Health Monitor* role to ignore certain health events, and change how it generates some health events.

What you should know

If you want to ignore all health events, deactivate the Health Monitor role completely. If you want to temporarily ignore an entity's health events because you are performing maintenance work on it, set it to maintenance mode.

IMPORTANT: Clearing a health event in the monitoring list does not remove it from the *Health history* query filter, but it could make some of the health statistics calculations impossible.

To select which health events to monitor:

1 Open the **System** task, and click the **Roles** view.

2 Select the **Health Monitor** role, and click the **Properties** tab.

3 Under **Events to monitor**, select or clear the desired events.

   Most health events come in pairs, such as *Database lost* and *Database recovered*. They can only be selected or ignored together.

4 Add criteria for generating the events, as follows:

   Criteria is only supported for some events. For example, you can configure the *CPU usage high* health event to only generate on servers whose CPU runs higher than 80% for a period of 10 seconds.

   a) Select the event to modify, and click **Edit** (✎) at the bottom of the list.
   b) In the event **details** window, adjust the values as required, and click **Save**.

5 Click **Apply**.

Related Topics
Viewing system health events on page 249

Setting entities in maintenance mode

If you are changing the configuration settings of an entity, such as a role, or must do work on the physical counterpart of the entity (maintenance on a video unit, intrusion detection unit, access control unit, or LPR unit), you can set the entity in *maintenance mode* so that the health statistics for that entity are not affected.

What you should know

Unexpected downtime (when an entity is unavailable) affects the health statistics of that entity. However, when an entity is in *maintenance mode*, the downtime is considered *expected* downtime, and is not used in calculating the availability of that entity.

NOTE: Setting an entity in maintenance mode does not stop the health events, but it reports all health events as information only.

You can set the following entities in maintenance mode: roles, video units, cameras, access control units, intrusion detection units, hardware zones, Patrollers, and LPR units.

You can also unlock a door for maintenance purposes from the door **Properties** tab.

To set an entity in maintenance mode:

1. Open the appropriate task in Config Tool.
2. Right-click the entity in the entity tree view, and click **Maintenance** (◆) > **Maintenance mode** (🚧).
3. In the *Maintenance mode* dialog box, click **Turn ON**.
4. Select how long you want to set the entity in maintenance mode for, from one of the following options:
   - **Indefinite:** No end date. You must manually turn off maintenance mode.
   - **Duration:** Maintenance mode is turned on for the number of days that you select.
   - **Specific end-time:** Maintenance mode is turned on until the date that you select.

   You can modify the duration while the entity is in maintenance mode.
5. In the **Reason** field, type the reason you are setting the entity in maintenance mode.
6. Click **Save**.

   Sometimes Federation™ role icons do not refresh right away. Press **F5** to refresh the entity tree.

   The entity is set to maintenance mode for the duration you specified. While the entity is in maintenance mode, the *Maintenance mode* icon (🚧) is displayed on the entity icon in the area view in Config Tool and Security Desk, as well as in Security Desk tiles and on maps when applicable. The reason the entity is in maintenance mode is shown when you hover over the entity icon in the area view and on maps.

Setting Security Center client applications in maintenance mode

If you are changing the configuration settings of your system, you can set all Security Center client applications (Security Desk, Config Tool, and Web Client) in *maintenance mode* so that the health statistics for your applications are not affected.

What you should know

Unexpected downtime (when an application is unavailable) affects the health statistics of that application. However, when an application is in *maintenance mode*, the downtime is considered *expected* downtime, and is not used in calculating the availability of that application.

NOTE: Setting an application in maintenance mode does not stop the health events, but it reports all health events as information only.

To set a Security Center client application in maintenance mode:

1 Open the **System** task, and click the **Roles** view.

2 Select the Health Monitor, and then click the **Properties** tab.

3 Switch the **Client app. maintenance mode** option to **ON**, and click **Apply**.

Viewing system messages

If you receive messages from the system, you can review them from the notification tray, and diagnose the trouble entities.

What you should know

You can receive three types of messages from the system:

- Health issues
- ⚠ Warnings
- ℹ Messages

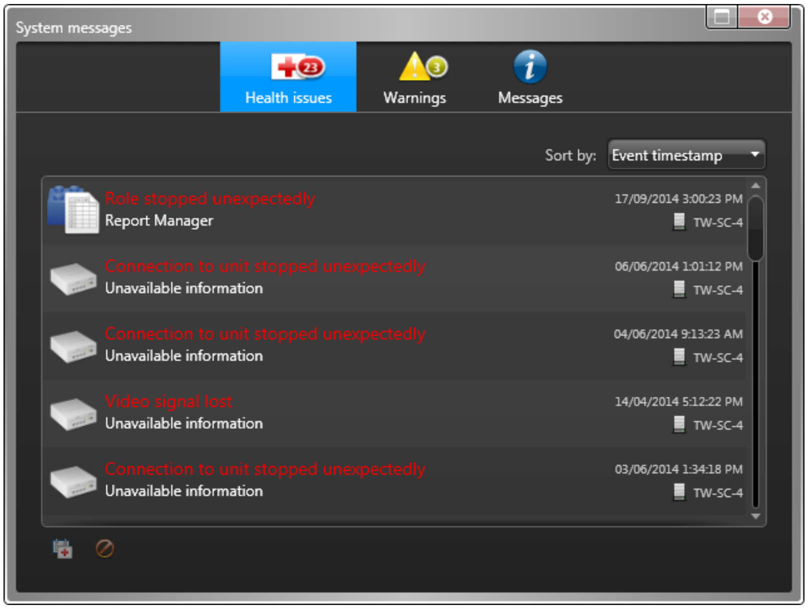
NOTE: System messages are not the same as health events related to entities. Health events can be health issues, but health issues are not necessarily health events.

To view system messages:

1 In the notification tray, double-click the **System messages** (6) icon.

2 In the *Health issues* tab of the *Notifications* dialog box, do one of the following:

- From the **Sort by** drop-down list, select how to display the health issues. You can sort them alphabetically by health event type, event timestamp, machine (computer name), or source (entity name).
- Click an entity to open its configuration pages, to diagnose the entity.
- Click in a row to launch a *Health history* task and view system health events.
- Click **Refresh** to update the content displayed in the *Health issues* tab.



Sort by: Event timestamp

Role stopped unexpectedly
Report Manager
17/09/2014 3:00:23 PM
TW-SC-4

Connection to unit stopped unexpectedly
Unavailable information
06/06/2014 1:01:12 PM
TW-SC-4

Connection to unit stopped unexpectedly
Unavailable information
04/06/2014 9:13:23 AM
TW-SC-4

Video signal lost
Unavailable information
14/04/2014 5:12:22 PM
TW-SC-4

Connection to unit stopped unexpectedly
Unavailable information
03/06/2014 1:34:18 PM
TW-SC-4

3 In the *Warnings* (⚠) tab, do one of the following:

- Click an entity to open its configuration pages. .
- Click **Details** (ℹ) to open the diagnostic window, which provides additional details about the warning.

  From this window you can save the warning as a text file, or click **Refresh** to rerun the diagnostic tests.

4 In the *Messages* (ℹ) tab, select a message, and do one of the following:
   - Click **Copy to clipboard** to copy the selected message to the clipboard.
   - Click **Clear all** to delete the selected messages.
   - Click **Clear all** to clear all messages.

5 Click ⊗ to close the *Notifications* dialog box.

Related Topics
Viewing system health events on page 249
Troubleshooting: entities on page 68

Viewing system health events

You can view system health events related to selected entities within a specified time range, using the *Health history* report.

What you should know

There are three severity levels of health events:

- Error
- Warning
- Information

Almost every entity in your system can generate health events. You can choose which health events to monitor by configuring the *Health Monitor* role. .

For example, if an entity is experiencing issues, you can search for past health events that have occurred in relation to that entity. If you want to search if there were critical errors that happened in the system during the last week, you can filter you search only for errors, and set a time range.

NOTE: Health events also appear in the notification tray as system messages (✚6) as they occur in real time.

To view system health events related to an entity:

1 From the home page, open the **Health history** task.

2 Set up the query filters for your report. Choose one or more of the following filters:

- **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
- **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the last week or the last month.
- **Health event:** Name of the health event.
- **Health severity:**

  Severity level of the health event:

  - ⓘ Information
  - ⚠ Warning
  - ❗ Error
- **Machine:** Select a computer that was having health issues to investigate.
- **Source entity:** Source entity of the event.
- **Source group:** Source entity group of the event. Usually a role or a unit.

3 To restrict the search to current health events only, click the **Show current health events** heading.

When the heading is enabled, it appears as **On** ●.

4 Click **Generate report**.

The health events of the selected entities are listed in the report pane.

Related Topics

Selecting health events to monitor on page 244
Viewing system messages on page 247

Report pane columns for the Health history task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Description:** Description of the event, activity, entity, or incident.
- **Error Number:** Identification number of the health error.
- **Event timestamp:** Date and time that the event occurred.
- **Health event:** Name of the health event.
- **IP address:** IP address of the unit or computer that generated the event.
- **Machine:** Computer where the health event occurred.
- **Occurrence count:** Number of times this health event occurred on the selected entity.
- **Physical address:** The MAC address of the equipment's network interface.
- **Severity:**

  Severity level of the health event:

  - ℹ Information
  - ⚠ Warning
  - ❗ Error
- **Source:** Source entity associated to the alarm or event.

Viewing the health status and availability of entities

You can monitor the overall health of your system, using the *Health statistics* report.

What you should know

By monitoring the health and availability of certain resources such as server roles, video units, door controllers, intrusion detection panels, and so on, you can identify instabilities, and even prevent critical system failures.

One of the important fields in the Health statistics report is the *Availability* of a given entity. Availability is expressed as a percentage.

To view the health status and availability of an entity:

1 Open the **Health statistics** task.

2 Set up the query filters for your report. Choose one or more of the following filters:

- **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
- **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the last week or the last month.
- **Source entity:** Source entity of the event.
- **Source group:** Source entity group of the event. Usually a role or a unit.

3 Click **Generate report**.

The health statistics for the selected entities are listed in the report pane. If health statistics could not be calculated for a given role or entity, the reason is shown in the *Calculation status* column of the report pane:

- **One or more events used to calculate availability are currently disabled:** The system administrator needs to select which health events to monitor by configuring the Health monitor role. .
- **One or more servers from the system are offline:** The server hosting the selected role is offline, therefore, the health statistics cannot be calculated for the role.

Example

A door controller called *Gym* was down four times over the last week, producing 90.72% availability. From the report results, you can see that this door controller is a potential concern, and have a maintenance crew come and look at the door.

Report pane columns for the Health statistics task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Availability:** The percentage of time available for a given entity.
- **Calculation Status:** If health statistics area unavailable, the reason is shown here.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.

- **Expected down-time:** How many days/hours/minutes the entity has been offline or unavailable through user intent or *Maintenance* mode. For example, deactivating a server role, or disconnecting a client application causes expected down-time. Expected down-time is never used in the *Availability* percentage calculation.
- **Failures:** How many failures have occurred.
- **MTBF:** Mean time between failures (in hours).
- **MTTR:** Mean time to recovery (in hours).
- **RTP packet lost high:** The number of *Real-time Transport Protocol* packets lost.
- **Source:** Source entity associated to the alarm or event.
- **Unexpected downtime:** How many days/hours/minutes the entity has been offline or unavailable after not having been set in *Maintenance mode*. Unexpected down-time is not caused by user intent.
- **Up-time:** How many days/hours/minutes the entity has been online and available.

Monitoring your computer resources

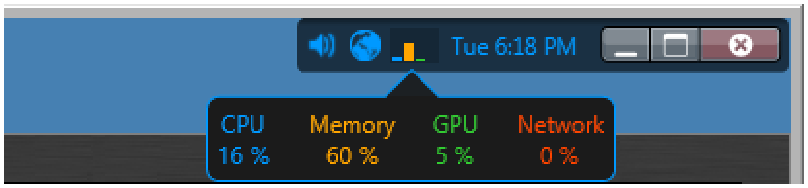
You can monitor the usage percentage of your computer resources by hovering the mouse pointer over the **Resources meter** icon in the notification tray. Click the same icon to view a summary of the hardware installed on your computer and their current use in a dialog box.

What you should know

If you do not see the **Resources meter** icon () in the notification tray, set its display property to **Show**.

To monitor the resources on your computer:

1 Hover your mouse pointer over the **Resources meter** icon in the notification tray to view the current usage of your computer resources in percentages.



CPU	Memory	GPU	Network
16 %	60 %	5 %	0 %

The usage of your computer resources is shown in four categories:

- CPU (blue)
- Memory (oange)
- GPU (green)
- Network (red)

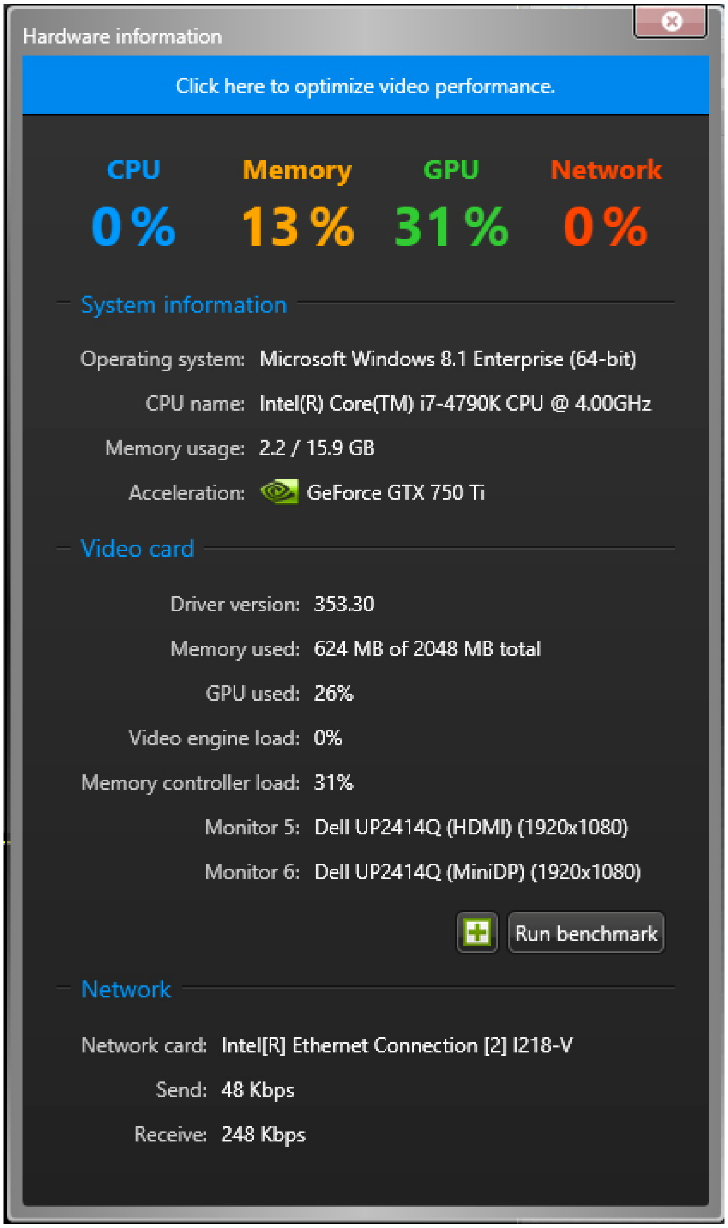
NOTE: The GPU (Graphic Processing Unit) is shown only if your video card supports hardware acceleration and if that feature is turned on in the Security Desk video options. See *Video options* in the *Security Desk User Guide*.

2 Click the **Resources meter** icon in the notification tray to view detailed information about your computer resources in the Hardware information dialog box.

Hardware information dialog box

The Hardware information dialog box gives you a summary of the hardware components detected on your computer as well as their current usage percentage. You can also run the hardware benchmark tool from the Hardware information dialog box.

When performance doesn't match your expectation, use this information to find out which aspect of your system is causing the bottleneck. If your video card has reached its limits, display less video streams.



CPU 0 %

Memory 13 %

GPU 31 %

Network 0 %

System information

Operating system: Microsoft Windows 8.1 Enterprise (64-bit)

CPU name: Intel(R) Core(TM) i7-4790K CPU @ 4.00GHz

Memory usage: 2.2 / 15.9 GB

Acceleration: GeForce GTX 750 Ti

Video card

Driver version: 353.30

Memory used: 624 MB of 2048 MB total

GPU used: 26%

Video engine load: 0%

Memory controller load: 31%

Monitor 5: Dell UP2414Q (HDMI) (1920x1080)

Monitor 6: Dell UP2414Q (MiniDP) (1920x1080)

Network

Network card: Intel[R] Ethernet Connection [2] I218-V

Send: 48 Kbps

Receive: 248 Kbps

Video card information is not available if you are connected to your computer through remote desktop.

The GPU (Graphic Processing Unit) usage percentage is shown only if your video card supports hardware acceleration and if that feature is turned on in the Security Desk video options. If your computer has multiple video cards, click the **Acceleration** drop-down list to pick the one you want to monitor. For information about enabling the *Hardware acceleration* feature, see the *Security Desk User Guide*.

For more information about running the hardware benchmark tool, see Using the hardware benchmark tool on page 255.

Related Topics

Troubleshooting: Hardware acceleration issues on page 467

Using the hardware benchmark tool

The hardware benchmark tool enables you to calibrate your settings to optimize the performance of your installed video cards. You can run the hardware benchmark tool in Config Tool or Security Desk.

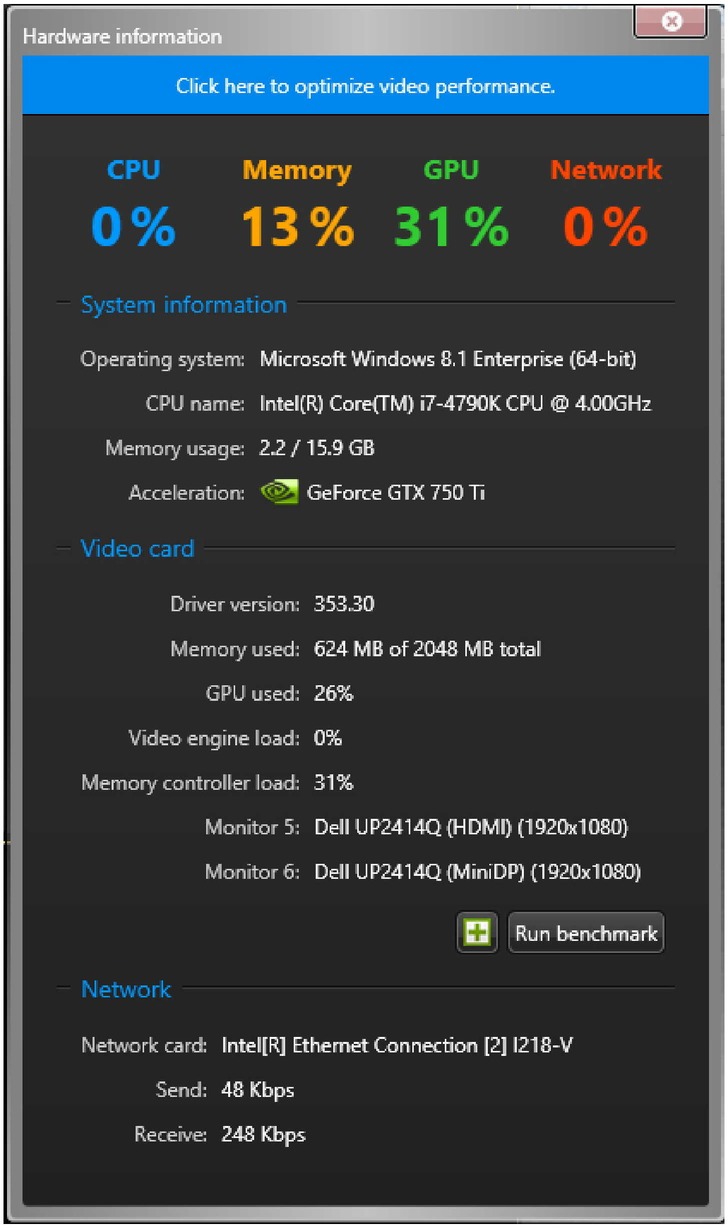
What you should know

- You are prompted to run the hardware benchmark tool the first time you start Security Desk. There is also a yellow warning icon that appears on the notification tray whenever you change your video card configuration. There are no prompts in Config Tool.
- Running the benchmark tool is GPU intensive. Close all other tasks and applications when performing a benchmark test to ensure you get valid results.
- For best results, make sure your GPU drivers are up to date before running the hardware benchmark tool.

To use the hardware benchmark tool:

1 Hover your mouse pointer over the **Resources meter** icon in the notification tray.

The **Hardware information** dialog box opens:



System information

Operating system: Microsoft Windows 8.1 Enterprise (64-bit)

CPU name: Intel(R) Core(TM) i7-4790K CPU @ 4.00GHz

Memory usage: 2.2 / 15.9 GB

Acceleration: GeForce GTX 750 Ti

Video card

Driver version: 353.30

Memory used: 624 MB of 2048 MB total

GPU used: 26%

Video engine load: 0%

Memory controller load: 31%

Monitor 5: Dell UP2414Q (HDMI) (1920x1080)

Monitor 6: Dell UP2414Q (MiniDP) (1920x1080)

Network

Network card: Intel[R] Ethernet Connection [2] I218-V

Send: 48 Kbps

Receive: 248 Kbps

2 From the **Acceleration** drop-down list, select the video card you want to run the benchmark test on.

3 Click **Run benchmark**.

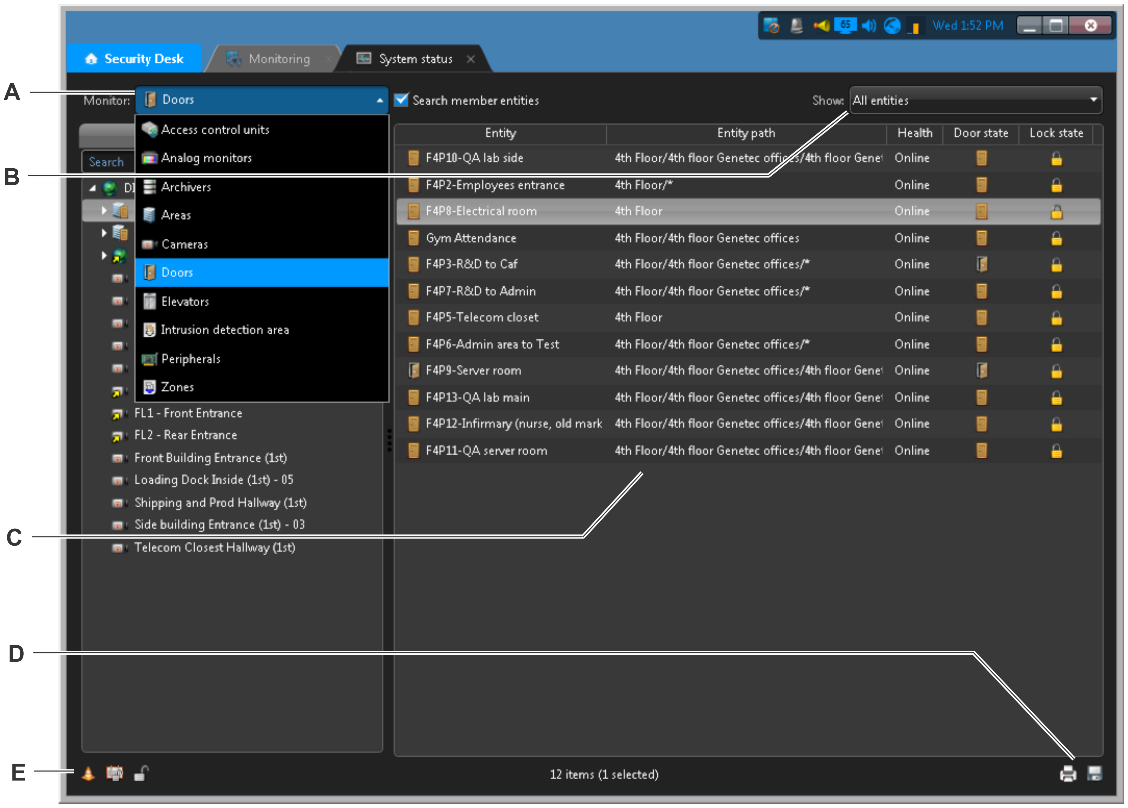
Once the benchmark test is complete, the **Frame rate** capability of the selected card is listed.

4 Click **Close**.

Overview of the System status task

Use the System status task to monitor the current status of different types of entities and investigate health issues they might have.

The following figure shows the System status task.



Monitor: Doors

☑ Search member entities

Show: All entities

Entity	Entity path	Health	Door state	Lock state
F4P10-QA lab side	4th Floor/4th floor Genetec offices/4th floor Genet	Online	🚪	🔒
F4P2-Employees entrance	4th Floor/*	Online	🚪	🔒
F4P8-Electrical room	4th Floor	Online	🚪	🔒
Gym Attendance	4th Floor/4th floor Genetec offices	Online	🚪	🔒
F4P3-R&D to Caf	4th Floor/4th floor Genetec offices/*	Online	🚪	🔒
F4P7-R&D to Admin	4th Floor/4th floor Genetec offices/*	Online	🚪	🔒
F4P5-Telecom closet	4th Floor	Online	🚪	🔒
F4P6-Admin area to Test	4th Floor/4th floor Genetec offices/*	Online	🚪	🔒
F4P9-Server room	4th Floor/4th floor Genetec offices/4th floor Genet	Online	🚪	🔒
F4P13-QA lab main	4th Floor/4th floor Genetec offices/4th floor Genet	Online	🚪	🔒
F4P12-Infirmary (nurse, old mark	4th Floor/4th floor Genetec offices/4th floor Genet	Online	🚪	🔒
F4P11-QA server room	4th Floor/4th floor Genetec offices/4th floor Genet	Online	🚪	🔒

12 items (1 selected)

A	Entity types you can monitor.
B	Type of issues that you can monitor.
C	The entity statuses are listed in the report pane.
D	print or Export the report.
E	Entity-specific commands.

System status task columns

In the System status task, you can monitor the current status of different types of entities and investigate the health issues that they might have.

The following table lists the columns that are displayed for each entity type in the **Monitor** drop-down list.

Entity	Column	Description
Access control units	Entity	Unit name

Entity	Column	Description
	Health	Online, Offline, or Warning
	IP address	IP address of the unit
	Sync	Synchronization status
	AC fail	Yes (✓) or No (blank)
	Battery fail	Yes (✓) or No (blank)
	Firmware	Firmware version of the unit
	Tampered	Indicates whether the unit has been tampered with Yes (✓) or No (blank)
	Maintenance	Indicates if the access control unit is currently in maintenance mode, and the duration of the maintenance mode
Analog monitors	Entity	Analog monitor name
	Entity path	List of all parent areas, starting from the system entity. If the analog monitor has multiple parent areas, "*|" is shown as the path
	Health	Online, Offline, or Warning
	Connected entity	Name of the cameras currently displayed in the analog monitor
Applications	Entity	Type of application (Config Tool or Security Desk)
	Source	Machine it is running on
	Username	Name of the user who is connected
	Version	Software version of the client application
Areas	Entity	Area name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
	Threat level	Indicates if a threat level is currently activated on the selected area, along with the threat level name. If no threat level is set, the column is blank
	Security clearance	(Only visible to administrative users) Indicates the minimum security clearance level required from cardholders to access this area, on top of the restrictions imposed by the access rules

Entity	Column	Description
	People count	Working (✓) or Not working (blank)
	Antipassback	Hard, Soft, or None (no *antipassback*)
	Interlock	Working (✓) or Not working (blank)
	Priority	*Interlock* input priority: Lockdown or Override
Archivers	Entity	Archiver name
	Servers	List of servers assigned to host this role
	Active cameras	Number of cameras that are currently active
	Archiving cameras	Number of cameras that have archiving enabled
	Used space	Amount of space used on the disk
	Archiving disk space usage	Percentage of space used on the disk
	Archiver receiving rate	Rate at which the Archiver is receiving data
	Archiver writing rate	Rate at which the Archiver is writing to disk
	Maintenance	Indicates if the Archiver is currently in maintenance mode, and states the duration of the maintenance mode
Cameras	Entity	Camera name
	Entity path	List of all parent areas, starting from the system entity. If a camera has multiple parent areas, “*|” is shown as the path
	Health	Online, Offline, or Warning
	Recording	Recording state
	Analog signal	Lost, Available, or Unknown (*IP cameras*)
	Blocked	Indicates if the camera is currently blocked from some users. Blocked (✓), or not blocked (blank)
	Maintenance	Indicates if the camera is currently in maintenance mode, and states the duration of the maintenance mode
Doors	Entity	Door name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning

Entity	Column	Description
	Door state	Open (🚪) or closed (🚪)
	Lock state	Locked (🔒) or unlocked (🔓)
Elevators	Entity	Elevator name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
Health issues	Entity type	Icon representing the entity type
	Entity	Entity name
	Source	For a local entity, shows the server it is running on. For a *federated entity*, shows the Federation™ role name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
	Maintenance	Indicates if the entity is currently in maintenance mode, and states the duration of the maintenance mode
Intrusion detection areas	Entity	Intrusion detection area name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
	Alarm state	Active, normal
	Arming state	*Master armed*, *Perimeter armed*, Disarmed (ready to arm), Disarmed (not ready), Disarmed (input trouble), Arming, or Armed (Alarm active)
	Bypass	Active/inactive (represented by an icon)
	Trouble	Yes (✓) or No (blank)
Intrusion detection units	Entity	Intrusion detection unit name
	Health	Online, Offline, or Warning
	AC fail	Yes (✓) or No (blank)
	Battery fail	Yes (✓) or No (blank)
	Tamper	Yes (✓) or No (blank)
	Maintenance	Indicates if the intrusion detection unit is currently in maintenance mode, and states the duration of the maintenance mode

Entity	Column	Description
Macros	Entity	Macro name
	Start time	Time the macro was started
	Instigator	Name of the user who started the macro
Peripherals	Name	Peripheral name
	Type	In (Input), Out (Output), Reader
	State	Normal, Active, or Shunted (inputs and readers)
	Additional info	Settings specific to the type of peripheral
	Controlling	Entity controlled by the peripheral.
	Health	Online, Offline, or Warning
	Logical ID	Logical ID assigned to the peripheral
	Physical name	Peripheral name assigned by the system
Roles	Entity	Role name
	Health	Online, Offline, or Warning
	Current server	Name of server currently hosting the role
	Servers	List of servers assigned to host this role
	Version	Software version of role
	Status	Activated (🟢) or Deactivated (🟠)
	Maintenance	Indicates if the role is currently in maintenance mode, and states the duration of the maintenance mode
Routes	Route	Route name, showing the two networks it joins
	Current configuration	*Unicast TCP*, Unicast *UDP*, or *Multicast*
	Detected capabilities	Unicast TCP, Unicast UDP, or Multicast **NOTE:** A *Redirector* is required on each network to be able to detect the capabilitie.
	Status	OK, or warning message stating the reason of the problem **NOTE:** A *Redirector* is required on each network to be able to display the status
Servers	Entity	Server name

Entity	Column	Description
	Health	Online, Offline, or Warning
	Roles	Roles assigned to this server
	Certificate	Indicates whether the server has a current *identity certificate*, and the validity period of the current certificate
	Maintenance	Indicates if the server is currently in maintenance mode, and states the duration of the maintenance mode
Zones	Entity	Zone name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
	State	Normal, Active, or Trouble
	Armed	Indicates if the zone is armed or not
	Maintenance	Indicates if the hardware zone is currently in maintenance mode, and states the duration of the maintenance mode

Monitoring the status of your Security Center system

You can monitor the current status of different types of entities, and investigate health issues they might have, using the *System status* report.

What you should know

Use the System status report to monitor your system. For example, if you have a camera that is not working, you can select the camera entity in the *System status* task, and then diagnose why it is offline. From the *System status* task, you can also launch the *Health history* task and generate a health report to investigate further.

When monitoring *Routes*, a *Redirector* must be configured on each network to be able to detect the network capabilities and display the current status.

To monitor the status of your system:

1 Open the *System status* task.

2 From the **Monitor** drop-down list, select one of the following:
- Access control units
- Analog monitors
- Applications (only administrators)
- Areas
- Archivers
- Cameras
- Cash registers
- Doors
- Elevators
- Health issues
- Intrusion detection area
- Intrusion detection units (only administrators)
- Macros (only administrators)
- Peripherals
- Roles (only administrators)
- Routes (only administrators)
- Servers (only administrators)
- Zones

3 If required, select an area in the *Selector*.

4 To search for entities within nested areas, select the **Search member entities** option.

The related entities, roles, applications, and items are listed in the report pane.

5 (Optional) Do one of the following, depending on the selected entity:
- To launch a *Health history* report, click 📋.
- To troubleshoot the selected entity, click ✚.
- To print the report, click 🖨.
- To change the configuration of an entity, right-click the entity in the report pane, and click **Configure entity** (⚙).
- To save the report, click 💾.

Related Topics

System status task columns on page 257
Viewing system health events on page 249
Troubleshooting: entities on page 68

14

System audits

This section includes the following topics:

Investigating user related activity on the system

You can view all user activity related to video, access control, and LPR, using the *Activity trails* report.

Before you begin

To receive results in the Activity trails report, you must already be monitoring user activity. You can select which activities to monitor and record in the database from the System task

What you should know

For example, you can use the *Activity trails* task to find out who played back which video recordings, who blocked a camera, who activated a threat level, who requested a credential badge to be printed, who used the *Hotlist and permit editor* task, or who enabled hotlist filtering.

To investigate user related activity on the system:

1. From the home page, open the **Activity trails** task.
2. In the **Activities** filter, select which of the following activities you want to investigate:
   - Access control:
     - **Access control unit rebooted (manually):** Who manually rebooted an access control unit.
     - **Access control unit synchronization started (manually):** Who manually started an access control unit synchronization.
     - **Antipassback violation forgiven:** Who forgave an antipassback violation.
     - **Badge printed:** Who printed a credential badge.
     - **Credential requested:** Who requested a credential badge to be printed, and why.
     - **Credential request canceled/completed:** Who completed or canceled a credential badge print request.
     - **Device shunted:** Who shunted (disabled) an access control device.
     - **Door maintenance mode set/canceled:** Who unlocked a door by setting it in maintenance mode, or who canceled the maintenance mode on a door.
     - **Door unlocked (manually):** Who manually unlocked a door.
     - **Door unlock schedule overridden (lock/unlock):** Who overrode the lock or unlock schedule of a door.
     - **Door unlock schedule override canceled:** Who canceled the unlock schedule override of a door.
   - Events:
     - **PTZ activated/locked:** Who activated/locked the PTZ commands and on which camera.
     - **PTZ zoom started/stopped:** Who started/stopped zooming in/out, and on which camera.
   - General:
     - **Alarm acknowledged/forcibly acknowledged:** Who acknowledged or forcibly acknowledged an active alarm.
     - **Alarm forwarded/snoozed:** Who forwarded or snoozed an active alarm.
     - **Alarm triggered (manually):** Who manually triggered an alarm.
     - **All alarms forcibly acknowledged:** Who forcibly acknowledged all active alarms.
     - **Connected to remote Security Desk:** Who connected to a remote Security Desk workstation.
     - **Disconnected from remote Security Desk:** Who disconnected from a remote Security Desk workstation.
     - **Intrusion alarm triggered:** Who manually triggered an intrusion alarm.

    - **Intrusion detection area disarmed:** Who disarmed an intrusion detection area.
    - **Intrusion detection area master/perimeter armed:** Who master or permimeter armed an intrusion detection area.
    - **Output triggered (manually):** Who triggered an output pin (for example, using a hot action).
    - **Report exported/generated:** Who exported or generated which reports.
    - **Report printed:** Who printed a report.
    - **Threat level set/cleared:** Who set or cleared a threat level, and on which area or system.
    - **User logged on/off:** Who logged on or off of which Security Center client application.
    - **Zone armed/disarmed:** Who armed or disarmed a zone.
  - LPR:
    - **Application updated:** Who updated a Patroller or a Sharp unit.
    - **Hotlist or permit list edited:** Who loaded a hotlist or permit list, or added, modified, or deleted license plates in the list.
    - **Photo evidence report printed (Hits/Reads):** Who printed a hits/reads evidence report.
    - **Plate filtering enabled:** Which LPR Manager role has plate filtering enabled.
    - **Read edited/triggered:** Who edited/triggered a license plate read.
    - **Read/hit protected:** Who protected a license plate read or hit.
    - **Read/hit unprotected:** Who unprotected a license plate read or hit.
  - Video:
    - **Archive backup started/stopped (manually):** Who manually started or stopped video from being backed up from an Archiver.
    - **Archive duplication started/stopped (manually):** Who started or stopped video from being duplicated from one Archiver to another.
    - **Archive restore started/stopped (manually):** Who started or stopped video archive from being restored to an Archiver.
    - **Archive retrieval from units started/stopped (manually):** Who started or stopped transferring video from video units to an Archiver.
    - **Bookmark deleted/modified:** Who deleted or modified a bookmark.
    - **Camera blocked/unblocked:** Who blocked or unblocked a camera.
    - **Connected/Disconnected to/from analog monitor:** Who connected to or disconnected from an analog monitor.
    - **Live streaming started/stopped:** Which camera was displayed or removed.
    - **Playback streaming started:** Which recording was played.
    - **PTZ command sent:** What did the user do with the PTZ.
    - **Snapshot printed/saved:** Who printed or saved a snapshot.
    - **Video exported:** What did the user export and where did they save it.
    - **Video file deleted (manually):** Who deleted a video file from the system.
    - **Video file protected/unprotected:** Who started or stopped protection on a video file.
    - **Video stream not delivered:** Whose video request was terminated without having a single frame being rendered.
    - **Video unit identified/rebooted/reconnected:** Who identified/rebooted/reconnected a video unit.
    - **Visual tracking enabled/disabled:** Who enabled or disabled *visual tracking* in a tile.

3. Set up the other query filters for the report. Choose from one or more of the following filters:
   - **Application:** Which client application was used for the activity.

  - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the last week or the last month.
  - **Events:** Select the events of interest. The event types available depend on the task you are using.
  - **Impacted:** The entities that were impacted by this activity.
  - **Initiator:** User or role responsible for the activity.

4. Click **Generate report**.

   The activity results are listed in the report pane.

Report pane columns for the Activity trails task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Initiator:** Who or what role performed the activity.
- **Initiator type:** The type of entity that initiated the activity.
- **Activity name:** Type of activity.
- **Description:** Description of the event, activity, entity, or incident.
- **Impacted entity:** Which entities were impacted by this activity.
- **Impacted entity type:** The type of entity impacted by this activity.
- **Initiator machine:** Which computer the activity was performed on.
- **Initiator application:** The application used for this activity.
- **Event timestamp:** Date and time that the event occurred.
- **Impacted entity version:** The version number of the entity impacted by this activity. This field is empty if the impacted entity is not a role.
- **Initiator application version:** The version number of the application. This field is empty if the activity is initiated by a role entity.
- **Initiator version:** The version number of the initiator. This field is empty if the activity is initiated by a user.

Finding out what changes were made to the system configuration

You can find out what configuration changes were made on the system, who made them, when, and on which entity settings (before and after values), using the *Audit trails* report.

What you should know

The Audit trails report is helpful if you see that the properties of an entity have changed and you must find out who made those changes and when (for example, if the recording mode of a camera has been modified). Also, if you requested an update for an entity (for example, the privileges for a user), you can check to see if the changes have been made from Config Tool.

To find out what changes are made to the system configuration:

1. From the home page, open the *Audit trails* task.
2. Set up the query filters for the report. Choose from one or more of the following filters:
   - **Application:** Which client application was used for the activity.
   - **Entities:** Select the entities you want to investigate. You can filter the entities by name and by type.
   - **Modification time:** Entities modified within the specified time range.
   - **Modified by:** User or role responsible for the entity modification.
3. Click **Generate report**.

   The description of the changes (before and after values) to the selected entities, as well as who made those modifications and when, are listed in the report pane.

Report pane columns for the Audit trails task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Entity:** Name of the entity affected by the modification.
- **Entity type:** Type of entity affected by the modification.
- **Description:** The description of the entity modification.
- **Initiator:** Who or what role made entity modification.
- **Initiator type:** The type of entity initiating the entity modifications.
- **Initiator machine:** The computer used to make the change.
- **Initiator application:** The application used to make the change.
- **Initiator application version:** The version number of the application. This field is empty if the activity is initiated by a role entity.
- **Modification time:** Time the entity was last modified.

Configuration changes logged by the Security Center system

All configuration changes are logged by the system. You can investigate those changes with the *Audit trails* report.

The following table outlines the change descriptions you can expect from the *Audit trails* report.

Modification type	Description
Entity creations	Entity created: <*Entity name at creation*>.
Entity deletions	Entity deleted: <*Entity name at deletion*>.
Membership modifications	• <*Entity*> is now a member of <*Group entity*>. • <*Entity*> is no longer a member of <*Group entity*>. **NOTE:** <Group entity> can be an area, a partition, a cardholder group, or a user group.
Access rights modifications	• <*User/User group*> gained access rights to <*Partition*>. • <*User/User group*> lost access rights to <*Partition*>. • <*User/User group*> is now partition administrator of <*Partition*>. • <*User/User group*> is no longer partition administrator of <*Partition*>.
Privilege modifications	Value of <*Privilege*> changed from <*Old value*> to <*New value*>.
Property modifications	Value of <*Property*> changed from <*Old value*> to <*New value*>. **NOTE:** Not all property modifications are described with before and after values. For the exact list of properties that show this level of details, see Property changes logged with the before and after values on page 271.
Role activations/deactivations	Value of Active state changed from <*Old value*> to <*New value*>.
Map modifications	• <*Entity*> has been added as a link to map <*Map entity*>. • <*Entity*> has been removed as a link from map <*Map entity*>. • <*Entity*> setting modified. • <*Camera entity*> setting modified to Motion on/off. • <*Camera entity*> setting modified to Recording on/off. • <*Zone entity*> state settings modified. • Map layers added/removed (<*layer(s)*>) • Georeference modified. • Default view modified. • Background modified.

Property changes logged with the before and after values

Most property modifications logged by the system are described with before and after values.

The following table lists all property modifications logged with the before and after values, ordered by entity type. Changes that are not explicitly listed in this table are logged with the generic description *Properties modified*.

Entity type	Configuration tab	Changes described with before and after values
All entity types	Identity	Name Description Logical ID Relationships • Actions • Partition membership • All other specific relationships
All unit types	Location	All properties
Access control unit	All tabs	All properties (except peripheral settings)
Access Manager (role)	All tabs	All properties
Access rule	All tabs	All properties
Active Directory (role)	All tabs	All properties
Active Directory Federation Service (role)	All tabs	All properties
Alarm	All tabs	All properties
Area	Properties	All properties
	Advanced	All properties (except door setttings: perimeter or captive)

Entity type	Configuration tab	Changes described with before and after values
Archiver (role)	Camera default settings	Recording • Recording modes (Schedule and Mode) • Record audio • Record metadata • Redundant archiving • Automatic cleanup • Retention period • Time to record before an event • Time to record after a motion • Default manual recording length Encryption • On/Off • Certificates
	Resources	Advanced settings • Video wartermarking • Delete oldest files when disks are full • Enable edge playback requests • Enable thumbnails requests • Protected video threshold • Disk load warning threshold • Max archive transfer throughput • Video files • Maximum length • Maximum size
Badge template	All tabs	All properties

Entity type	Configuration tab	Changes described with before and after values
Camera	Video	Video quality • Schedule • Resolution • Constant bit rate • Bit rate • Maximum allowed bit rate • Image quality • Frame rate • Key frame interval • Key frame interval measure (seconds/images) • Bit rate priority • Recording frame rate • All specific compression settings from manufacturers Stream usage Network settings • Connection type • Multicast address and port Boost quality on manual recording • On/Off • Compression settings for manual recording (same as Video quality) Boost quality on event recording • On/Off • Compression settings for manual recording (same as Video quality)
	Recording	Recording • Inherit from Archiver/Custom settings • Recording modes (Schedule and Mode) • Record audio • Record metadata • Redundant archiving • Automatic cleanup • Retention period • Time to record before an event • Time to record after a motion • Default manual recording length Encryption • On/Off • Certificates

Entity type	Configuration tab	Changes described with before and after values
	Motion detection	Schedule On/Off Software/Unit motion detection Sensitivity Consecutive frame hits Motion zones • Add/remove • Motion mask • Motion on threshold • Motion on event • Motion of threshold • Motion off event • Sensitivity • Motion mask
Cardholder	All tabs	All properties
Credential	All tabs	All properties
Directory Manager (role)	All tabs	All properties
Federation (roles)	All tabs	All properties
Health Monitor (role)	All tabs	All properties
Hotlist	Properties	Priority Hotlist path
	Advanced	All properties
LPR (task)	General settings	All settings
LPR Manager (role)	Properties	General settings - All settings Live - All settings File association - All settings Matching - All settings Geocoding - All settings Plate filtering - All settings Email notification - All settings XML import - All settings XML export - All settings Update provider - All settings

Entity type	Configuration tab	Changes described with before and after values
Map Manager (role)	Resources	All properties
Overtime rule	Properties	All properties
Parking facility	Properties	All properties
Partition	Properties	All properties
Patroller	Properties	All properties
Permit	Properties	Permit path
	Advanced	All properties
Permit restrictions	Properties	All properties
Report Manager (role)	All tabs	All properties
User	Properties	Status Personal information - All settings Password settings • Expiration (in days) • Change on next logon User level PTZ override
	Advanced	Logon settings - All settings Security Desk settings - All settings Limit archive viewing
User group	Properties	• Email address • User level • PTZ override • Members
	Advanced	Logon settings - All settings Security Desk settings - All settings Limit archive viewing
Zone Manager (role)	All tabs	All properties
Visitor	All tabs	All properties

Part III

System security

This part includes the following chapters:

15

Introduction to system security

This section includes the following topics:

Defining who can access Security Center

When determining who is able to access Security Center, you should define the partitions (what the boundaries are), and then select the user groups and individual users who can access those partitions.

What you should know

While Security Center protects your company's assets (buildings, equipment, important data collected in the fields, etc), your job as administrator is to protect the Security Center software against illegal access.

When securing access to your software, you should ask the three following questions:

- Who uses the system? (which users and user groups can log on)
- What do they use it for? (what privileges do the users have)
- What parts of the system are they allowed to access? (which partitions can the users access)

It is easier to define security partitions when you first set up your system. That way, as you create entities your system, you can place them directly into the partitions where they belong. If you start by creating users first, you might end up having to revisit their access rights every time you add a new partition to your system.

To define who can access Security Center:

1 Decide whether partitions are helpful in your situation.

2 If partitions are helpful, identify the parts of your system that are relatively independent of each other, and create a partition for each part.

   Example: If your system covers multiple sites, and if the security staff at each site work independently of the other sites, then create a partition for each site.

3 Identify the groups of users who share the same roles and responsibilities, create a user group for each.

   Example: All security operators can form one group, and all investigators can form another group.

4 If you have subgroups working on different partitions, define a user group to represent each subgroup, add them as members of the larger user group, and assign them to their corresponding partitions.

   Each individual subgroup would be allowed to access a different partition. In this situation, the purpose of the parent user groups is to separate the users according to their roles and responsibilities. The purpose of the child user groups is to further separate users based on what they can access in the system.

   Depending on whether you want the user management to be centralized or decentralized, each individual subgroup can belong to the same partition as their parent user group, managed by the same partition administrator, or can belong to different partitions, managed by different partition administrators.

5 Define the individual users and add them as members of the user groups.

   BEST PRACTICE: Try to add the users as members of the smallest group. Let each user inherit everything from the parent user group, and only resort to configuring them individually for exceptions.

Protecting your data center against outside threats

If the security policy of your company requires all corporate databases to reside on a secured network, you must create *Directory gateways* to allow the Security Center applications located outside the secured network to log on to the system.

Before you begin

Make sure that the *Number of additional Directory servers* supported by your Security Center license allows you to add the Directory gateways you need to create. The Directory gateways are counted as *Directory servers* in your Security Center license.

What you should know

All Security Center applications (roles and client applications) must connect to a Directory server in order to log on to the system. All Directory servers must access the Directory database where the system configuration is stored. If the Directory database resides on a secured network, no applications located outside the secured network are allowed to access it. To avoid violating the security policy, you must create Directory gateways on the non-secured network.

To create Directory gateways:

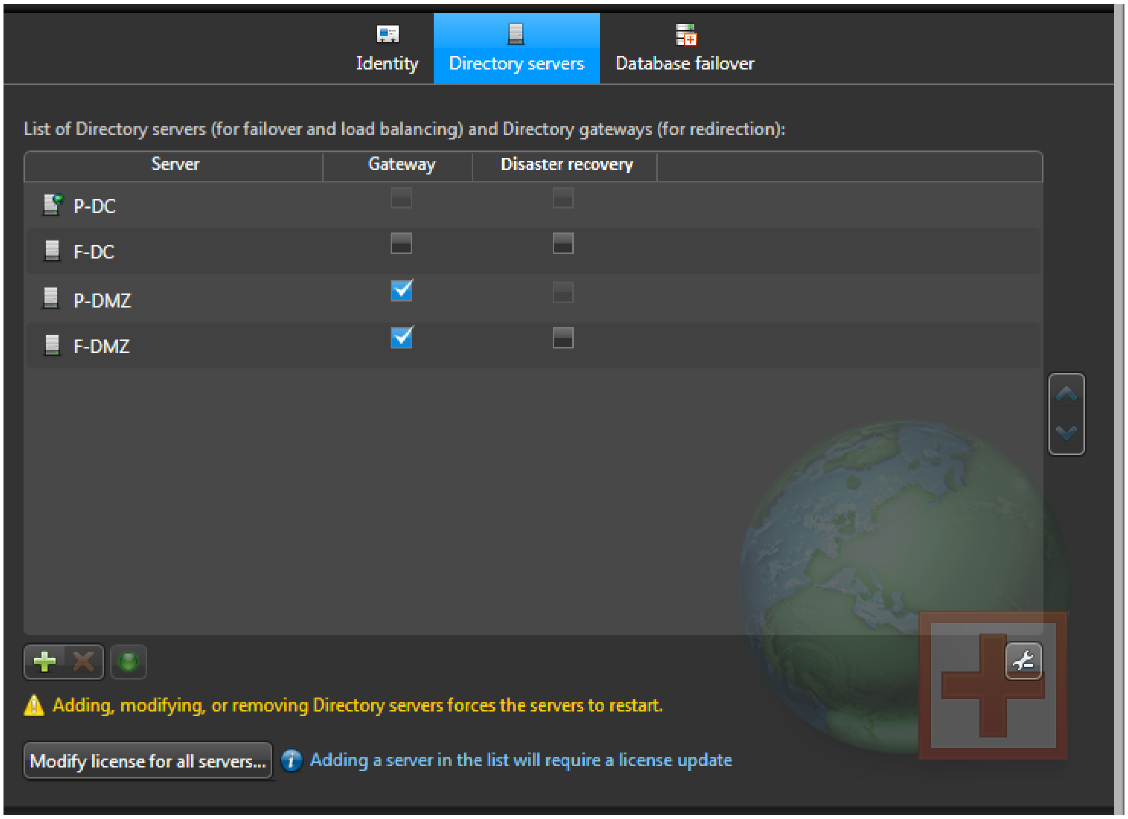
1. From the Config Tool home page, open the *System* task, and click the **Roles** view.
2. Select the **Directory Manager** (🌐) role, and then click **Directory servers** tab.
3. At the bottom of the server list, click **Advanced** (⚙).

   An extra column, **Gateway**, appears in the list.
4. At the bottom of the list, click **Add an item** (✚).
5. In the dialog box that appears, select the server you want to add, and click **Add**.
6. Add more servers to the list if necessary.
7. Select the **Gateway** option on servers you want to use as Directory gateways.

   A Directory gateway must be located on the non-secured network. It does not need to access the Directory database, but needs to connect to the main server. The following example shows a system with two Directory servers (one of which is the main server) and two Directory gateways.

   NOTE:

   - *Load balancing* only occurs between servers of the same type. All Directory servers belong to one load balancing pool, and all Directory gateways belong to another. A user trying to connect to a Directory gateway will not be redirected to a Directory server, and vice versa.
   - The **Disaster recovery** option only applies to Directory servers, not to Gateways.



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

Server	Gateway	Disaster recovery
P-DC	☐	☐
F-DC	☐	☐
P-DMZ	☑	☐
F-DMZ	☑	☐

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

Adding a server in the list will require a license update

8 Update your license to include the servers you've just promoted to Directory gateways.

9 Click **Apply**.

After you finish

If you have client workstations that are forced to connect to a specific Directory, update their settings so they connect to one of the Directory gateways instead.

Related Topics

Preparing Directory failover and load balancing on page 143

16

Partitions

This section includes the following topics:

About partitions

A partition is a type of entity that defines a set of entities that are only visible to a specific group of users. For example, a partition could include all areas, doors, cameras, and zones in one building.

Partitions eliminate the tedious task of creating one-to-one relationships between users and the entities they are allowed to see in the system. If a user has no rights to a partition, that partition and everything it contains is hidden from that user.

Each partition is defined by the following:

- **List of members:** Entities that belong to the partition (areas, doors, cameras, cardholders, users, and so on).
- **List of authorized users:** Users and user groups that have the right to access the entities in the partition. The type of user access (view, add, modify, delete, and so on) varies according to the *user privileges*. Exceptions to the basic privileges of a user can be configured for each partition the user has access to.

NOTE: An authorized user of a partition is not necessarily a member of that partition, nor is a user who is a member of a partition necessarily an authorized user.

Benefits of partitions

Dividing your system into smaller parts has the following two main benefits:

- It reduces the scope of what a user can access for security reasons. For example, in a multisite system, it might be undesirable for the security team of one site to be able to see or interfere with the activities of a security team on another site.
- It reduces the scope of a user's work to make it more manageable. If a user is only concerned with one part of the system (one site in a multi-site system), it is better not to be distracted by the entities the user is not responsible for.

Partition administrators

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

System-created partitions

By default, two partitions are created in Security Center. They are invisible unless you explicitly created other partitions in your system. The idea is that if you do not need to divide your system into partitions, you do not want to see any partition at all.

- **Root partition:** The *root* partition (🌐) is the partition that contains everything your create in your system. It is named after your main server. When there are no user-created partitions in the system, all created entities belong to the root partition, and all users are authorized users of the root partition.
- **System partition:** The *System* partition (🌐) is a partition that is exclusively managed by the system for the purpose of keeping certain system entities always accessible to all users, such as the Always schedule, the Default network entity, the main server entity, the Health Monitor role, the Report Manager role, and so on. No one can alter the System partition, not even the system administrators.

The root partition and the System partition are the only two top level partitions in the system. All partitions you create are subordinate to the root partition.

Creating partitions

To divide your system into smaller, manageable parts, and hide some of those parts from certain users, you can create partitions.

What you should know

The first partition you create is always added to the root partition. Subsequent partitions you create are added to the partition you select in the entity tree. If none are selected, the system will ask you to specify under which partition you want to create the new partition.

To create a partition:

1. From the Config Tool home page, do one of the following:
   - Open the **User management** task, click **Add an entity** (➕), and then click **Partition**.
   - Open any administration task, click **Add an entity** > **Show all** > **Partition**, or click **More** (▾) beside the **Add** (➕) button, and then click **Partition**.
2. If a partition is selected in the entity tree before you click **Add**, then the new partition is immediately created under the selected partition.
   1. Enter the name of the **New partition** that appears.
   2. In the **Identity** tab, enter the partition description.
3. If no partition was selected in the entity tree before you click **Add**, then the Create partition wizard appears.
   1. In the **Basic information** page, enter the name and description of the new partition.
   2. From the **Partition** drop-down list, select the parent partition that this new partition should belong to.

   The new partition is created.
4. If you already have entities ready to be added to the new partition, add them now.
5. If users and user groups are already created in your system, grant them access rights for the new partition.

The partition is created. New entities that you create can be added directly into the partition.

Related Topics

About partitions on page 282

Updating the content of partitions

You can control the visibility of entities to users in your system by adding or removing entities from the partitions these users are authorized to access.

What you should know

When you put related entities, such as cardholders and credentials, into different partitions, users that are not authorized to access all the partitions involved may not have all the access rights they need to perform their tasks. To simplify the partition configuration process, when you add or remove entities from a partition, the system automatically adds or removes their related entities to that partition, following rules guided by common practices. The implicit rules applied by the system are as follows:

- Adding a user group or a cardholder group also adds their members.
- Adding a user or a cardholder does not automatically add their parent groups.
- Removing a user group or a cardholder group also removes their members.
- Removing a user or a cardholder does not automatically remove their parent groups.
- Adding a cardholder also adds their associated credentials.
- Removing a cardholder also removes their associated credentials.
- Adding a credential does not automatically add its associated cardholder.
- Removing a credential does not automatically remove its associated cardholder.
- When adding an entity that has child entities attached (such as areas and roles), you need to specify whether or not you want to add its child entities as well (which includes everything that's below that entity's hierarchy).
- When removing an entity that has child entities attached (such as areas and roles), you need to specify whether or not you want to remove its child entities as well (which includes everything that's below that entity's hierarchy).
- Adding an entity to a partition does not remove it from the other partitions it belongs to. There is no limit to the number of partitions an entity can belong to.
- Removing an entity from a partition automatically adds it to the root partition if that entity does not belong to any other user-created partition.
- You cannot remove an entity from the root partition if that entity does not belong to any other partition.

To update the content of a partition:

1 From the Config Tool home page, open any administration task, and select a tab that shows an entity tree.

If the partitions are not visible, click **Show partitions** (🌐) in the **Search** box or press **F4**.

2 Select the partition you want to modify, and click the **Properties** tab.

The current contents of the partition are displayed in the **Members** list.

3 Do either one of the following:

- To add entities to the partition, click **Add** (➕), select the entities from the Search dialog box, and then click Select.
- To remove entities from the partition, select the entities from the Members list, and then click **Remove** (✖).

TIP: Alternatively, you can change the content of partitions directly from the entity tree, using drag-and-drop to move entities, and **CTRL**+drag-and-drop to copy entities.

All changes are immediately applied.

Granting access rights for partitions

To allow users to access the entities contained in a partition, you must grant access rights for that partition to the concerned users and user groups.

What you should know

Access rights for partitions are governed by the following rules:

- Access rights for partitions are inherited from parent user groups.
- Inherited access rights cannot be revoked.
- Access rights not granted to a user group can be granted to the members of the user group.
- Granting access rights for a partition to a user or user group also grants access rights for its child partitions to the same user or user group.
- Revoking access rights for a parent partition from a user or user group also revokes access rights for its child partitions from that user or user group, except when those access rights are inherited from parent user groups.
- Revoking access rights for a child partition from a user or user group does not revoke the access rights for its parent partition from that user or user group.

To grant access rights for a partition to a user:

1. From the Config Tool home page, open the **User management** task, select a user, and then click the **Access rights** tab.
2. Select the checkbox beside the partition you want to grant access rights for.

   This action automatically grants access rights for all its child partitions as well.
3. To revoke access rights for some of the child partitions, clear the checkbox beside the selected child partitions.
4. If necessary, promote this user to partition administrator.
5. Click **Apply**.

Promoting users to partition administrator

To allow a user or user group to have full administrative rights for a partition and its members, you can promote that authorized user to partition administrator.

What you should know

A user who is an administrator of a partition is also the administrator of all its child partitions.

To promote a user to partition administrator:

1. From the Config Tool home page, open the **User management** task, select a user, and then click the **Access rights** tab.
2. In the row corresponding to the partition for which you want to grant the selected user administrator rights to, select the checkbox in the **Administrator** column.
3. Click **Apply**.

17

Users and User groups

This section includes the following topics:

About user groups

A user group is a type of entity that defines a group of users who share common properties and privileges. By becoming member of a group, a user automatically inherits all the properties of the group. A user can be a member of multiple user groups. User groups can also be nested.

Benefits of user groups

Since all the users that are part of the user group automatically inherit all the properties of that group, this simplifies the configuration of users on large systems.

Administrators user group

The *Administrators* user group is a system entity that is created during installation. It cannot be deleted or renamed. Members of this user group are also known as *system administrators*. They have the same administrative rights as the *Admin* user, and their rights cannot be revoked.

BEST PRACTICE: For reasons of traceability, rather than letting everyone use the same *Admin* account, it is best to create a separate user account for each administrator.

Creating user groups

To group users who share common properties and privileges, you can create user groups.

What you should know

You can also import user groups from your corporate directory service.

To create a user group:

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

2 Click **Add an entity** (✚), then click **User group** (👥).

3 In the **User group information** page, enter a name and description for the user group.

4 From the **User group** drop-down list, select the parent group for the new user group.

The user group automatically inherits the properties of its parent user group.

NOTE: Concerning the user group's partition membership:

- If you select **Unassigned**, the new user group will be added to the root partition.
- If you select a parent user group, the new user group will be added to the same partition that the parent user group belongs to.

5 To grant the user group a predefined set of privileges, select a **Privilege template** from the drop-down list.

NOTE: If you are unsure of what privileges the user group needs, you can postpone this decision to later. The privilege template can be applied at any time.

6 Click **Next**.

7 (Only if partitions are in use) In the **Access rights** page, select the partitions for which access rights are to be granted to this user group.

8 Click **Next**.

9 In the **Creation summary** page, verify that both the partition the user group belongs to and the ones the user group is authorized to access are as you intended.

10 Click **Create** > **Close**.

The new user group is created.

11 (Optional) Make this user group a subordinate of another user group.

Related Topics

Privilege templates on page 298

Adding subordinate user groups

To save time on configuring your system, you can create sub-user groups that inherit all the attributes of their parent group.

What you should know

Adding sub-user groups is helpful if you have multiple levels in your management team, and the sub-groups share almost all the same properties and privileges (for example, a day shift user group and a night shift user group on your security team).

To add a subordinate user group:

1 Open the **Security** task, and click the **User groups** view.

2 Select the user group to configure.

3 In the **Relationships** section of the **Identity** tab, select **Parent user groups**, and click **Insert an item** (✚).

4 Select one or more parent user groups, and click **Select** > **Apply**.

Adding users as members of user groups

To simplify the configuration of your system, you can add users as members of a user group so they inherit all the properties of that group.

To add a user as a member of a user group:

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

2 Select the user group to configure, and click the **Properties** tab.

3 Under the **Members** section**,** click **Add** (✚).

4 Select one or more users, and click **Select** > **Apply**.

TIP: Alternatively, you can modify the user groups' membership directly from the entity tree, using drag-and-drop to move, and **CTRL**+drag-and-drop to copy.

About users

A user is a type of entity that identifies a person who uses Security Center applications and defines the rights and privileges that person has on the system. Users can be created manually or imported from an Active Directory.

Each user is assigned a username and a password, which are the credentials required to log on to the system.

What a person can do on the system is restricted by their user attributes:

- **Privileges:** Limits the types of activities the user can perform on the system.
- **Access rights for partitions:** Limits the entities the user can exercise their privileges on.

A user can be a member of one or more *user groups*. Users can inherit the privileges and the access rights from their parent user groups.

Admin user

The *Admin* user is a user created by default and cannot be deleted or renamed. It has full administrative rights to configure Security Center. A person logged on as *Admin* can add, modify, and delete any entity in Security Center.

BEST PRACTICE: The *Admin* user is created with a blank password at software installation. For security reasons, you should immediately change the *Admin* user's password after software installation.

User levels

User levels range from 1-254. Level 1 is the highest user level, with the most privileges. The user level can be inherited from a parent user group. If the user has multiple parents, the highest user level is inherited. If the user has no parent group, the lowest user level (254) is inherited.

User levels affects three things in Security Center:

- They determine which users are logged out of the system when a threat level is set. For example, if you configure a threat level to trigger the *Set minimum user level* action, when the threat level is set, users with a lower user level than the one you specified are logged out.
- They determine which users can continue viewing a video stream when a camera is blocked in Security Desk. When you block a camera, users that have a lower user level than the one you specified can no longer view the video stream.
- They determine which user has priority over the PTZ controls of a camera when two or more users are trying to take control of a camera at the same time.

  Users can be given different user levels for PTZ controls that override their general user level. Priority is always given to the user with the highest level (1=highest). If two competing users have the same user level, it is decided on a first come first served basis.

  Once a user gains control over a PTZ camera, it is locked by that user. This means no other users can take control of that camera unless they have a higher user level. The control over the PTZ camera is automatically released after a period of inactivity (configured from the camera’s Hardware tab).

Related Topics

About privileges on page 296
About partitions on page 282

Creating users

To allow someone to log on to Security Center, you must create a user entity for them with logon credentials.

What you should know

You can also import users from your corporate directory service.

For security purposes, the *Entity name* for this user must be unique, because it is also the username they use to log on to Security Center.

To create a user:

1. From the Config Tool home page, open the *User management* task.
2. Click **Add an entity** (✚), then click **User** (👤).
3. In the **User information** page, enter a username that does not already exist.
4. Type a password for this user to log on to Security Center, and then confirm the password.
5. Enter the user's first and last name.
6. From the **User group** drop-down list, select the parent group for the new user.

   The user automatically inherits the properties of its parent user group.

   NOTE: Concerning the user's partition membership:

   - If you select **Unassigned**, the new user will be added to the root partition.
   - If you select a parent user group, the new user will be added to the same partition that the parent user group belongs to.

7. To grant the user a predefined set of privileges, select a **Privilege template** from the drop-down list.

   NOTE: If you are unsure of what privileges the user needs, you can postpone this decision to later. The privilege template can be applied at any time.

8. (Only if partitions are in use) In the **Access rights** page, select the partitions for which access rights are to be granted to this user.
9. Click **Next**.
10. In the **Creation summary** page, verify that both the partition the user belongs to and the ones the user is authorized to access are as you intended.
11. Click **Create** > **Close**.

The new user account is created.

After you finish

Configure the user.

Related Topics

Privilege templates on page 298

Configuring user settings

After a user is created in Security Center, you can configure their properties, and limit what they are allowed to do on the system.

Before you begin

Create the user.

What you should know

Instead of configuring the properties of an individual user, you can add the user as a member of a user group, so they inherit all the properties of the group.

To configure a user's settings:

1. From the Config Tool home page, open the *User management* task.
2. Select the user to configure, and click the **Properties** tab.
3. To temporarily prevent the user from logging on to Security Center, deactivate the user profile.
4. If you want to send emails or messages to this user, type an email address in the **Email address** field, and click **Apply**.

   You can send emails to users using the *Send an email* and *Email a report* actions.
5. Change the user's password or their password settings.
6. In the **User level** option, specify if the user inherits their user level from its parent user group, or set a specific level, and click **Apply**.
7. (Optional) Configure a different user level for controlling PTZ motors.
8. Grant access rights for partitions to the user.
9. Assign privileges to the user.
10. Customize how the user can log on.
11. To allow the user to remotely control Security Desk workstations, you must select the workstations they can control.
12. Click the **Advanced** tab.
13. To cycle the user's open tasks when they log on to Security Desk, switch the **Start task cycling on logon** option to **ON**, and click **Apply**.

    TIP: To prevent the user from stopping the task cycling once the Security Desk is open, deny them the *Start/stop task cycling* privilege.
14. When the user exports video (G64x) or snapshots, the system can include metadata (for example, camera name, creation date, and camera coordinates) which can be useful in incident investigation. To enable metadata with exported files, switch the **Include additional properties on export/snapshot** option to **ON** and click **Apply**.

Related Topics
About users on page 291

Deactivating user profiles

You can deactivate the profile of users that should no longer be allowed to log on to Security Center.

What you should know

A user cannot log on when their profile is deactivated. Deactivating a user's profile while the user is logged on will immediately log off the user.

To deactivate a user’s profile:

1. From the Config Tool home page, open the *User management* task.
2. Select the user to configure, and click the **Properties** tab.
3. Switch the **Status** option to **Inactive**, and click **Apply**.

Changing password settings for users

You can set a user's password to expire after a certain amount of time, force users to change their password on next logon, or enforce a minimum complexity for all user passwords.

What you should know

Password complexity requirements apply to all new passwords, and take effect when a user changes their current password.

Only users who have the *Change own password* user privilege can change their own password. Otherwise, they must contact their administrator to change their password.

To change the password settings for a user:

1. From the Config Tool home page, open the *User management* task.
2. Select the user to configure, and click the **Properties** tab.
3. To change the user's password, click **Change password**, type a password, confirm the password, and click **OK**.
4. To set an expiry date for the user's password, switch the **Expires** option to **ON**, and select the number of days.

   The system automatically warns users if their passwords are expiring soon, and gives them a chance to set a new password immediately. You can set the password expiry notification period to between 0 and 30 days from the System task.
5. To require the user to change their password the next time they log on to Patroller or Security Desk, switch the **Change on next logon** option to **ON**.
6. Click **Apply**.
7. To add complexity requirements to user passwords, open the **System** task, click the **General settings** view, and click the **User password settings** page.
8. In the **Enforce a minimum number of** section, select from the following requirements, and type a value:
   - **Characters:** Minimum number of characters.
   - **Upper case letters:** Minimum number of upper case letters.
   - **Lower case letters:** Minimum number of lower case letters.
   - **Numerical characters:** Minimum amount of numbers.
   - **Special characters:** Minimum number of special characters.
9. Click **Apply**.

About privileges

Privileges define what users can do, such as arming zones, blocking cameras, and unlocking doors, over the part of the system they have access rights to.

User privileges in Security Center are divided into the following groups:

- **Application privileges:** Grant access to the Security Center applications.
- **General privileges:** Grant access to the generic Security Center features.
- **Administrative privileges:** Grant access to entity configuration in Config Tool.
- **Task privileges:** Control accessibility to the various Security Center tasks.
- **Action privileges:** Control the *actions* that can be performed on the system entities.

For a detailed list of available privileges, see: Security Center privileges on the Genetec™ Technical Information site.

Privilege hierarchy

Privileges are organized in a hierarchy, with the following behavior:

- For a child privilege to be allowed, the parent privilege must be allowed.
- If a parent privilege is denied, all child privileges are denied.
- A child privilege can be denied when the parent privilege is allowed.

Privilege inheritance

Privilege settings can be inherited from user groups and replaced at the member (user or user group) level according to the following rules:

- A privilege that is undefined at the group level can be allowed or denied at the member level.
- A privilege that is allowed at the group level can be denied at the member level.
- A privilege that is denied at the group level is automatically denied at the member level.
- When a user is a member of multiple user groups, the user inherits the most restrictive privilege settings from its parents. This means that *Deny* overrules *Allow*, and *Allow* overrules *Undefined*.

Exceptions to privilege rules

The following exceptions apply to the privilege rules:

- **System administrators:** The *Admin* user, and the members of the *Administrators* user group, have a special status that grants them full administrative rights. These users can configure Security Center as they see fit; they can view and modify all entities in all partitions. The *Admin* user and the *Administrators* user group are created at installation and cannot be deleted or renamed.
- **Partition administrators:** A user or user group assigned to a partition can be given the status of *Partition administrator* over that partition. This special status confers full administrative rights over the entities contained in that partition. It supersedes all privileges configured at the partition level for that user or user group. Partition administrators can add, modify, and delete all entities within their partitions, including roles, users, user groups, and child partitions. Unlike users with the administrator status, the *Application*, *General*, and *Task* privileges can be denied to partition administrators.
- **Entities only administrators can configure:** There are entities in the system that can only administrators can configure. They are *partitions*, *roles*, *servers*, *users*, and *user groups*. Among them, *servers* can only be configured by system administrators. Administrative rights over these entities

cannot be granted through privileges. The properties of these entities are hidden to non-administrative users.

Privilege exceptions for partitions

A user (or user group) has a set of *basic privileges* that is the end result of the privileges inherited from their parent user groups, plus the ones explicitly allowed or denied to the user.

When a user is given access to a partition, their basic privileges are applied by default to the partition. Later, an administrator or a partition administrator can overwrite the privileges a user has over a specific partition. For example, a user can be allowed to configure *alarms* in partition A, but not in partition B. This means that a user can have a different set of privileges for each partition they have access to. Only *Administrative* and *Action* privileges, plus the privileges over *public tasks*, can be overwritten at the partition level.

Privilege templates

Privilege templates are *predefined* privilege configurations, based on standard security personnel profiles, that you can apply to users and user groups to simplify the creation process. Once applied, you can fine tune the privileges manually.

You cannot rename, modify, or delete the privilege templates, but you can apply them at any time. You can freely modify the privilege settings after a privilege template is applied to a user or user group.

BEST PRACTICE: Create one user group for each privilege template if necessary. After your model user groups are created, users can inherit privileges from them.

Types of privilege templates

Security Centerprovides the following privilege templates:

- **Reporting:** This template only grants the privileges to run Security Desk and to execute the most basic reporting tasks, excluding those for AutoVu™ LPR. A user with this set of privileges alone cannot view any video, control any physical devices, or report incidents.
- **Operator:** This template is for security operators who need to monitor real time events in the system. It grants them the privileges to use the Monitoring task, view video, manage visitors, credentials, and badge templates, add bookmarks and incidents, save snapshots, unlock doors, and so on.
- **Investigator:** This template is for investigators. It grants the privileges to use the Monitoring task, view video, control PTZ cameras, record and export video, add bookmarks and incidents, use investigation tasks, manage alarms and visitors, override door unlock schedules, save tasks, and so on.
- **Supervisor:** This template is for people who have supervisory responsibilities. It grants the same privileges as the *Investigator* template, plus the privileges to use maintenance tasks, manage cardholders and credentials, modify custom fields, set threat levels, block cameras, and perform people counting.
- **Provisioning:** This template is for the system installer. It grants almost all configuration privileges, with only a few exceptions (managing roles, macros, users, user groups, custom events, activity trails, threat levels, and audio files).
- **Basic AutoVu™ Operator:** This template is for security operators using AutoVu™ LPR. It grants them privileges to use LPR tasks, configure LPR entities, create LPR rules, monitor LPR events, and so on.

Assigning privileges to users

You must grant privileges to users in order for them to do anything in Security Center, including logging on, using Security Desk, and so on.

What you should know

Users have a set of basic privileges, which are privileges explicitly granted to them or inherited from their parent user groups, plus a set of privileges for every partition for which they are an authorized user. Privileges granted or denied at the partition level replace the basic privileges.

You can grant specific privileges to individual users, or allow users to inherit privileges from their parent user groups.

To assign privileges to a user:

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

2 Select the user to configure, and click the **Privileges** tab.

3 Select the different columns to grant or deny privileges.

  Some privileges might already be granted or denied if the user is part of a user group, or if the user was assigned a privilege template when the entity was created.

  - **Allow:** The privilege is granted to the user.
  - **Deny:** The privilege is denied to the user.
  - **Undefined:** This privilege must be inherited from a parent user group. If the user is not a member of any group, or if the privilege is also undefined at the parent user group level, then the privilege is denied.

4 At the bottom of the screen, click **Add** (➕) to create a set of exceptions to the basic privileges for a given partition the user is authorized to access.

5 To apply a privilege template, click (⚙), then click one of the following:

  - **Apply template:** Select one of the privilege templates to apply.
  - **Set configuration to read-only:** Set all entity configuration privileges found under the *Administrative* privileges group to *View properties*.
  - **Set configuration to read-write:** Allow the modification of all entity configurations, including *Add* and *Delete*.

6 Click **Apply**.

Related Topics

About privileges on page 296
Privilege templates on page 298

Customizing user logon options

You can select how and when users are allowed to log on to Security Center.

What you should know

The settings apply to the local workstation, and affect Security Desk and Config Tool for all users. Changes only take effect the next time a user starts Security Desk or Config Tool.

NOTE: If **Use Windows credentials** is set to **Always** or the **Force Directory to** option is selected, and a user is stuck and cannot log on, hold CTRL + SHIFT, and click **Log on**. This either lets the user log on using their Security Center credentials, or forces the **Directory** field to be displayed.

To customize user logon options:

1 From the home page in Config Tool, click **Options** > **General**.

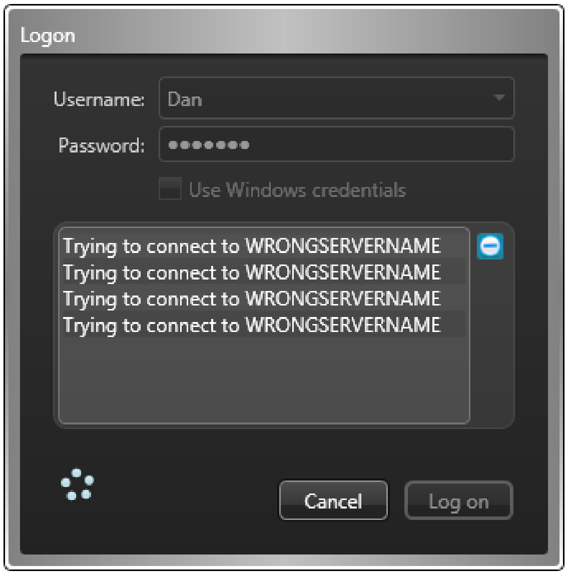
2 To force users to log on using Windows credentials, set the **Use Windows credentials** option to **Always**.

For this option to work, the users who are expected to log on using this computer must be imported from an *Active Directory*.

3 To restrict the access of all users to a specific Directory, select the **Force Directory to** option, and type the name of the Directory.

With this option, users cannot choose the Directory to which they want to connect; the **Directory** field is not displayed in the *Logon* window. However, they can automatically be redirected to another Directory when load balancing is used.

NOTE: If there is a mistake in the Directory name (for example, a typo), then the next time users try to log on, they will not be able to connect.



Trying to connect to WRONGSERVERNAME
Trying to connect to WRONGSERVERNAME
Trying to connect to WRONGSERVERNAME
Trying to connect to WRONGSERVERNAME

4 To bypass Directory load balancing, select the **Prevent connection redirection to different Directory servers** option.

Users will connect to the default Directory or to the Directory they specify when logging on, and will not be automatically redirected to another server. This option is meaningful only if Directory *load balancing* is configured.

5 Click **Save**.

6 To limit the number of workstations a user can log on to at the same time, do the following:

a) Open the **User management** task.

b) Select the user you want to configure, and click the **Advanced** tab.

c) Switch the **Limit concurrent logons** option to **ON**, and select the number of workstations.

7. To select when a user can log on, click **Add an item** (+) under the **User logon schedule** section.
8. Select predefined schedules, and click **Select**.

   If you select multiple schedules, the schedule conflict rules apply. When two schedules with the same priority level overlap, the blocking schedule has priority over the allowing schedule.

9. To log the user off after a period of inactivity, switch the **Auto lock** option to **ON**, and select how long the session must remain inactive before being logged off.

   This option only applies to Security Desk. Before being logged off, the message `Session is about to lock` is displayed to the user. After the application is locked, the user must log back on to resume with the current session.
10. Click **Apply**.
11. To require the user to log on to Security Center with a logon supervisor, in the **User management** task, select the user to be the supervisor, and click the **Advanced** tab.
12. Under the **Logon supervisor of** section, click **Add an item** (+), select the user to be supervised, and click **OK**.
13. Click **Apply**.

Related Topics

Importing security groups from an Active Directory on page 323

Forcing Security Desk to run in full screen mode

If a user's job is to focus on monitoring live video, you can force Security Desk to run in full screen mode to prevent the user from switching to Windows mode.

What you should know

You can also set Security Desk to start in full screen operation mode on a specific workstation.

To force Security Desk to run in full screen mode for a user:

1. From the Config Tool home page, open the *User management* task.
2. Select a user, and click the **Privileges** tab.
3. Expand the **Application privileges**, and the **Security Desk** privileges.
4. Deny the privilege **Change client views** to that user.
5. Click **Apply**.

Security Desk now always runs in full screen mode for that user. The *Restore Down* command and the **F11** key (switch between full screen and windowed mode) are disabled.

Setting Security Desk to start in full screen mode on workstations

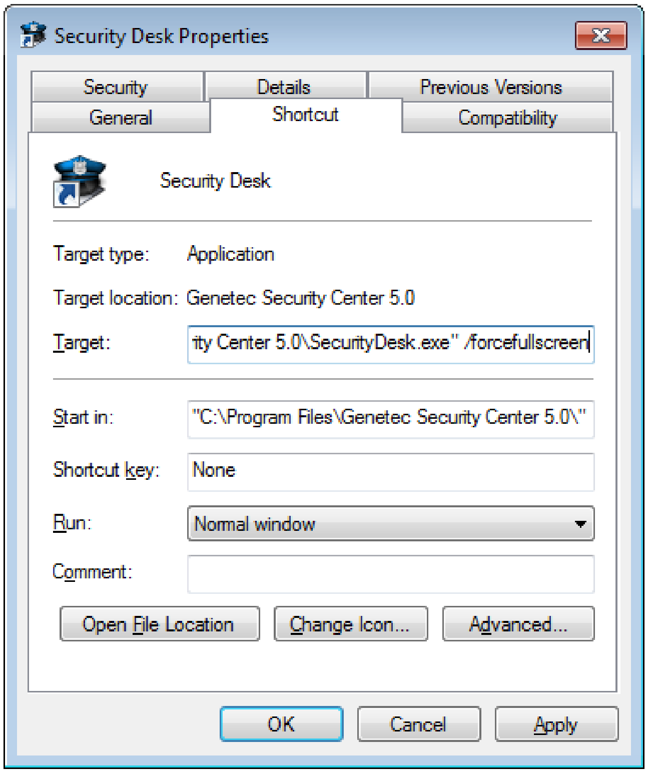
If a workstation is mainly used for monitoring live video, you can set Security Desk to always start in full screen mode on that workstation.

What you should know

Setting Security Desk to start in full screen mode does not prevent the user from minimizing the Security Desk window with Alt+ESC or to switch to another application with Alt+TAB.

To set Security Desk to start in full screen mode on a workstation:

1. On the workstation, open the **Security Desk Properties** dialog box.
2. Select the **Shortcut** tab, and add the option `/forcefullscreen` (or `/ff`) to the end of the string found in **Target**.



Target type: Application

Target location: Genetec Security Center 5.0

Target: ity Center 5.0\SecurityDesk.exe" /forcefullscreen

Start in: "C:\Program Files\Genetec Security Center 5.0\"

Shortcut key: None

Run: Normal window

Comment:

3 Click **Apply**.

The next time a user starts Security Desk using this shortcut, the application starts in full screen mode. The *Restore Down* commands and the F11 key (switch between full screen and windowed mode) are disabled.

Selecting which workstations users can remotely control

You can select which Security Desk workstations and monitors a user is allowed to remotely control using a CCTV keyboard, or using the *Remote* task in Security Desk.

What you should know

Every monitor controlled by Security Desk is assigned a unique *monitor ID* (displayed in the notification tray, and found in the *Logical ID* page in the System task). Using a CCTV keyboard, you can display an entity on a remote Security Desk workstation by specifying its monitor ID, *tile ID*, and the *logical ID* of the entity.

For more information about using the *Remote* task in Security Desk, see the *Security Desk User Guide*.

To select which workstations a user can remotely control:

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

2 Select the user to configure, and click the **Advanced** tab.

3 Under the **Allow remote control over** section, click **Add an item** (✚).

4 From the drop-down list, select one of the following entity types:

- **User:** Any Security Desk workstation where that user is logged on can be remotely controlled.
- **User group:** Any Security Desk workstation where a member of that user group is logged on can be remotely controlled.
- **Application:** The specified workstation (*COMPUTER - SecurityDesk*) can be remotely controlled, regardless of who is logged on.

5 Select the associated entities, and click **OK** > **Apply**.

Selecting which user activities to log

You can select which types of user-related activity are logged in the database, and available for reporting in the *Activity trails* task.

What you should know

The activities you can log are events that are generated by users who connected to Security Center.

To select which user activities to monitor:

1 From the Config Tool home page, open the **System** task.
2 Click the **General settings** view, and then click the **Activity trails** page.
3 From the list, select the events to monitor.

   You can select general events, or events specifically related to video, access control, or LPR.

4 Click **Apply**.

You can now search for events in your system that were triggered by users, using the Activity trails task.

Related Topics
Event types on page 908
Investigating user related activity on the system on page 266

18

TLS and Directory authentication

This section includes the following topics:

What is Transport Layer Security protocol?

Transport Layer Security (TLS) is a protocol that provides communications privacy and data integrity between two applications communicating over a network. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

What you should know

Starting from Security Center 5.4, TLS is used for connections to the Directory from client workstations and expansion servers. With TLS, you have the option to enforce Directory authentication on client workstations and servers during software installation.

What are the benefits of TLS?

TLS provides numerous benefits to clients and servers over other methods of authentication, including:

- **Strong authentication:** Authenticate the Directory to client applications, proving the identity of the server before connecting to it. Protects against *man-in-the-middle* attacks.
- **Data integrity:** All data are transmitted with an integrity check value.
- **Message privacy:** Protects against eavesdropping.

  NOTE: The potential of such threats is present only if you allow connections from the WAN (as opposed to through a secure VPN) or when your corporate network has been physically compromised.
- **Algorithm flexibility:** Provides options for the authentication mechanisms, encryption algorithms, and hashing algorithms that are used during the secure session.
- **Ease of use:** Most of its operations are completely invisible to the client. This allows the client to have little or no knowledge of the security of communications and still be protected from attackers.

Limitations

- Man-in-the-middle protection is only enforced if you choose to turn on Directory authentication on each machine (Client or Server).
- Machines running Security Center 5.3 and earlier, and Mobile Server 4.0, can only connect to Security Center 5.5 Directory using the old communication protocol.
- Client certificate are not yet supported for Config Tool and Security Desk.

Backward compatibility

Backward compatibility is enabled by default at system installation. When the 5.5 Directory receives a connection request from Security Center 5.3 and earlier, it automatically switches to the old communication protocol (less robust against network attacks). If network vulnerability is an issue to your organization, you can disable backward compatibility, and force all machines to upgrade before they can connect to your system.

Related Topics
Server - Properties tab on page 841

What is Directory authentication?

Directory authentication is a Security Center option that forces all client and server applications on a given machine to validate the identity certificate of the Directory before connecting to it. This measure prevents man-in-the-middle attacks.

When do I need Directory authentication?

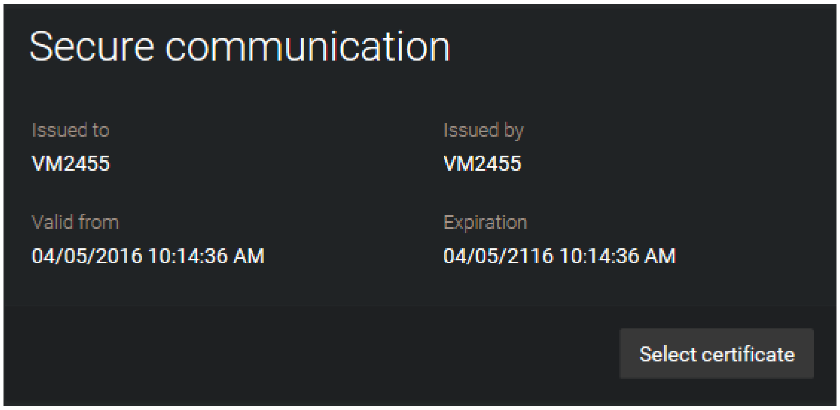
The purpose of Directory authentication is to protect against *man-in-the-middle* attacks. If you do not have applications connecting to your system over the Internet (or any untrusted network), the potential for this sort of attacks is very low. In that case, you are probably safe not to enable this option.

What is an identity certificate?

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

How it works

When installing the Server components of Security Center, a *self-signed certificate* named *GenetecServer-{MachineName}* is automatically created in the Local Computer Certificate Store. You can view the current certificate in the Server Admin **Genetec Server** tab of your server, under the *Server communication* section.



Secure communication

Issued to: VM2455

Issued by: VM2455

Valid from: 04/05/2016 10:14:36 AM

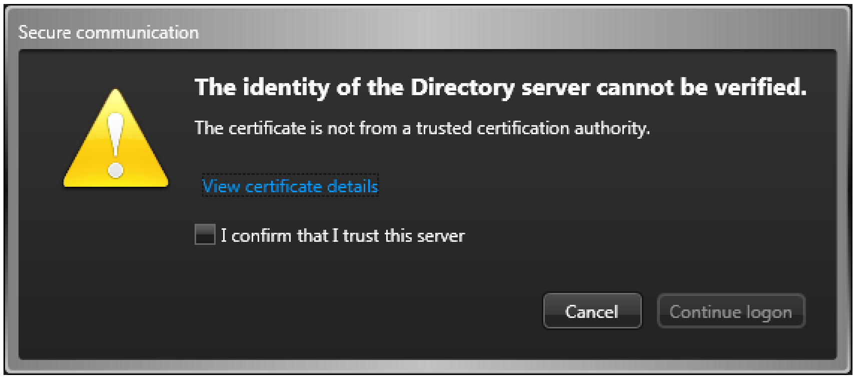
Expiration: 04/05/2116 10:14:36 AM

The self-signed certificates are used to identify the *expansion servers* to the *main server*, so the password used to connect to the main server does not need to be stored locally on the expansion servers.

Directory authentication is enabled at Security Center installation by selecting the option **Turn on Directory authentication** in the *Security Settings* page. For more information, see the *Security Center Installation and Upgrade Guide*.

BEST PRACTICE: If you choose to enable Directory authentication, we recommend that you replace the self-signed certificate on the main server with one issued by a trusted *certificate authority*. The CA can be internal or from a third party. This allows you to deploy a highly secured system without forcing your users to be aware of the underlying mechanism.

If you choose to keep the self-signed certificate on the main server, then the first time a workstation is used to connect to the Directory, the user will be prompted to confirm that the Directory server can be trusted.


Secure communication

The identity of the Directory server cannot be verified.

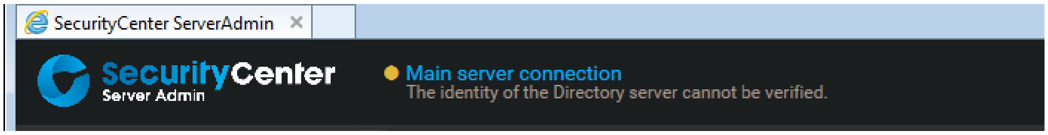
The certificate is not from a trusted certification authority.

View certificate details

□ I confirm that I trust this server

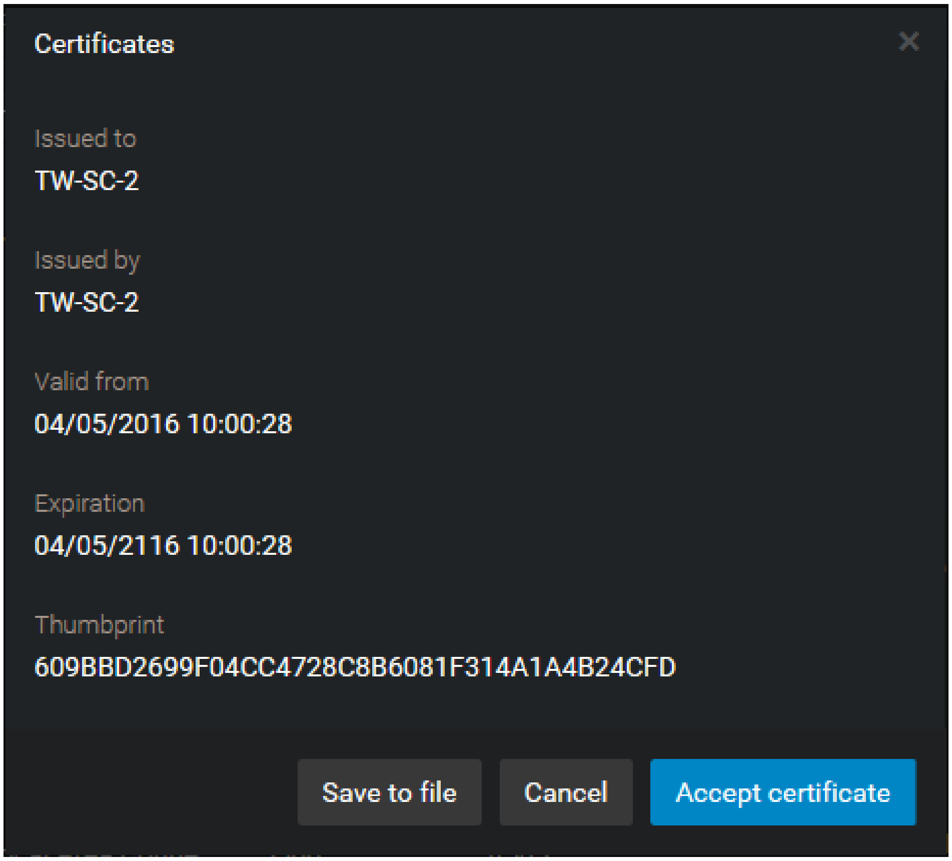
Once a user confirms that the main server can be trusted, the certificate is whitelisted, and the dialog box will not appear again.

The same confirmation is required on expansion servers. The first time you log on to the expansion server with Server Admin, you will see this message on the dashboard.



● Main server connection
The identity of the Directory server cannot be verified.

You must click on **Main server connection**, and then click **Accept certificate** in the dialog box that appears.


Certificates

Issued to
TW-SC-2

Issued by
TW-SC-2

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

Expiration
04/05/2116 10:00:28

Thumbprint
609BBD2699F04CC4728C8B6081F314A1A4B24CFD

Once the main server is confirmed, you can change the password or the certificate on either the main server or the expansion server, and never have to confirm your trust again, as long as the two servers stay connected while you make the change.

Requirements

For Directory authentication to work, the following conditions must be met:

- DNS must be configured on the network. Servers and client workstations must be able to resolve the main server name.
- The main server name must be resolved by the DNS to the common name on the Directory certificate.
- Client workstations and expansion servers must be able to trust the certificate provided by main server. Otherwise, a user intervention is always required to accept the certificate the first time a machine is used to connect to the main server.

How do I change this setting after installation?

To change the Directory authentication setting after software installation, you must edit the *GeneralSettings.gconfig* file on each computer where you want it changed.

Changing the Directory authentication setting

You can choose to turn Directory authentication on or off on each computer, by changing the TLS channel policy setting in their respective *GeneralSettings.gconfig* file.

What you should know

Directory authentication is enabled at Security Center installation by selecting the option **Turn on Directory authentication** in the *Security Settings* page. For more information, see the *Security Center Installation and Upgrade Guide*.

After Security Center is installed, if you want to change this setting, you must edit the *GeneralSettings.gconfig* file on each computer.

To change the Directory authentication setting after software installation:

1 Open the *GeneralSettings.gconfig* file in the configuration folder with a text editor.

The configuration folder is found under the Security Center installation folder (default = *C:\Program Files (x86)\Genetec Security Center 5.5*\ConfigurationFiles).

2 Edit the `<tlsChannel policy="value">` tag.

Change the value to `"AllowAll"` to disable Directory authentication, or to `"TrustedOnly"` to enable it.

3 Save your changes and restart the *Genetec Server* service.

Disabling backward compatibility

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

What you should know

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

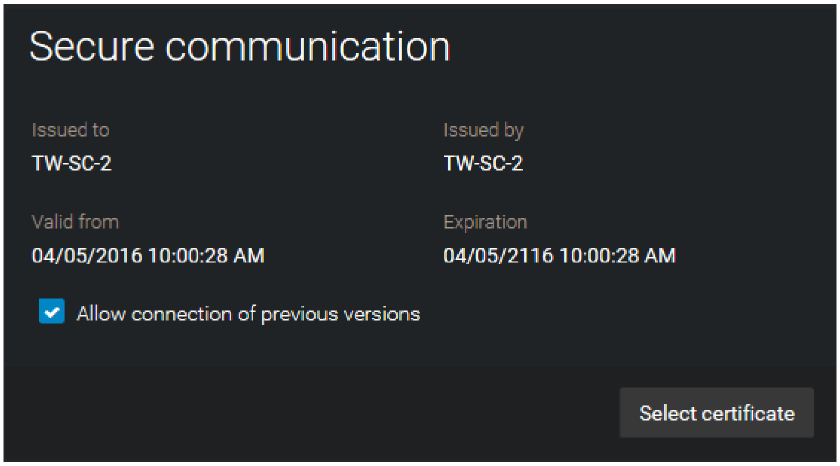
CAUTION: Mobile Server 4.0 does not support TLS. Disabling backward compatibility means that the Mobile apps and the Web Clients will no longer be able to connect to Security Center. All expansion servers that have not yet been upgraded to version 5.5 will also cease to work.

To disable backward compatibility:

1 Connect to Server Admin of your main server with a web browser.

2 Click the main server (🌐) in the server list.

3 Under *Secure communication*, clear the **Allow connection of previous versions** option.



Secure communication

Issued to
TW-SC-2

Issued by
TW-SC-2

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

Expiration
04/05/2116 10:00:28 AM

☑ Allow connection of previous versions

4 Click **Save**.

Backward compatibility is disabled. The next time someone tries to connect to your system with an older Security Center application, they will get the *Client-server versions are incompatible* error.

Replacing default certificates

In order to replace the *self-signed certificate* on a server with a certificate from a trusted source, you must import the new certificate into the Local Computer Certificate Store of your server before you can select it in Server Admin.

Before you begin

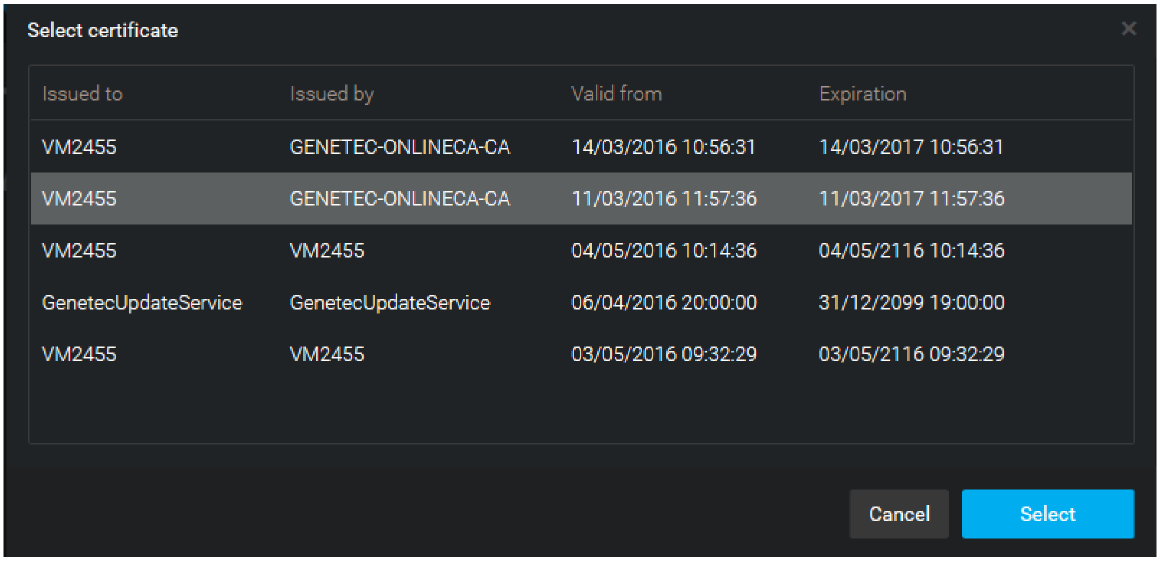
Follow your company's procedure regarding the enrollment of certificates. If your situation requires you to create a custom request, make sure you follow the recommendations required for Security Center.

What you should know

To improve the security of your system, you only need to replace the self-signed certificate on your main server (or all Directory servers if you have Directory failover configured). It is not necessary to change the certificate on all expansion servers.

To import a trusted certificate into the Local Computer Certificate Store of your main server:

1 On your main server, start Microsoft Management Console (mmc.exe).
2 In the *Console* window, expand **Certificates**.
3 Under **Certificates (Local Computer)**, right-click **Personal**, and then click **All Tasks** > **Import**.
4 Follow the instructions in the *Certificate Import Wizard* to import the certificate.
5 Open Server Admin on your server.
6 Click the **Genetec Server** tab.
7 Under *Secure communication*, click **Select certificate**.
8 In the dialog box that opens, select the new certificate you just imported and click **Select**.



Issued to	Issued by	Valid from	Expiration
VM2455	GENETEC-ONLINECA-CA	14/03/2016 10:56:31	14/03/2017 10:56:31
VM2455	GENETEC-ONLINECA-CA	11/03/2016 11:57:36	11/03/2017 11:57:36
VM2455	VM2455	04/05/2016 10:14:36	04/05/2116 10:14:36
GenetecUpdateService	GenetecUpdateService	06/04/2016 20:00:00	31/12/2099 19:00:00
VM2455	VM2455	03/05/2016 09:32:29	03/05/2116 09:32:29

NOTE: If the certificate you selected is not valid (not using Legacy key for example), an error message will be displayed and you won't be able to apply it.

9 Click **Save**, and restart the Genetec™ Server service.

Creating custom certificate requests for Security Center

Custom certificate requests must be created with specific parameters in order to work with Security Center. All certificate requests must be made from the server where certificate is going to be applied.

What you should know

Creating custom certificate requests should be your last resort. There are many simpler alternatives for requesting a certificate for your server. For example, you could enroll a certificate from a certificate template of your company's Active Directory domain. For more information, see Request Certificates by Using the Certificate Request Wizard on the Microsoft Technet Library.

To create a custom certificate request for Security Center:

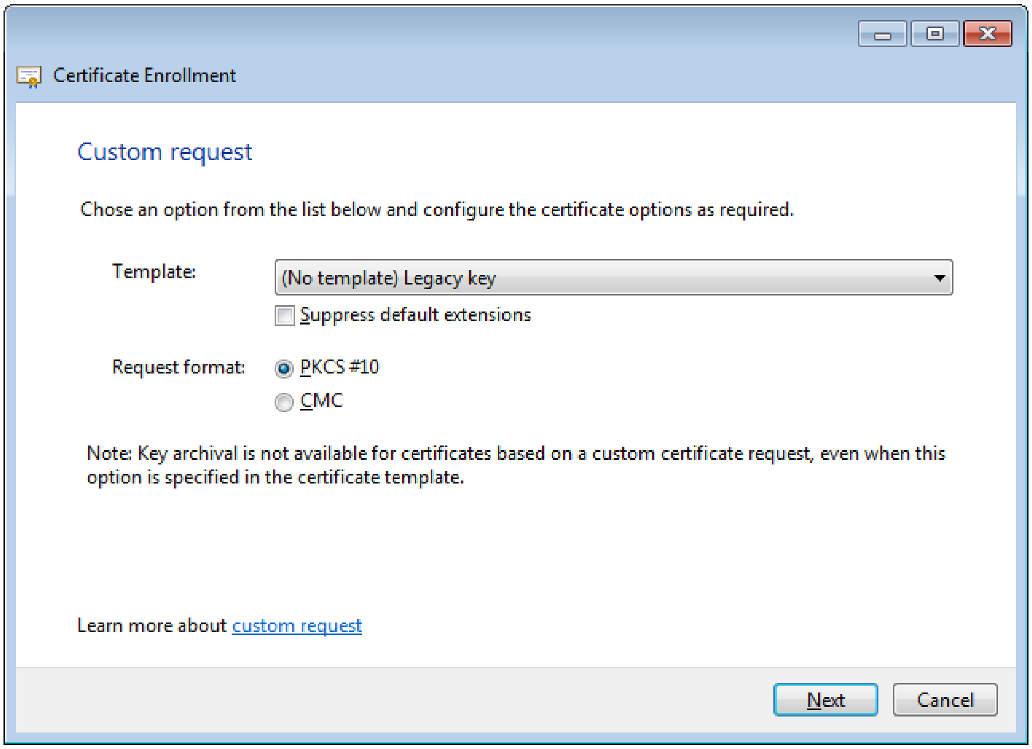
1 On your main server, start Microsoft Management Console (mmc.exe) and add the Certificates snap-in.
   a) In the *Console* window, click **File** > **Add/Remove Snap-in**.
   b) In the *Add or Remove Snap-ins* dialog box that appears, click **Certificates**, then click **Add** >.
   c) In the *Certificates snap-in* dialog box, click **Computer account** > **Next** > **Finish** > **OK**.

2 In the *Console* window, expand **Certificates**.

3 Under **Certificates (Local Computer)**, right-click **Personal**, and then click **All Tasks** > **Advanced Operations** > **Create Custom Request**.

4 In the *Certificate Enrollment* dialog box, click **Next** > **Proceed without enrollment policy** > **Next**.

5 In the *Custom request* page, select the options as shown below.



Custom request

Chose an option from the list below and configure the certificate options as required.

Template: (No template) Legacy key

☐ Suppress default extensions

Request format: ● PKCS #10 ○ CMC

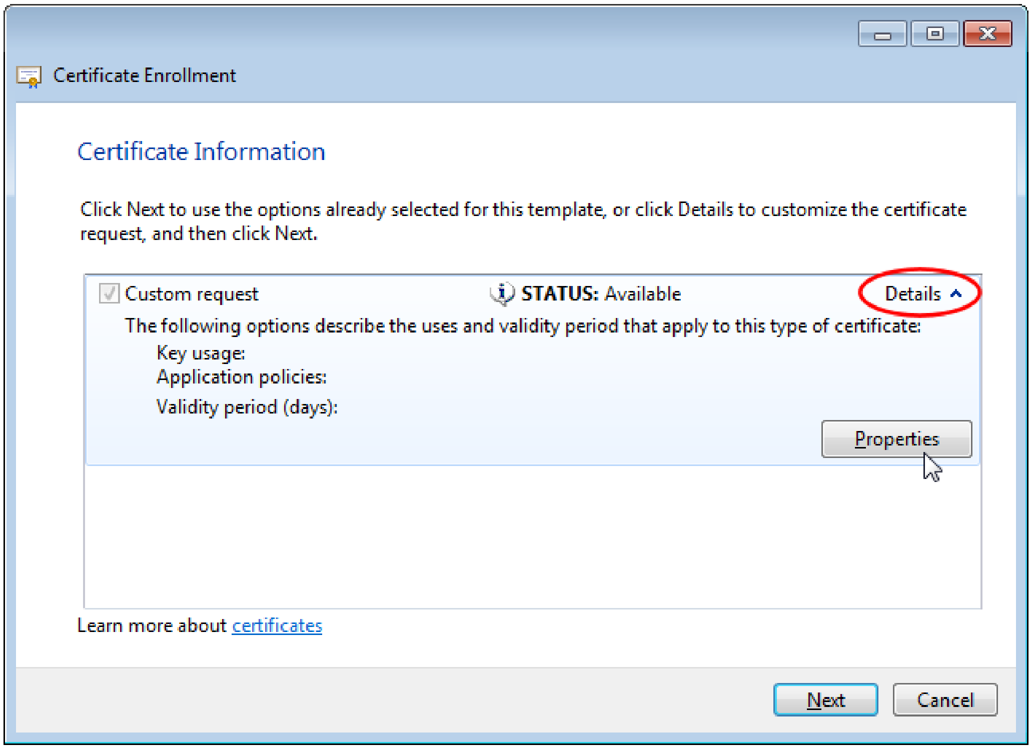
Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.

Learn more about custom request

IMPORTANT: For **Template**, select **Legacy key**. The default choice, **CNG key**, is not supported by .NET Framework 4.5, which is what Security Center uses.

6 Click **Next**

7 In the *Certificate Information* page, expand **Details**, and click **Properties**.



Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

☑ Custom request STATUS: Available Details

The following options describe the uses and validity period that apply to this type of certificate:

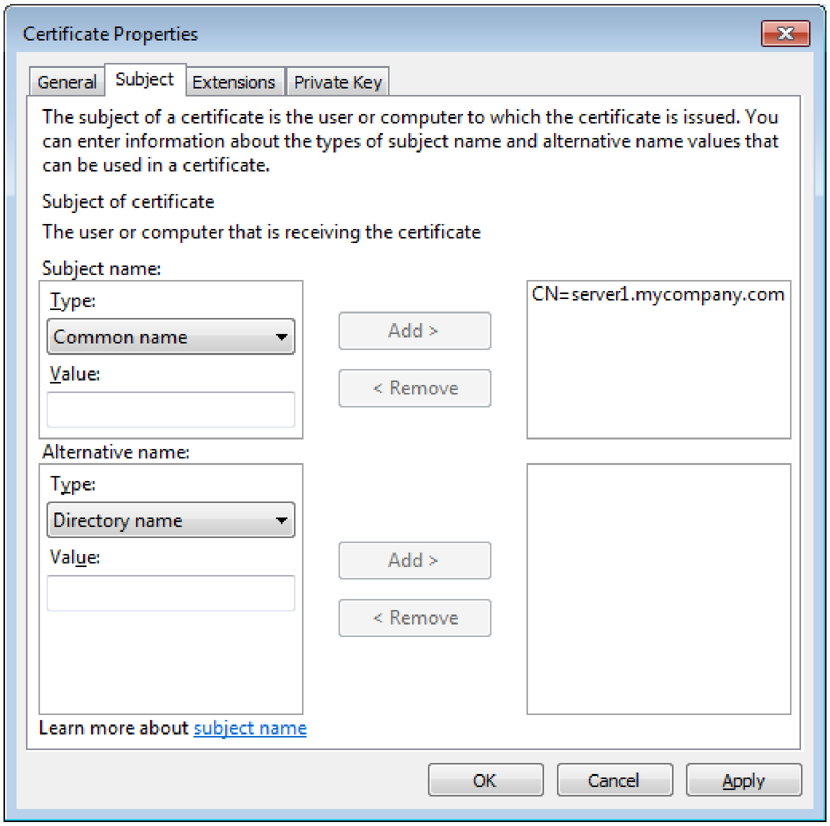
Key usage:

Application policies:

Validity period (days):

8 In the *Certificate Properties* dialog box, click the **Subject** tab, and enter the value of **Common name** under the **Subject name**.

IMPORTANT: The **Common name** must match the fully qualified domain name of the server. For example, if the hostname of your server is *server1*, and your domain is *mycompany.com*, then the fully qualified domain name for your server would be *server1.mycompany.com*.



Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

Value:

CN=server1.mycompany.com

Alternative name:

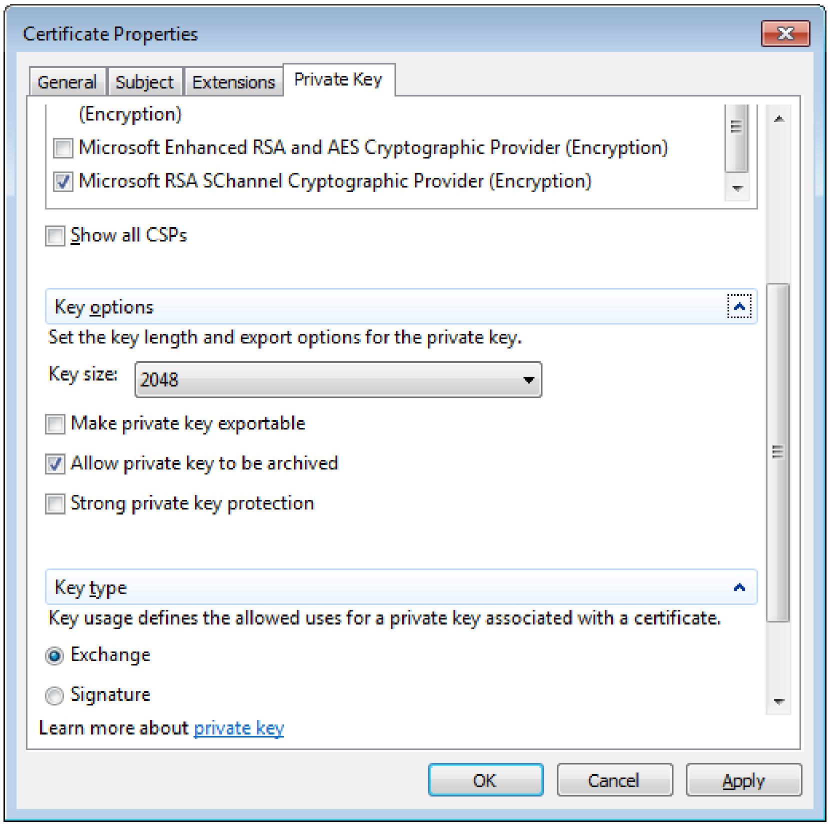
Type: Directory name

Value:

9 Click the **Extensions** tab, and set the following properties.

- **Key Usage:** Add **Digital signature** and **Key agreement**.
- **Extended Key Usage:** Add **Server Authentication** and **Client Authentication**.

10 Click the **Private Key** tab, and set the following properties.



(Encryption)

□ Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)

☑ Microsoft RSA SChannel Cryptographic Provider (Encryption)

□ Show all CSPs

Key options

Set the key length and export options for the private key.

Key size: 2048

□ Make private key exportable

☑ Allow private key to be archived

□ Strong private key protection

Key type

Key usage defines the allowed uses for a private key associated with a certificate.

● Exchange

○ Signature

Learn more about private key

- **Key Type:** Select **Exchange**. This must be set up first.
- **Cryptographic Service Provider:** Select only **Microsoft RSA SChannel Cryptographic Provider (Encryption)**. It is the last option in the list.
- **Key Options:** The **Key size** should be at least 2048.

11 Click **Apply** > **OK** > **Next**.

12 Enter the **File Name** and click **Finish**.

After you finish

Send the request (.csr) to your IT department or the external *certificate authority* for processing. Once the certificate has been generated, import and apply it to your server.

19

Active Directory integration

This section includes the following topics:

Integration with Windows Active Directory

Integrating a Windows Active Directory (AD) into Security Center allows you to manage all personnel and security information from a single location, whether it is for logical security (IT) or for physical security (controlling access to physical locations).

With AD integration, you can import security groups from an AD into Security Center as user groups, cardholder groups, or both. Members can be imported as users or cardholders. Both standard and custom attributes can be imported from the AD. Most imported fields can only be modified within the AD and are read-only in Security Center.

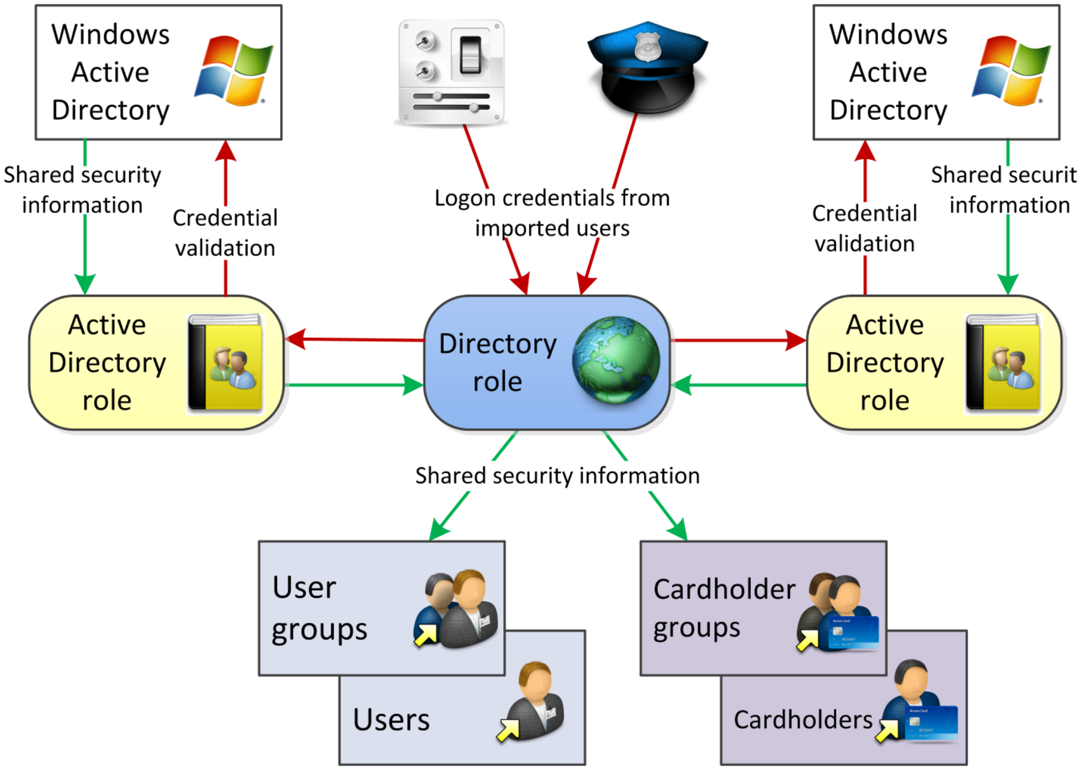
You can import entities from more than one AD if necessary. For example, from Security Center, you can manage access to a facility shared by multiple companies, such as an office building. As system administrator, you can import users and/or cardholders from their individual Active Directories, and manage them in separate partitions.

For larger AD setups that have many domains that are part of an AD forest, Security Center supports synchronizing Universal groups and connecting to a global catalog. A single *Active Directory* role can be used to synchronize a universal group. For more information about using Universal groups and global catalogs with Security Center, see About universal groups and global catalogs.

How AD integration works

To import users and/or cardholders from an AD, you must create an *Active Directory* role for the AD you want to import. The Active Directory role connects your Security Center system to an Active Directory server, and imports users and/or cardholders from selected security groups. Imported entities are identified in Security Center by a yellow arrow (↗) superimposed on the regular entity icon.

The Active Directory role synchronizes all the changes made on the AD with the imported entities in Security Center. It also pushes the logon credentials of imported users to the AD service for validation.



Benefits of AD integration

Having a centralized security information management system provides many benefits:

- Less data entry means fewer errors and better control during initial Security Center setup, because users and cardholders can be imported from an existing AD.
- Consistency and better security because all shared information is entered only once.
  - A new user account that is added to an imported security group automatically adds a new user and/or cardholder in Security Center.
  - A user account that is disabled in the AD automatically disables the corresponding user and/or cardholder in Security Center.
- Single logon capability for synchronized Security Center users. Users logged on to Windows do not have to log on to Security Center.

Active Directory synchronization

Through a process called *synchronization*, the *Active Directory* role also keeps all imported entities up-to-date with changes made on the AD.

All imported entities are synchronized with their source by the Active Directory role. Most of the attributes imported from the AD are read-only in Security Center, except for a few cardholder properties. Imported entities cannot be deleted unless they are deleted from the AD.

CAUTION: If you move a security account from a synchronized AD security group to one that is not synchronized, it is as though the account ceases to exist in Security Center. The Active Directory role deletes the corresponding entities (users and/or cardholders) from Security Center the next time it synchronizes with the AD.

Synchronization is always initiated from Security Center. There are two ways that you can start synchronization:

- **Manually:** Synchronization is performed when you explicitly request it. This is the default setting. The advantage of this approach is that you have perfect control over when you want the synchronization to be done.
- **On schedule:** The imported groups are synchronized using a scheduled task.

Information that can be synchronized with the AD

Both standard and custom Security Center fields can be imported from the AD, and kept synchronized with the AD. You can choose which user group, user, cardholder group, and cardholder fields to import from the AD in the *Links* tab of the Active Directory role.

The standard attributes you can import from the AD are:

- User group
  - Name
  - Description
  - Email address
  - All group members (users)
- User
  - Membership in the imported user group
  - Username
  - Password
  - Description
  - First name
  - Last name
  - Email address
  - Status: *Active* or *Inactive*
- Cardholder group
  - Name
  - Description
  - Email address
  - All group members (cardholders)

- Cardholder
  - Membership in the imported cardholder group
  - Cardholder name
  - Description
  - First name
  - Last name
  - Email address
  - Status: *Active* or *Inactive*
  - Picture (optional through the *Links* tab)
  - Partition (optional through the *Links* tab)
- Credential
  - Association to the imported cardholder
  - Credential name
  - Card data
  - Card format
  - Facility code
  - Card number
  - Status: *Active* or *Inactive*
  - Partition (optional through the *Links* tab)

Additional attributes are imported from the AD by mapping them to Security Center *custom fields*. The Active Directory role keeps all imported fields *synchronized* with the AD.

Related Topics
Scheduling a task on page 184
Mapping custom fields to synchronize with Active Directory on page 326

About Universal groups and global catalogs

Security Center supports synchronizing Universal groups that belong to a global catalog. Users from different domains in an AD forest can access Security Center using one *Active Directory* role connected to one domain controller (global catalog). There are some things you should know before synchronizing a Universal group that belongs to a global catalog.

Note the following when importing a Universal group that belongs to a global catalog:

- There must be a trust relationship configured between all domains in the AD forest.
- Primary groups are not supported.
- In order to retrieve the directories within a forest, the *Active Directory* role user must be able to read the *CN=Partitions, CN=Configuration, DC=ROOTDOMAIN, DC=COM* folder.
- If you are importing a Universal group that does not belong to a global catalog:
  - The *Active Directory* role contacts several ADs. The *Active Directory* role user must have the necessary permissions to access the different ADs within a forest.
  - The default port used to contact the AD is 389. If you are using a different port, you must append it to the AD server name defined in the **Active Directory** field on the *Properties* tab, for example: **ADServer.Genetec.com:3393**.
- If you are importing a Universal group that belongs to a global catalog:
  - The global catalog must be updated to include the attributes required for Security Center user and cardholder information. For the list of required attributes, see Global catalog attributes.
  - The default port used to contact the AD is 3268. If you are using a different port, you must append it to the AD server name defined in the **Active Directory** field on the *Properties* tab. The name and port number must be separated by a colon, for example: **ADServer.Genetec.com:3295**.

Benefits of using a global catalog

A global catalog stores a copy of all AD objects in a forest which provides many benefits:

- The need to query multiple domains for information is eliminated since everything is stored in the global catalog.
- Less time to process information.
- Less bandwidth used.
- Less replication of information.
- Requires only a single *Active Directory* role connection. All users can access Security Center using the global catalog.

Importing security groups from an Active Directory

To have a centralized personnel management system, you can import AD security groups into Security Center as user groups or cardholder groups.

Before you begin

If you are importing a universal group from a global catalog, read About universal groups and global catalogs.

What you should know

- When importing an AD security group, you must import all members of that group. If you want to import only a subset of its members, for example, only Security Center users, you must define a new AD security group with only the members you want to import.
- If you are integrating multiple ADs into Security Center, they must each belong to a different domain.
- If you have servers in your system that are running an earlier version of Security Center, you must upgrade the servers to the current version before using them to host a new Active Directory role.
- An AD security group can be imported as user group, cardholder group, or both.

To import a security group:

1 Open the **System** task, and click the **Roles** view.

2 Click **Add an entity** (✚) and select **Active Directory**.

3 On the **Specific info** page, do the following:

a) (If you have multiple servers in your system) From the **Server** drop-down list, select the *server* on which you want to host the role.

b) In the **Active Directory** field, enter the Host name or the IP address of the AD server.

If you are not using a default port, you must append the port number you are using to the AD server name, separated by a colon. For example, **ADServer.Genetec.com:123**. The default ports are as follows:

- Active Directory with no SSL: 389
- Active Directory with SSL: 636
- Global catalog no SSL: 3268
- Global catalog with SSL: 3269

c) Specify how you want the role to connect to the AD server.

You must have read access to the selected AD service.

- Use the Windows credentials assigned to the Genetec™ Server service that is running on the server hosting the Active Directory role.
- Specify a different set of Windows credentials (username, password).

4 On the *Basic information* page, enter the name, description, and partition where you want to create the Active Directory role.

5 Click **Next**, **Create**, and **Close**.

A new Active Directory role ( ) is created. Wait a few seconds for the role to connect to the AD server.

6 (Optional) If you are importing a universal group that connects to a global catalog, turn on the **Use global catalog** option.

7 On the **Properties** tab, select the AD security groups you want to import.

NOTE: There are two types of groups in Windows Active Directory: *distribution groups* and *security groups*. Security Center can only synchronize with security groups.

a) Click **Add an item** (+).

b) Select the security groups you want to add to your Active Directory role.

Use one of the following methods:

- (Recommended) Type the name of the group in **Find Active Directory groups,** and click 🔍.

  If the text you entered matches a single group, it is automatically added to the **Selected groups** list.

  If the text you entered matches multiple group names, a second dialog box appears listing all the group names that match the text you entered.

  Select the ones you want, and click **OK** to add them to the **Selected groups** list.

- From the **Selected groups** list, click (+).

  The *Active Directory members* dialog box appears.

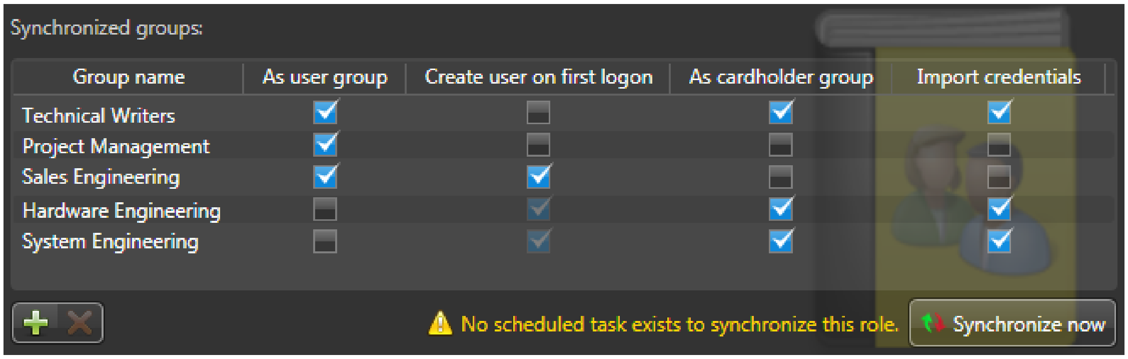
  Select a security group, and click **OK**. Only security groups can be synchronized. If you selected an item that is not a security group, the **OK** button remains disabled.

NOTE: The names shown in the dialog box are display names. Security Center only synchronizes the account names because they are guaranteed to be unique. Typically, the display names and the account names are the same. The only way to tell them apart is that the display names contain spaces.

c) Repeat the previous step as often as necessary until all security groups you want to synchronize with the AD are listed in **Selected groups**, and then click **OK**.

The selected groups are listed under **Synchronized groups** in the **Properties** tab.

8 For each of the synchronized groups, specify how you want to import them.



Synchronized groups:

Group name	As user group	Create user on first logon	As cardholder group	Import credentials
Technical Writers	☑	☐	☑	☑
Project Management	☑	☐	☐	☐
Sales Engineering	☑	☑	☐	☐
Hardware Engineering	☐	☑	☑	☑
System Engineering	☐	☑	☑	☑

⚠ No scheduled task exists to synchronize this role.

The following options are available:

- **As user group:** Select this option to import the synchronized group as *user group*, and the group members as *users*.
- **Create user on first logon:** This is the default option, and it creates an empty user group. User entities are only created when someone tries to logs on the first time. This option avoids having to create all user entities at once, which can freeze up the system. If you clear this option, all user entities are created at the same time as a user group.
- **As cardholder group:** Select this option to import the synchronized group as *cardholder group*, and the group members as *cardholders*. All synchronized cardholders are created at once.
- **Import credentials:** Select this option to import the credential information of the synchronized cardholders.

9 If you are importing the AD security group as cardholder group, select which cardholder fields you want to synchronize with the AD.

10 (Optional) Map custom fields to synchronize with the AD.

11 Click **Apply**, and then click **Synchronize now** (⇅).

All synchronized groups and their members are imported as Security Center entities according to your specifications, with a yellow arrow (↗) superimposed on their icon.

After you finish

Some additional configuration might be required, depending on what you synchronized with the AD:

- If you already had entities configured in your system, you might need to resolve certain conflicts due to the import.
- (Optional) Configure the imported user groups with proper privileges and security options, so that when new user entities are created, they can automatically inherit these properties from their parent user group.
- (Optional) Configure the imported cardholders and cardholder groups.
- (Optional) Create a scheduled task to synchronize imported entities with the AD on a regular basis.

After you create a scheduled task, the warning message **No scheduled task exists to synchronize this role** disappears from the **Properties** tab.

Related Topics
Integration with Windows Active Directory on page 318
Custom card formats on page 567
About federated entities on page 190

Mapping custom fields to synchronize with Active Directory

In addition to default attributes, you can import other attributes from the AD by mapping them to Security Center custom fields. The custom field mapping can be different for each Active Directory role in your system.

Before you begin

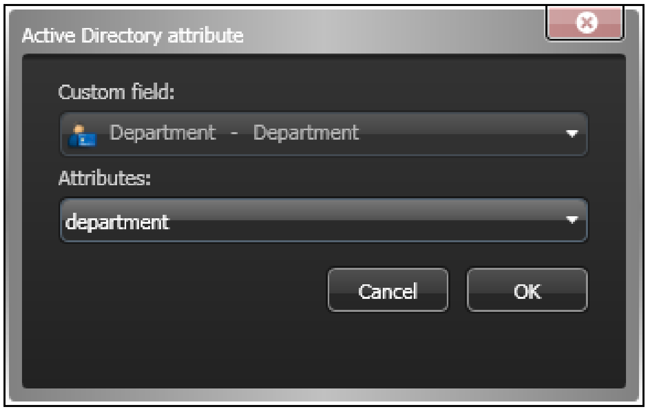
- Make sure that the workstation where Config Tool is running is on the same network domain as the AD server.
- Define the custom fields that will receive data from the AD.

What you should know

No more than 32 custom fields can be mapped to the AD.

To map custom fields to synchronize with Active Directory:

1 From the **Links** tab of the Active Directory role, under **Custm fields**, click **Add an item** (+).



Custom field: Department - Department

Attributes: department

2 Select the custom field and the AD attribute, and then click **OK**.

IMPORTANT: The data type of the custom field must match that of the AD attribute: text with text, decimal with decimal, date with date, etc. The Security Center image data type must be mapped to the AD binary data type, and the mapped AD attribute must contain a valid JPEG image.

The new mapping appears in the **Links** tab.

3 Repeat the previous steps as needed.

4 Click **Apply**.

The mapped custom fields are displayed in the **Links** tab. When you synchronize with the AD, they are read-only.

Resolving conflicts caused by imported entities

Conflict resolution might be necessary if you have existing entities (users and/or cardholders) in your database prior to importing entities from the AD.

What you should know

When a synchronized entity has the same name as a local entity, the Active Directory role sees it as a potential conflict. You can use the *Conflict resolution* tool to merge local entities with synchronized ones, by copying the non-synchronized fields from the local entity to the synchronized entity ( ). The relationships the local entity had with other entities in the system are also copied. When the merge is complete, the local entity is deleted, eliminating duplicate entities.

To resolve conflicts caused by imported entities:

1. Open the **System** task, and click the **Roles** view.
2. Select the Active Directory role ( ), and click **Conflict resolution** ( ).

   The **Active Directory conflict resolution** dialog box appears. All synchronized entities are listed to the left. The ones that conflict with a local entity are flagged in green.

3. Select a conflicting entity from the **Synchronized entities** list.

   All local entities that can be merged with the imported entity are listed to the right. Do one of the following:

   - Select **No selection** if you do not wish to merge it with a local entity.
   - Select the local entity to be merged with the imported entity.
4. Repeat the previous step for all synchronized entities flagged in green.
5. Click **Finish** to save the conflict resolution decisions to a file on disk.

   The default file name is *Conflict_Manifest.data*. Be sure to save the file to a location that can be accessed from your main server and all servers hosting the Access Manager role.

6. (Optional) If you have user conflicts to resolve, apply the conflict manifest to your Directory database.
   a) Connect to the Server Admin of your main server with a web browser.
   b) In the **Directory** tab, under the **Database** section, click **Resolve conflicts** ( ).
   c) In the dialog box that appear, browse to the *Conflict_Manifest.data* file.
   d) Click **Resolve conflicts**, then click **Back up**.

   The conflict resolution status is shown in a independent dialog box.
7. (Optional) If you have cardholder conflicts to resolve, apply the conflict manifest to your Directory database and your Access Manager database.
   a) Select your Access Manager role from the **Roles** view of the **System** task.
   b) Click the **Resources** tab, and click **Resolve conflicts** ( ).
   c) In the dialog box that appears, browse to the *Conflict_Manifest.data* file.
   d) Click **Resolve conflicts**, then click **Back up**.

   The conflict resolution status is shown in a independent dialog box.

After conflict resolution, all synchronized entities that are merged with a local entity inherit their local properties, and all merged local entities are deleted.

Deactivating users imported from an Active Directory

If you have users that are imported from an Active Directory, you can set the user’s status to inactive. The user becomes desynchronized from the AD until you activate the user again.

To deactivate a user imported from an Active Directory:

1 Open the **Security** task.

2 Select an imported user (👤), and click the **Properties** tab.

3 Set the **User status** option to **Inactive**.

4 Click **Apply**.

The user is no longer synchronized with the AD. It will only become synchronized again once you set the user’s status to **Active**.

Logging on to Security Center using an Active Directory user

When you’re signed on to Windows using an account that happens to be synchronized with Security Center, you can log on to Security Center without having to retype your username and password.

To log on to Security Center using an Active Directory user:

1 In the Security Center **Logon** dialog box, do one of the following:

- Use the single logon option by selecting **Use Windows credentials**.

  TIP: If you are already signed on to Windows using the account that is synchronized to your Security Center user, then use the single logon option.

- If multiple Active Directories are integrated into your system, enter the Windows domain along with your username (for example `genetec\dtsiang`), and then enter your password.

  NOTE: This is to let Security Center know which AD service to call for the validation of your credentials.

2 Click **Log on**.

Global catalog attributes

For the *Active Directory* role to successfully connect to a global catalog and synchronize users and cardholders in Security Center, the global catalog must be updated to include specific attributes.

User attributes

The global catalog must be updated with the following user attributes:

- distinguishedName
- objectGUID
- objectClass
- cn
- objectSid
- sAMAccountName
- displayName
- name
- mail
- description
- userPrincipalName
- userAccountControl
- accountExpires
- givenName
- sn
- tokenGroup
- memberof (For the SDK only)
- any attributes to be used in the Links tab

Group attributes

The global catalog must be updated with the following group attributes:

- distinguishedName
- objectGUID
- objectClass
- cn
- objectSid
- sAMAccountName
- name
- mail
- description
- groupType
- member

Container, domain, and organizational unit attributes

The global catalog must be updated with the following container, domain, and organizational attributes:

- distinguishedName
- objectGUID
- objectClass
- objectSid
- displayName
- name
- member

20

Claims-based authentication

This section includes the following topics:

What is claims-based authentication?

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

What is a claim?

A claim is a statement, such as a name, identity, key, or group, made by one subject about itself or another subject. Claims are issued by a provider, and they are given one or more values and then packaged in security tokens that are issued by a security token service (STS).

When do I need claims?

You need claims when you have external users who need to log on to your system and your company's IT service does not have the means to verify that they are who they claim to be. This is the case when the users are neither managed by Security Center nor imported from your company's Active Directory.

What are the benefits of claims?

Claims decouple the process of *authentication* from the process of *authorization*. The benefit of this decoupling is that it allows for *single sign-on* (the use of a single user authentication across multiple IT systems or even organizations).

In the context of Security Center, the process of authentication is handled by a custom *STS* or an *Active Directory Federation Services* server, and the process of authorization is handled by Security Center itself, through partitions and privileges.

Limitations

- Security Center only supports WS-Trust family protocols. WS-Federation passive authentication is not supported.
- *Multi-Factor Authentication (MFA)* is not supported by Security Center. Only classic authentication (username + password) and Windows authentication (**Use Windows credentials** option) are supported.
- Users federated through ADFS are only created in Security Center on first logon. You do not have the option to create all imported users at once like for Active Directory integration.

Requirements

In order to use ADFS for authentication, the following conditions must be met:

- The client workstation must be able to reach the ADFS server.
- The HTTPS encryption certificate of the ADFS service must be trusted by the client workstation.

Performance impact

- The scalability of the Directory is not impacted by this feature.
- User logons using ADFS credentials are expected to take slightly longer than regular logons, because they require that the client workstations connect to one or more remote ADFS servers before connecting to the Directory.

Backward compatibility

Claims-based authentication through ADFS is supported for client workstations running an older version of Security Desk or SDK, but only if the password is entered by the user. The **Use Windows credentials** option in the *Logon* dialog box only works for version 5.4 and later.

Deploying claims-based authentication through ADFS

You can use an *Active Directory Federation Services* server as the *claims provider* for Security Center, and allow users outside your company to log on to your system by establishing a trust chain from third-party's ADFS servers to your company's Security Center main server.

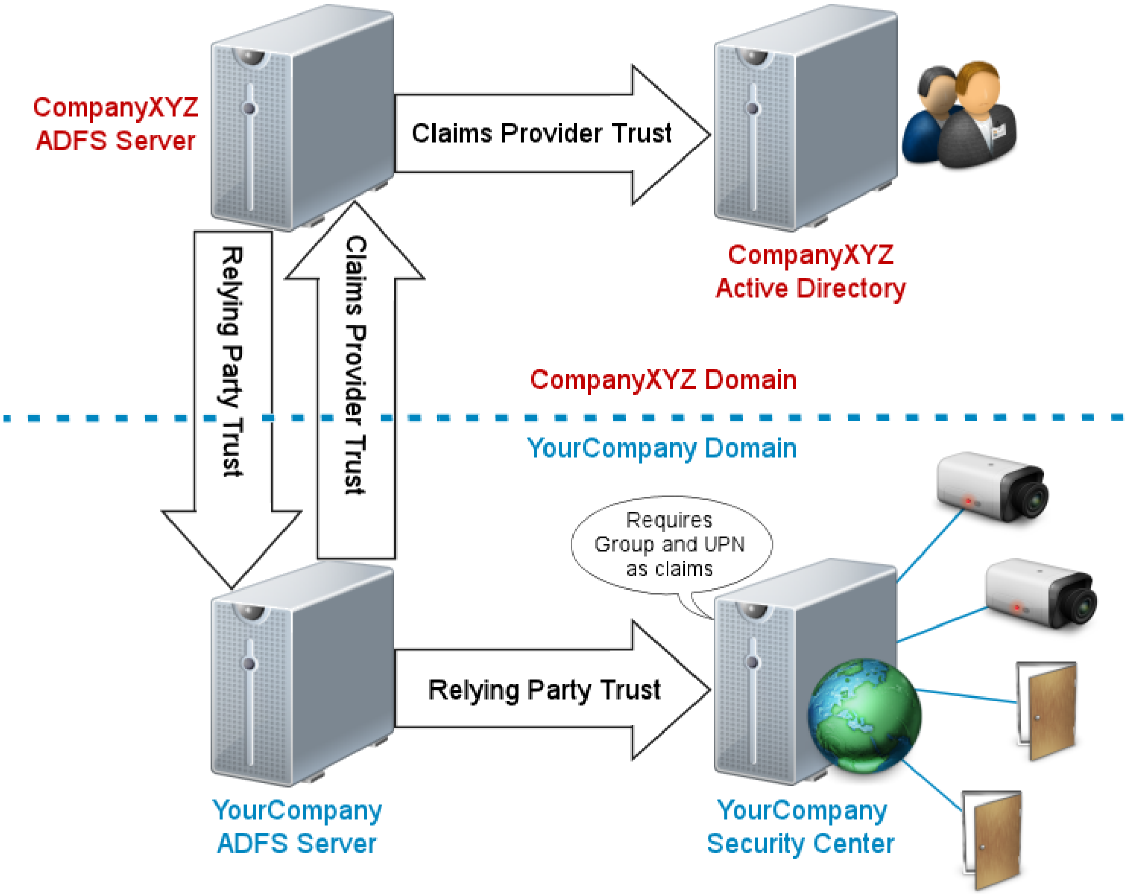
Before you begin

It is assumed that you are familiar with the concepts of claims-based authentication and that your company's ADFS server is operational. For general information on ADFS installation and configuration, please refer to the documentation provided by Microsoft®.

What you should know

For illustration purposes, let's assume that you want to allow external users from Company XYZ to access your company's Security Center system. Company XYZ has its own ADFS server that relies on its own Active Directory as claims provider. Company XYZ's servers are not on the same domain as your company's servers. Your company's ADFS server relies on Company XYZ's ADFS server as claims provider, and in turn, acts as claims provider to your company's Security Center system. Therefore, a chain of trusts must be established from the Company XYZ's Active Directory to the main server of your company's Security Center system.

NOTE: Security Center requires specific attributes as *claims*: *Group* and *UPN (User Principal Name)*.



BEST PRACTICE: If you want to accept security groups from your local Active Directory as Security Center user groups, do not federate them through the ADFS role, but import them through the Active Directory role instead. The latter approach offers more functionalities, such as the synchronization of all standard fields (first name, last name, email address, and so on), custom field mapping, and the option to create all users at role synchronization time.

To deploy claims-based authentication through ADFS:

1 Configure the trust chain outside your company's domain.

  Make sure that the following tasks are performed by the Company XYZ's IT personnel.

  a) Add a claims provider trust to Company XYZ's ADFS server for Company XYZ's Active Directory.
  b) Add a relying party trust to Company XYZ's ADFS server for your company's ADFS server.

2 Configure your local ADFS server as the claims provider for your Security Center system.

  a) On your company's ADFS server, open the AD FS Management snap-in.
  b) Add a claims provider trust to your ADFS for the third-party ADFS server.
  c) Configure the claim rules for the third-party claims provider.
  d) Add a relying party trust to your ADFS server for Security Center.
  e) Configure the claim rules for Security Center, the relying party you just added.

3 Configure your Security Center system to receive claims from your local ADFS server.

  a) Connect to your Security Center system with Config Tool.
  b) Create a user group for each ADFS group you accept as Security Center user groups.
  c) Create the Active Directory Federation Services role.

All users authenticated through ADFS must log on using fully qualified usernames, meaning that they must add their domain name to their usernames, such as in `user@CompanyXYZ.com`.

IMPORTANT: There is currently a known issue regarding the use of a local Active Directory and ADFS. When you have external users authenticated through ADFS in your system, all users imported from your local Active Directory must also use fully qualified user names, even though they belong to the same domain as your Security Center system.

Adding a claims provider trust for a third-party ADFS

To allow users from an external organization (Company XYZ) to connect to your Security Center system, your company's ADFS server must trust the claims provided by Company XYZ's ADFS server.

Before you begin

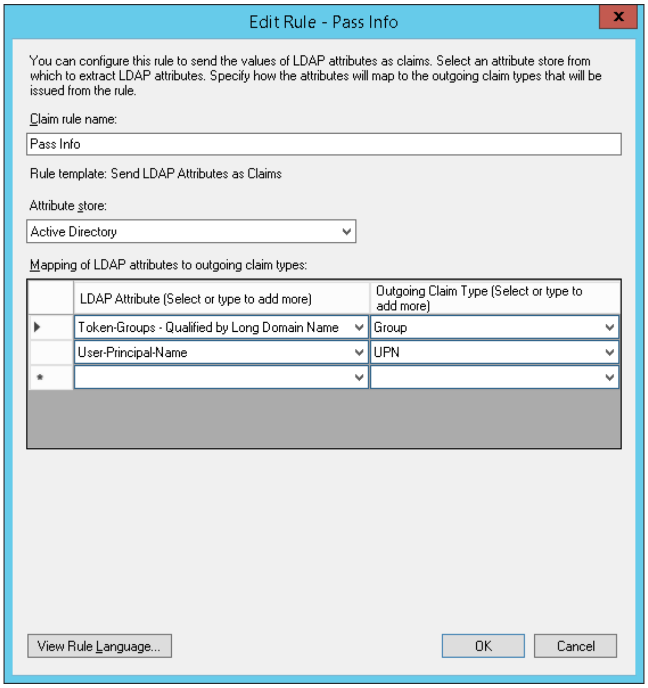
Make sure Company XYZ has done the following:

- Add a claims provider trust to Company XYZ's ADFS server for Company XYZ's Active Directory.
- Add a relying party trust to Company XYZ's ADFS server for your company's ADFS server.

What you should know

This task is part of the deployment process for claims-based authentication using ADFS based on a sample scenario.

NOTE: Security Center requires specific attributes as *claims*: *Group* and *UPN (User Principal Name)*.



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
Pass Info

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	Token-Groups - Qualified by Long Domain Name	Group
	User-Principal-Name	UPN
*		

Adding a claims provider trust to your company's ADFS server is outside the scope of this document. For information on these topics, see the documentation on ADFS from Microsoft®.

Configuring claim rules for a third-party claims provider

After you created the claims provider trust on your ADFS server for the third-party ADFS server, you must configure what claims the latter must forward to your ADFS server.

Before you begin

The *AD FS Management* window must be open on your ADFS server, and the claims provider trust must be created for the third-party ADFS server.

What you should know

This task is part of the deployment process for claims-based authentication using ADFS based on a sample scenario.

To configure the claim rules for the third-party claims provider:

1 In the *AD FS* window, click **Trust Relationships** > **Claims Provider Trusts**, select the claims provider that corresponds to the third-party ADFS, and click **Edit Claim Rules** in the *Actions* pane.

The *Edit Claims Rules* window opens.

2 If no claim rule exists for **UPN**, add one.

a) Click **Add Rule**.

b) In the **Claim rule template** drop-down list, select **Pass Through or Filter an Incoming Claim**, and click **Next**.

c) Configure the rule and click **Finish**.

- **Claim rule name:** Enter a name that helps you remember the rule.
- **Incoming claim type:** Select **UPN**.
- **Pass through only claim values that match a specific email suffix value:** Select this option, and enter an email suffix value. For example: `CompanyXYZ.com`.

  BEST PRACTICE: It is recommended to filter the claims coming from a third-party claims provider as a security precaution, so that the third-party claims provider cannot send unexpected values. This is done, for example, to prevent Company XYZ from pretending that its users are from your company, and get elevated privileges. **Pass through all claim values** should be avoided when dealing with third-party claims providers.

3 If no claim rule exists for **Group**, add one.

a) Click **Add Rule**.

b) In the **Claim rule template** drop-down list, select **Pass Through or Filter an Incoming Claim**, and click **Next**.

c) Configure the rule and click **Finish**.

- **Claim rule name:** Enter a name that helps you remember the rule.
- **Incoming claim type:** Select **Group**.
- **Pass through only claim values that start with a specific value:** Select this option, and enter a start value. For example: `CompanyXYZ\` or `CompanyXYZ.com\`. Ask your IT department to find out which form should be used.

4 Click **Apply**.

Adding a relying party trust for Security Center

For an ADFS server to act as the *claims provider* for your Security Center system, you must add your Security Center system to the relying party trusts of the ADFS server.

Before you begin

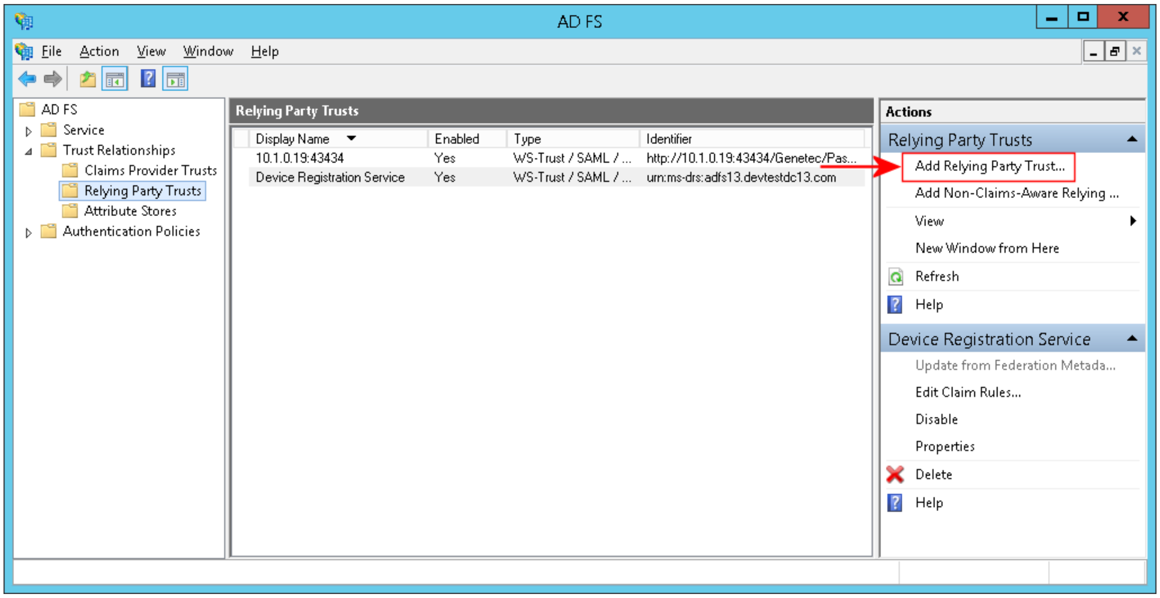
The *AD FS Management* snap-in window must be open on your ADFS server.

What you should know

This task is part of the deployment process for claims-based authentication using ADFS based on a sample scenario.

To add a relying party trust to your ADFS server for Security Center:

1 In the *AD FS* window, click **Trust Relationships** > **Relying Party Trusts** > **Add Relying Party Trust**.



Display Name	Enabled	Type	Identifier
10.1.0.19:43434	Yes	WS-Trust / SAML / ...	http://10.1.0.19:43434/Genetec/Pas...
Device Registration Service	Yes	WS-Trust / SAML / ...	urn:ms-drs:adfs13.devtestdc13.com

The *Add Relying Party Trust Wizard* window opens.

2 Click **Start** > **Enter data about the relying party manually** > **Next**.

3 In **Display name**, enter a name that represents your company's Security Center system.

For example, `YourCompany Security Center`.

4 Click **Next**, select **AD FS profile**, and then click **Next**.

A token encryption certificate may be entered, but it is optional and it is not required for Security Center because Security Center does not use any confidential or secret information in its *security tokens*, and tokens are only sent over secured channels within Security Center, never in clear over the network.

5 Click **Next**, and then **Next**.

Do not enable WS-Federation or SAML 2.0 support.

6 In **Relying party trust identifier**, enter a string to identify the *main server* of your Security Center system, and then click **Next**.

An example would be to use the URL of your main server: `https://MainServer.YourCompany.com`.

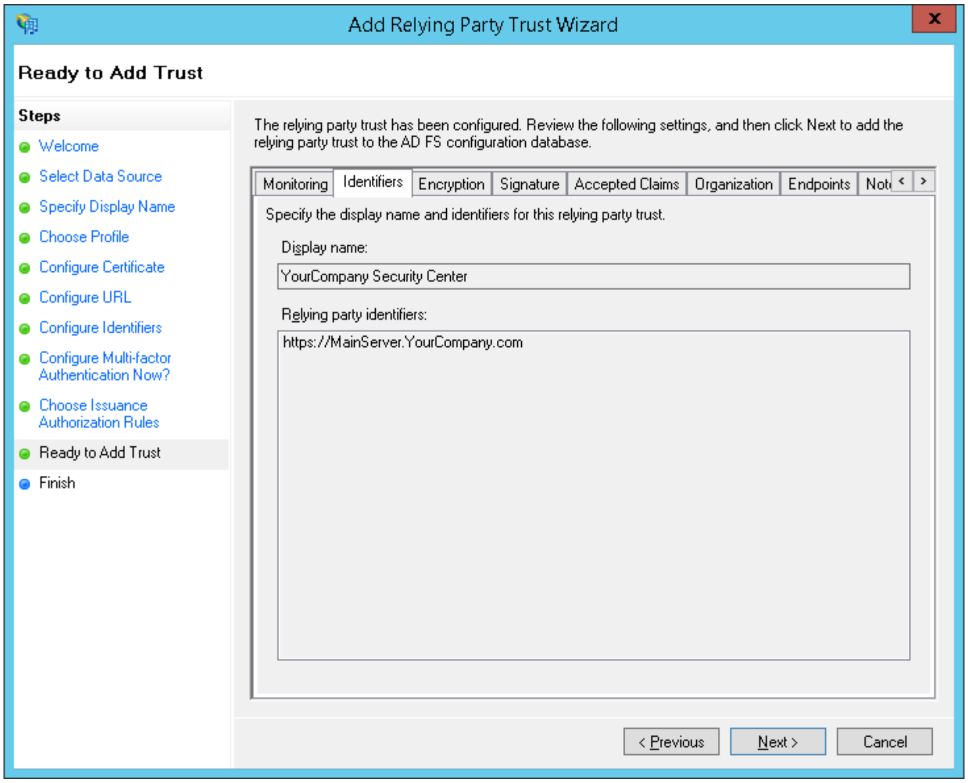
IMPORTANT: Write this name down, because you need to enter exactly the same identifier in a subsequent step, when you configure your ADFS role on the Security Center server.

7 Click **I do not want to configure multi-factor authentication settings...**, and then click **Next**.

8 Choose the option for the initial behavior of this relying party's **Issuance Authorization Rules**, and click **Next**.

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose between **Permit all users** and **Deny all users**. The simplest choice is to permit all users. Advanced ADFS administrators can choose to deny all users by default and manage issuance rules manually.

9 Click **Identifiers**, and review the **Display name** and **Relying party identifiers** you entered, and click **Next**.



The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the display name and identifiers for this relying party trust.

Display name: YourCompany Security Center

Relying party identifiers: https://MainServer.YourCompany.com

10 Leave the option **Open the Edit Claim Rules dialog...** selected, and click **Close**.

Configuring claim rules for Security Center

After you created the relying party trust on your ADFS server for Security Center, you must configure what claims Security Center requires.

Before you begin

The *AD FS Management* window must be open on your ADFS server, and the relying party trust must be created for your Security Center main server.

What you should know

This task is part of the deployment process for claims-based authentication using ADFS based on a sample scenario.

To configure the claim rules for Security Center:

1 In the *AD FS* window, click **Trust Relationships** > **Relying Party Trusts**, select the relying party that corresponds to your Security Center system, and click **Edit Claim Rules** in the *Actions* pane.

The *Edit Claims Rules* window opens.

2 Add a first claim rule for **UPN**.

a) Click **Add Rule**.

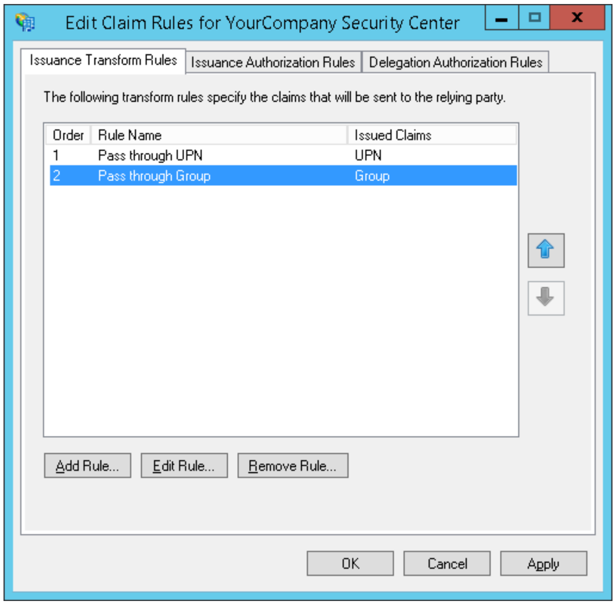
b) In the **Claim rule template** drop-down list, select **Pass Through or Filer an Incoming Claim**, and click **Next**.

c) Configure the rule and click **Finish**.

- **Claim rule name:** Enter a name that helps you remember the rule.
- **Incoming claim type:** Select **UPN**.
- **Pass through all claim values:** Select this option.

3 Add a second claim rule for **Group**.

Follow the instructions for UPN claim rule. Only this time, change **UPN** to **Group**.


Edit Claim Rules for YourCompany Security Center
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Pass through UPN	UPN
2	Pass through Group	Group

Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

4 Click **Apply**.

Mapping remote ADFS groups to Security Center

To accept remote ADFS groups as valid user groups in Security Center, you must create a Security Center user group for each of them.

Before you begin

All ADFS servers involved in the trust chain must be fully configured.

To map accepted remote ADFS groups to Security Center:

1. Create a user group for each ADFS group you accept as Security Center user groups.

   The user groups must have the exact same name as defined in the remote Active Directories, followed by the remote ADFS domain name.

   For example, if the company XYZ domain has a user group called *Operators*, then the user group in Security Center must be named *Operators@CompanyXYZ.com*.

2. Apply the desired access rights and privileges to these user groups.

After you finish

Add the user groups mapped to remote ADFS groups to the list of Accepted user groups in your ADFS role.

Creating Active Directory Federation Services roles

In order for Security Center to receive claims from an ADFS server, you need to create and configure an ADFS role within Security Center.

Before you begin

- All ADFS servers involved in the trust chain must be fully configured.
- Map the accepted remote ADFS groups to Security Center user groups.

What you should know

Active Directory Federation Services (ADFS) is a component of the Microsoft® Windows® operating system that issues and transforms claims, and implements federated identity. It is also a type of role that enables Security Center to receive claims from an external ADFS server.

You need to create one ADFS role in Security Center for each root ADFS you have. In our sample scenario, your local ADFS server is your root ADFS, therefore you only need to create one ADFS role.

In a situation where you do not have a local ADFS server, but multiple independent third-party ADFS servers acting as *security token services* for Security Center, then you need to create an ADFS role for each of them, and add a relying party trust for Security Center to each of these ADFS server's configuration.

To create an ADFS role:

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

2 Click **Add an entity** (+) > Active Directory Federation Services.

3 In the **Basic information** page, enter a name and description for the role.

4 Select a **Partition** this role is a member of, and click **Next**.

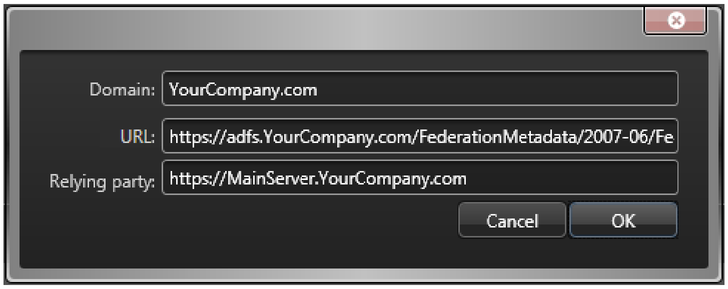
Partitions determine which Security Center users have access to this entity. Only users that are part of the partition can view or modify the ADFS role.

5 Click **Next** > **Create** > **Close**.

A new ADFS role (🌐) is created.

6 Click the **Properties** tab, and configure the **Trust chain (domains)**.

a) Click **Add an item** (+), configure the ADFS server, and click **OK**.



Domain: YourCompany.com

URL: https://adfs.YourCompany.com/FederationMetadata/2007-06/Fe

Relying party: https://MainServer.YourCompany.com

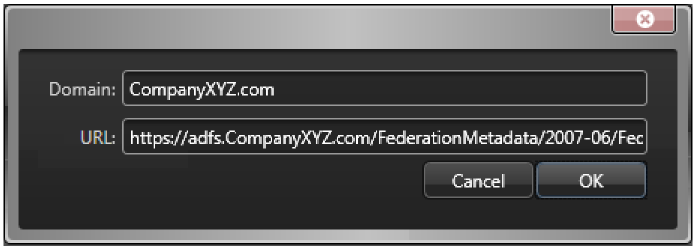
- **Domain:** This is your local ADFS server's domain. Example: `YourDomain.com`.
- **URL:** This is the address of your ADFS server's metadata document. It is always in the following format:

  ```
  https://adfs.YourCompany.com/FederationMetadata/2007-06/
  FederationMetadata.xml
  ```

  Simply replace `adfs.YourCompany.com` with the name of your ADFS server.
- **Relying party:** This is the identifier that was entered as the **Relying party identifier** when you added the relying party trust for Security Center.

This is how Security Center identifies itself as the relying party to the ADFS server, even when the role fails over to another server.

b) Click **Add an item** (➕), configure the remote ADFS server, and click **OK**.



Domain: CompanyXYZ.com

URL: https://adfs.CompanyXYZ.com/FederationMetadata/2007-06/Fec

- **Domain:** This is your remote ADFS server's domain. Example: `CompanyXYZ.com`. Users from that domain must append the domain to their usernames when they log on to Security Center. Example: `johnny@CompanyXYZ.com`.
- **URL:** This is the address of the remote ADFS server's metadata document. It is always in the following format:

  ```
  https://adfs.CompanyXYZ.com/FederationMetadata/2007-06/FederationMetadata.xml
  ```

  Simply replace `adfs.CompanyXYZ.com` with the name of the remote ADFS server.

c) If you configured more than one remote ADFS servers as claims providers to your local ADFS server, add them now.

7 Configure the external user groups that Security Center is going to accept.

a) In the *Accepted user groups* section, click Click **Add an item** (➕).

b) In the dialog box that appears, select the user groups mapped to the remote ADFS groups, and click **OK**.

All users who are members of the accepted user groups would be able to log on to your system. They must all append their domain name after their username in order to log on. Security Center does not keep nor validate their passwords. The ADFS server does. Security Center simply trusts them as authentic users if the ADFS accepts them.

8 Click **Apply**.

21

Fusion stream encryption

This section includes the following topics:

What is fusion stream encryption?

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

What is a fusion stream?

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

Benefits of fusion stream encryption

The benefits of fusion stream encryption are as follows:

- No data captured by Security Center is stored or transmitted as *plaintext*. This means that the privacy of your data is protected even if you outsource the management of your data center.
- Data streams are encrypted using the US government approved AES 128-bit encryption standard.
- The keys used to encrypt the data streams change every minute, discouraging any kind of brute-force attack.
- Each data stream is encrypted with a different key stream, reducing the attack surface.
- The key streams are encrypted using *public key encryption*, ensuring that only authorized client machines (with a valid *private key* installed) can view the encrypted data.
- If a private key is compromised (leaked out), you can prevent it from ever being used again on your system.
- Encryption overhead is kept to a minimum by encrypting the data stream only once. Auxiliary Archivers do not have to re-encrypt the data.

Limitations

The limitations of fusion stream encryption are as follows:

- Multicast from the camera is disabled when data streams must be encrypted.
- Recordings on the edge cannot be encrypted. Turn edge recording off if you want encryption.
- Encrypted video cannot be viewed with Security Center 5.3 and earlier.
- Encrypted video cannot be viewed on Security Center Mobile devices.
- Software motion detection is not possible when encryption is on.
- Thumbnails cannot be generated for encrypted video.
- Encryption cannot be added after the video has been archived.

  However, you can still encrypt your exported video files. For more information, see the *Security Desk User Guide*.
- New encryption keys cannot be added to archived data,which means that authorization to view archived data cannot be granted to new machines.
- Encryption certificates are only validated for expiration dates. This means that any certificate you enroll takes effect immediately, regardless of its activation date.
- Encryption cannot be removed from the video archives.

The workaround is to export your video in ASF format.

- Encrypted video cannot be exported in legacy G64 format.

  When you export encrypted video in G64x format, the video is exported with encryption. All the information necessary in order for authorized client machines to decrypt the video are found in the G64x file.
- Encrypted video cannot be recovered if you lose your private keys.

  See Best practices for managing private keys on page 352.

How does fusion stream encryption work?

The application of *fusion stream encryption* requires that all client machines authorized to view encrypted data have a *private key* installed. The private key must match one of the *encryption certificates* configured on the Archiver.

Two-level encryption

The Archiver uses a two-level encryption strategy to protect the privacy of your data.

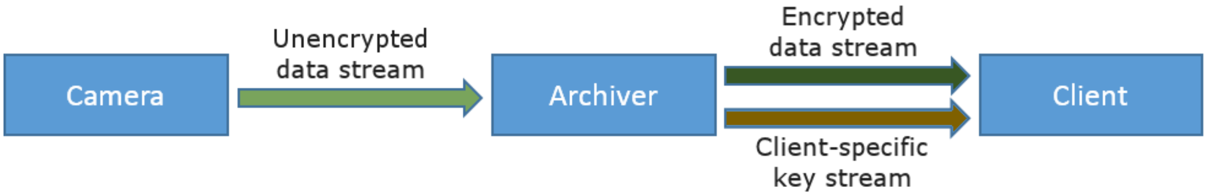
- First-level encryption: The Archiver receives the data stream as *plaintext* from the camera. Then the Archiver encrypts the data stream using randomly generated *symmetric keys* that change every minute. The stream of symmetric keys is called the *master key stream*. The master key stream is the *first key* needed to unlock the private data. It is shared by all client machines.
- Second-level encryption: To ensure that only authorized clients can access the master key stream, the Archiver protects it using *public key encryption* (see RSA). The Archiver encrypts the master key stream individually for each authorized client, using a *public key*. Only the client that has the *private key* (matching the public key) installed can unlock the master key stream (the *first key*). The private key is the *second key* needed to unlock the private data. This private key must be kept on the client machine.

The public and private keys are part of an *encryption certificate* that is created for a specific client. The certificate also identifies the client. To enable encryption, the certificate must be stripped of its private key and handed to the Archiver. The Archiver then takes the public key from the certificate to encrypt the master key stream for that client. For this reason, the encrypted master key stream is called the *client-specific key stream*.

When the client requests encrypted data, it identifies itself to the Archiver by sending its certificate along with the data request. Based on the certificate, the Archiver knows which client is requesting the data, and sends the corresponding client-specific key stream with the encrypted data stream to the client. Since only the intended client has the matching private key, only the intended client can decrypt the information.

Summary

All video that must be protected must first go through the Archiver before it is sent to the requesting client. The Archiver encrypts the video, and sends the requested information bundled in a composite stream called the *fusion stream*. The fusion stream contains both the encrypted data streams, and their corresponding client-specific key streams.



If the fusion stream is intercepted by an unauthorized party on its way to the intended client, it remains protected because the unauthorized party does not have the private key, and thus cannot decrypt the data contained within.

BEST PRACTICE: It is recommended to create the encryption certificate on the client machine that will be requesting to view the video. This limits the exposure of the private key.

Related Topics

Preventing users from viewing encrypted data on a specific machine on page 357
Authorizing a new client to view all data from an encrypted camera on page 360

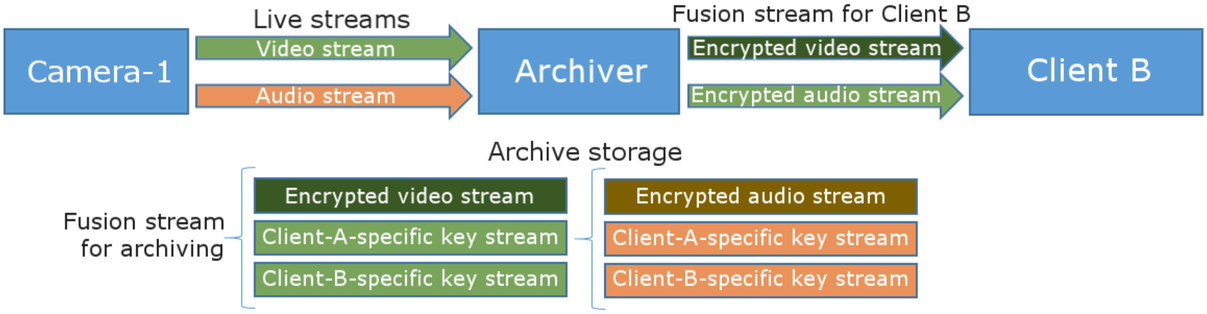
Fusion stream encryption scenarios

When a client machine requests a data stream (video, audio, metadata) from an encrypted camera, the Archiver sends a *fusion stream* containing all the information the client needs, and only what it needs.

Scenario setup

You want all video and audio from Camera-1 to be encrypted. You want Client A and Client B (workstations) to have access. First you request and install an *encryption certificate* on each of them. Then, you enable the encryption on the Archiver in charge of Camera-1, using the certificates you obtained for Client A and Client B.

The following diagram illustrates your setup with Client B requesting video from Camera-1.


Live streams
Fusion stream for Client B
Camera-1
Video stream
Audio stream
Archiver
Encrypted video stream
Encrypted audio stream
Client B
Archive storage
Fusion stream for archiving
Encrypted video stream
Client-A-specific key stream
Client-B-specific key stream
Encrypted audio stream
Client-A-specific key stream
Client-B-specific key stream

What happens when encryption is enabled

- Motion detection by Archiver on Camera-1 is disabled.
- Multicast from Camera-1 is disabled.
- The Archiver generates a fusion stream for archiving, which includes (see illustration):
  - One encrypted video stream.
  - One *client-specific key stream* so Client A can decrypt the video stream.
  - One client-specific key stream so Client B can decrypt the video stream.
  - One encrypted audio stream.
  - One client-specific key stream so Client A can decrypt the audio stream.
  - One client-specific key stream so Client B can decrypt the audio stream.

Scenario: Client B requests only video from Camera-1

- Client B sends a request for video from Camera-1 to Archiver, with its encryption certificate.
- The Archiver responds by sending a fusion stream to Client B, which includes (see illustration):
  - Encrypted video stream.
  - Client-specific key stream for Client B to decrypt the video.

Scenario: Client B requests both video and audio from Camera-1

- Client B sends a request for video and audio from Camera-1 to Archiver, with its encryption certificate.
- The Archiver responds by sending a fusion stream to Client B, which includes:
  - Encrypted video stream.
  - Client-specific key stream for Client B to decrypt the video.

- Encrypted audio stream.
- Client-specific key stream for Client B to decrypt the audio.

Performance impact of fusion stream encryption

Fusion stream encryption impacts the performance of the Archiver and the Security Desk workstations. You may need to reevaluate the type and number of machines you need if you plan on enabling this feature.

Encryption impact on Archiver performance

The first encryption certificate enabled on the Archiver will reduce the capacity of the Archiver by 30%. Each additional encryption certificate applied to all cameras further reduces the Archiver capacity by 4%.

Example

Your Archiver supports 300 cameras without encryption.

Number of certificates enabled	Number of supported cameras
0 encryption certificates (no encryption)	300 cameras
1 encryption certificate	210 cameras
5 encryption certificates	178 cameras
10 encryption certificates	145 cameras
20 encryption certificates	96 cameras

BEST PRACTICE: Do not exceed 20 encryption certificates per Archiver.

Encryption impact on workstation performance

Video encryption can increase the CPU usage by up to 40% when viewing low resolution video (CIF). The impact becomes less noticeable as the resolution of the video increases, because much more processing power is spent on decoding the video than on decrypting the video. The impact on performance becomes unnoticeable when viewing HD and Ultra-HD video.

Best practices for managing private keys

The effectiveness of *fusion stream encryption* relies on an external *public key infrastructure* to manage the *private keys*. The entire security of the system is based on the fact that the private keys remain secret. Hence, the transfer and handling of the private keys must be done in a secure manner.

Safeguarding the private keys

The safest way to handle a public-private key pair is to generate the *encryption certificates* directly on the client machine, then assign this certificate (only the public key part) to the Archiver responsible for performing the encryption. This way, you reduce the attack surface by ensuring that the private key never leaves the client machine where it is used.

If you want to use the same private key on multiple client machines, make sure you distribute it in a secure way. Use a strong password to encrypt the private key while in transit. To learn how to do this, see Import or export certificates and private keys.

After all copies of the private key are installed on the client machines, you can safely delete the temporary files that were used to distribute the private key.

BEST PRACTICE: If your company uses Active Directory Domain Services (ADDS), it is recommended to use the Credential Roaming mechanism, where private keys are associated to user group profiles instead of specific machines.

Preventing private key disclosure

You might worry about users exporting the private keys from their client machines. To reduce this risk, you can follow any of these *defense in depth* best practices.

- **Mark private keys as non-exportable:** To prevent Windows clients from extracting private keys, you can mark private keys as non-exportable.

  You set the non-exportable flag when you import a certificate.

  This is how:

  1. Create a certificate and export the public and private keys in PFX format. Use a strong password to encrypt the private key.
  2. Import only the public key for the Archiver servers.
  3. Import the private key for each individual machine, and set the private key as non-exportable.
     ```
     certutil -importPFX [PFXfile] NoExport
     ```
  4. When the private key has been imported for all machines, destroy the original PFX file.

  IMPORTANT: There are third-party applications that do not enforce the non-exportable flag. Because it is possible to export private keys by using these third-party applications, marking private keys as non-exportable is not entirely foolproof.

- **Run the operator account in unprivileged mode:** You can prevent your Security Desk users from exporting the private keys by installing the certificates on the local computer store instead of the users' personal stores, and by denying them administrator privileges. However, Security Desk still needs to have access to the private keys. This means that you need to run Security Desk as an administrator, and enter the password for the Security Desk users.

- **Restrict the use of applications through Windows Group Policy:** You can prevent the Security Desk users from accessing the private keys by blocking the tools used to manipulate the certificates, such as *certmgr.msi*, through Windows Group Policy.

Creating a private key backup

If you lose your private keys, you cannot recover your encrypted data. It is recommended that you use of a secured backup client machine to create an extra encryption certificate for all of the data that you encrypt. The private key corresponding to this certificate must not be used on any other client machine. The sole purpose of this backup machine is so that you have a backup solution in case all private keys used on your client machines are lost.

Setting up fusion stream encryption

To set up *fusion stream encryption*, you need to request and install *encryption certificates* on the machines that are authorized to view encrypted cameras, and then use those certificates to enable this feature on the Archiver.

What you should know

Fusion stream encryption is for the protection of your data privacy. To protect your data against tampering, see Protecting video files against tampering on page 452.

To set up fusion stream encryption:

1. Request and install the encryption certificates on the client machines that are authorized to access your company's private data.
2. Enable encryption on your Archiver or individual cameras.

Requesting and installing encryption certificates

To authorize a client machine to view encrypted data, you must request an *encryption certificate* from the client machine, install the certificate with the *private key* locally, and hand the certificate with only the *public key* to the Archiver in charge of encryption.

Before you begin

There are many ways to request and manage *digital certificates*. Before you proceed, consult your IT department about the policies and standard procedures followed at your company.

What you should know

The encryption certificate contains a pair of public and private keys. The public key is used by the Archiver to encrypt the private data for a specific client machine. The private key is used by the client machine to decrypt the private data.

BEST PRACTICE: The private key should never leave the machine where it is needed.

To request and install an encryption certificate on a client machine:

1. Log on as a local administrator of the client machine.
2. Add the Certificates snap-in to your local computer account.

   Installing the certificates in the local computer store gives you more control over the management of private keys.
3. Follow your company's procedure for requesting and installing the certificate.
4. If the client is only supposed to have access to encrypted data for a limited time, set the certificate's expiry date accordingly.
5. If you do not plan on running the Config Tool from this computer, export the certificate with only the public key to a certificate (.cer) file.

   Save the certificate file to a location that can be accessed from where you plan on running the Config Tool.

After you finish

Enable encryption on your Archiver or individual cameras.

Related Topics

Best practices for managing private keys on page 352

Enabling fusion stream encryption

To protect the privacy of your data, you can enable *fusion stream encryption* on the Archiver role or on individual cameras.

Before you begin

Request and install the encryption certificates on the client machines authorized to access your company's private data.

What you should know

It is not necessary to install the certificates on the Archiver server. The encryption certificates are applied to the Archiver through the Config Tool. For this reason, the Config Tool must have access to the certificates, either from the certificate store of the local machine, or from exported certificate (.cer) files.

IMPORTANT: To enable encryption, you must add at least one certificate to the Archiver.

To enable fusion stream encryption:

1. From the Config Tool home page, open the *Video* task.
2. Do one of the following:
   - To enable encryption on the Archiver, select the Archiver role to configure, and click the **Camera default settings** tab.
   - To enable encryption on a camera, select the camera to configure, click the **Recording** tab, and then click **Custom settings**.
3. Click **Show advanced settings**, and turn **Encryption** on.
4. Under **Certificates**, click **Add an item** (➕).

   The **Select certificate** dialog box appears.
5. Do one of the following:
   - If the encryption certificates are installed on your local computer, select them from the **Installed certificates** list and click **OK**.
   - If they are not installed on your local computer, do the following:
     1. Click **Browse certificate file**.
     2. Click ... to open the browser window, and navigate to the folder where the certificates files are saved.

        The browser looks for **X.509 Certificates** files by default. If you do not find the files you want, look for **Personal Information Exhange** files instead.
     3. Select the certificates you want and click **Open**.
     4. If the certificate file is password protected, click ⊕, and enter the **Password**.
     5. (Optional) Click **Validate file** to make sure the selected file contains a public key.
     6. Click **OK**.
6. Click **Apply**.

The Archiver starts encrypting all data streamed from the selected cameras. Only client workstations with one or more of the configured certificates installed locally are able to view the data recorded from this point on.

Related Topics

Disabling fusion stream encryption on page 356
Preventing users from viewing encrypted data on a specific machine on page 357
Preventing compromised certificates from being used in your system on page 358
Authorizing a client to view new data from an encrypted camera on page 359
Authorizing a new client to view all data from an encrypted camera on page 360

Disabling fusion stream encryption

You can disable *fusion stream encryption* on the Archiver role or on individual cameras.

What you should know

You can disable fusion stream encryption by turning the **Encryption** switch off on either the Archiver or a camera.

BEST PRACTICE: Do not remove the *encryption certificates* from the Archiver in case you want to turn encryption back on.

To disable fusion stream encryption:

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

2 Do one of the following:

- To disable encryption on the Archiver, select the Archiver role to configure, and click the **Camera default settings** tab.
- To disable encryption on a camera, select the camera to configure, click the **Recording** tab, and then click **Custom settings**.

3 Click **Show advanced settings**, and turn **Encryption** off.

4 Click **Apply**.

The Archiver stops encrypting all future data streamed from the selected cameras. Video archives that were encrypted in the past remain encrypted.

Related Topics

Removing encryption from video archives on page 361

Preventing users from viewing encrypted data on a specific machine

If you no longer want people to use a specific client machine to access the data from an encrypted camera, you can remove the *encryption certificate* used to enable *fusion stream encryption* on that camera, from that machine.

What you should know

Access to data from encrypted cameras is controlled through the encryption certificates installed on the machine used to access the data, as opposed to through user privileges. Only follow this procedure if you are changing the configuration of a machine, not because an encryption certificate is compromised. If you think the distribution of an encryption certificate has been compromised, you can prevent it from ever being used again on your system.

IMPORTANT: If this client is the only machine that can access the encrypted camera, make sure you do not lose its encryption certificate (containing the *private key*). If you lose the certificate, you cannot recover the encrypted archives for that camera. If you have only one machine that can view the encrypted camera, follow the recommended best practices for managing private keys.

To stop a client machine from viewing data from an encrypted camera:

1. Log on to the client machine as a local administrator.
2. Add the Certificates snap-in to your local computer account.
3. Delete the certificates corresponding to the encrypted cameras that you no longer want people to view on this machine.
4. If this client is the only one using this certificate, also remove the certificate from the Archiver.

   This prevents the Archiver from performing unnecessary encryption. For information on how to remove a certificate from the Archiver, see Preventing compromised certificates from being used in your system on page 358.

The client will no longer be able to view new or archived data from the camera, so long as the camera remains encrypted.

Related Topics

How does fusion stream encryption work? on page 348

Preventing compromised certificates from being used in your system on page 358

Authorizing a client to view new data from an encrypted camera on page 359

Preventing compromised certificates from being used in your system

If you suspect that an *encryption certificate* has been compromised, you can prevent the certificate from ever being used again in your system by removing it from the Archiver and deleting all key streams that were generated with that certificate.

What you should know

The encryption certificate (containing the *private key*) is what allows a client machine to query the Archiver for encrypted data, and to decrypt the key stream and the data when it is received from the Archiver. For more information, see How does fusion stream encryption work? on page 348

CAUTION: From the Archiver, if you remove the last certificate used to encrypt a camera, the camera ceases to be encrypted and all future data from that camera becomes accessible to all machines in your system. However, data that was previously encrypted remains encrypted.

To prevent an encryption certificate from being used in your system:

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

2 Do one of the following:

- If encryption is configured at the Archiver level, select the Archiver and click the **Camera default settings** tab.
- If encryption is configured at the camera level, select the camera and click the **Recording** tab.

3 From the **Certificates** list, select the compromised certificate, and click **Remove the item** (✖).

NOTE: You cannot leave **Encryption** on if there are no certificates configured.

4 Click **Apply**.

5 In the message box that appears, do one of the following:

- Click **Yes** to delete the selected certificate with the associated key streams (*client-specific key streams*).

  BEST PRACTICE: This is the recommended choice if you know your certificate has been compromised.

  CAUTION: If this certificate is the only certificate from which you can access your encrypted data, deleting it means you can never recover your data.
- Click **No** to delete only the selected certificate from the Archiver, without deleting the associated key streams.

  This option stops the Archiver from generating new key streams from the selected certificate. This prevents the affected client machines from accessing the new data from the encrypted camera. This does not prevent the data that was archived prior to this operation from being accessed from machines on which the selected certificate is installed.

6 Click **Apply**.

Related Topics

Preventing users from viewing encrypted data on a specific machine on page 357
Authorizing a new client to view all data from an encrypted camera on page 360

Authorizing a client to view new data from an encrypted camera

You can grant a new client machine the rights to access the future data from an encrypted camera by adding a new *encryption certificate* (public key) for that client to the Archiver in charge of that camera.

Before you begin

Adding more encryption certificates to an Archiver impacts its performance. See Performance impact of fusion stream encryption on page 351.

What you should know

A client machine has access to encrypted data because the Archiver transmits both the encrypted data stream and the key stream to the client. The key stream gives the client its first key to unlock the encrypted data. The client needs a *second key* to decrypt the *first key*, which is its *private key*. When you add the client's certificate to the Archiver, you are asking the Archiver to create a new *first key* that the client is able to unlock.

IMPORTANT: If this client is the last machine that has access to the data from the encrypted camera, make sure you do not lose its private key. If you do, you will not be able to recover the encrypted archives for that camera. If you are in that situation, follow the recommended best practices for managing private keys.

To authorize a new client to view the new data from an encrypted camera:

1 Request and install an encryption certificate for the new client machine.

2 Add the new certificate (public key) to the Archiver in charge of the camera.

For information on how to do this, see Enabling fusion stream encryption on page 355.

The new client machine can access any new data from the encrypted camera from this point on, but cannot access the data archived prior to this operation.

Related Topics

Preventing users from viewing encrypted data on a specific machine on page 357
Authorizing a new client to view all data from an encrypted camera on page 360

Authorizing a new client to view all data from an encrypted camera

You can grant a new client access to all the data of an encrypted camera by importing the *encryption certificate* (private key) of another client that does have access.

Before you begin

IMPORTANT: Private keys must be handled with care. See Best practices for managing private keys on page 352.

To authorize a new client to view all data from an encrypted camera:

1 Export the certificate of an authorized client machine with the private key.
2 Import the certificate with the private key to the new client machine.

The new client now has all the access rights granted to the original client through the imported encryption certificate. If the original client has access to more than one encrypted camera through this certificate, the new client now has access as well.

Related Topics

How does fusion stream encryption work? on page 348
Preventing compromised certificates from being used in your system on page 358
Authorizing a client to view new data from an encrypted camera on page 359

Removing encryption from video archives

You cannot remove the encryption from your video archives. However, you can export your video archives without encryption, using the ASF format.

Before you begin

You need a client machine authorized to access the encrypted camera, and a Security Center user account that has both the *Use ASF format* and *Remove encryption* privileges.

To export video from an encrypted camera without the encryption:

1. Open Security Desk from the authorized client workstation.
2. Export the video you want in ASF format.

   For information on exporting video, see the *Security Desk User Guide*.

Part IV

Video

This part includes the following chapters:

- "Video at a glance" on page 363
- "Video deployment" on page 366
- "Cameras" on page 396
- "Video archives" on page 431
- "Troubleshooting video" on page 459

22

Video at a glance

This section includes the following topics:

About Omnicast™

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

Omnicast™ main features are as follows:

- View live and playback video from all *cameras*
- View up to 64 video streams side-by-side on a single workstation
- View all cameras on independent *timelines* or on synchronized timelines
- Full PTZ control, using a PC or CCTV keyboard, or on screen using the mouse
- Digital zoom on all cameras
- Motion detection on all cameras
- Visual tracking: follow individuals or moving objects across different cameras
- Search video by *bookmark*, motion, or date and time
- Export video
- Protect video against accidental deletion
- Protect video against tampering by using watermarks

Omnicast™ also provides video support for *events* tracked by other systems unified under Security Center.

- Enhance all event reporting with live and playback video
- Enhance alarm monitoring with live and playback video
- Enhance intrusion detection with live and playback video
- Enhance access control system (Synergis) with live and playback video
  - Video verification: compare *cardholder* picture with live and playback video
  - Consolidate all access events with live and playback video
- Enhance *LPR* system with live and playback video

Entities related to video surveillance

The video surveillance system supports many of the entities that are available in Security Center.

Icon	Entity	Description
	Archiver (role)	Role that controls the video units and manages the video archive.
	Auxiliary Archiver (role)	Role that supplements the video archive produced by the Archiver. It is capable of archiving any camera on the system.
	Media Router (role)	Role that takes care of the routing of all audio and video streams on the network.
	Network	Network (with specific streaming capabilities) that the Media Router takes into account while making routing decisions.
	Server	Server on your network. Used to host the roles needed on your system.
	Area	Logical grouping of cameras and camera sequences.
	Analog monitor	Represents a physical analog monitor connected to a video decoder.
	Camera	A single video source on the system. Might support audio.
	Camera (PTZ enabled)	PTZ camera (also known as dome camera).
	Camera sequence	A pre-arranged order for the display of video sequences in a rotating fashion within a single tile in Security Desk.
	Monitor group	Group of analog monitors sharing common characteristics.
	Schedule	Date and time range. Might support daytime and nighttime.
	Video unit	IP unit incorporating one or more video encoders.
	Partition	Group of entities on the system visible only to a group of users.
	User	Individual who uses Security Center applications.
	User group	Group of users sharing common characteristics.

23

Video deployment

This section includes the following topics:

Preparing to deploy your video surveillance system

To make sure that your video surveillance deployment goes smoothly, you need to perform a series of pre-configuration steps.

Before deploying your video system:

1 Have a network diagram showing all public and private networks used within your organization, their *IP address* range, their video transmission capabilities (*Multicast, Unicast UDP*, and *Unicast TCP*).

For public networks, you also need the name and public IP address of their proxy servers.

TIP: Ask your IT department for this information.

2 Open the ports used by Security Center for communication and video streaming, and make sure they are redirected for firewall and *NAT* purposes.

3 Install the following Security Center software components:

a) Security Center Server software on your main server.

The *main server* is the computer hosting the *Directory* role.

b) (Optional) Security Center Server software on expansion servers.

An *expansion server* is any other server on the system that does not host the Directory role. You can add expansion servers at any time.

c) Security Center Client software on at least one workstation.

For more information about installing Security Center, see the *Security Center Installation and Upgrade Guide*.

4 Have a list of *partitions* (if any).

Partitions are used to organize your system into more manageable subsystems. This is especially important in a multi-tenant environment. If, for example, you are installing one large system in a shopping center or, office tower, you might want to give local administration privileges to the tenants. By using partitions, you can group the tenants so that they can only see and manage the contents of their store or office, but not the others.

5 Have a list of all known users with their names and responsibilities.

To save time, identify users who have the same roles and responsibilities, and organize them into user groups.

NOTE: For large installations, users and user groups can be imported from a Windows *Active Directory*.

6 Install and connect all video equipment (video units, fixed and PTZ cameras) on your company's IP network, with the following information:

- Manufacturer, model, and IP address of each video unit
- Login credentials (username and password) if applicable
- Communication protocol used (HTTP or *HTTPS*)

TIP: A site map (floor plans) showing where the cameras are located would be helpful.

7 If you have cameras connected to a conventional CCTV matrix (*hardware matrix* in Omnicast), you need the following:

- An Omnicast™ 4.x system to manage the video encoders connected to the CCTV matrix outputs.
- An Omnicast™ 4.x system federated in Security Center.

After you finish

Deploy your video surveillance system.

Related Topics

Importing security groups from an Active Directory on page 323
Setting up Omnicast™ federation on page 194

Deploying your video surveillance system

To integrate a variety of video capabilities, you can deploy your video surveillance system once the pre-configuration steps are completed.

Before you begin

Perform the pre-configuration steps.

What you should know

Information about how to set up a typical video installation is described here. Your process might be different, depending on your specific installation requirements.

To deploy your video system:

1 Use the **Admin** account on Config Tool to connect to your system.
2 Create a partition for each independent user group.

By first defining the partitions, you won't have to move entities around after you've created them.

3 To organize the entities in your system (areas, doors, and so on), configure the area view.
4 Set up the Archiver role.
5 Configure your networking environment.
6 If necessary, set up additional Archiver roles.
7 Configure the Auxiliary Archiver roles.
8 Configure the Media Router role.
9 Define custom fields for your system entities.
10 Create user groups and create users.
11 If necessary, federate remote Omnicast™ systems.
12 Create alarms.

About Archivers

Archiver is the role that is responsible for the discovery, status polling, and control of video units. The Archiver also manages the video archive and performs motion detection if it is not done on the unit itself.

All communications between the system and the video units are established through the Archiver role. All events generated by the units (motion, *video analytics*, and so on) are forwarded by the Archiver to the concerned parties on the system. The Archiver also manages the *video archives* and performs *motion detection* on video units that do not support the motion detection feature. Multiple instances of the Archiver role can be created on the system.

Configuring Archiver roles

To have your Security Center system manage your cameras, video archive, and motion detection, you must configure the Archiver role.

What you should know

When Omnicast™ is enabled in your license, an Archiver role is created by default and assigned to the *main server*.

To configure the Archiver role:

1. From the Config Tool home page, open the *Video* task.
2. Select the Archiver role to configure, and then click the **Resources** tab.
3. Configure the archive database.
4. Configure the archive storage settings.
5. (Optional) Change the role's host server.
6. To keep viewing video even if the server hosting the Archiver role goes offline, set up Archiver failover.
7. Add the video units that you want this Archiver role to control.
8. Click the **Extensions** tab and finish configuring the extensions that were created when you added the video units.

   For a list of settings in the **Extensions** tab, see Archiver: Extensions tab on page 859.
9. Click the **Camera default settings** tab and configure the default camera settings for all cameras recorded by this Archiver role.

   For a list of settings in the **Camera default settings** tab, see Configuring default camera settings on page 377.
10. Configure the cameras associated to the video units you just added.
11. If recording is performed on edge units, set up video archive transfer.

After you finish

If you have a large system, you can distribute the load by creating more Archiver roles and hosting them on separate *servers*.

Related Topics

About Archivers on page 370

Moving the Archiver role to another server

In Security Center, if the server that hosts the *Archiver* role breaks, is too slow, or has limited disk space, you can move the role to another server without having to install any additional software.

Before you begin

Make sure you have another server configured and ready to accept a new role.

What you should know

Each Archiver is responsible for the *video archives* of the *cameras* it controls. The video archives include the archive database and the archive storage. Each of these components can be hosted on either the same server or a different server than the one hosting the Archiver. When moving the Archiver to a another server, you must ensure that the new server also has access to these video archives.

To move the Archiver role to another server:

1. From the Config Tool home page, open the *Video* task.
2. Select the Archiver role to configure, and then click the **Resources** tab.
3. If your current server is still running, and both the archive database and archive storage are local to your current server, back up the entire content of its video archives.
   a) In the **Archive transfer** section, temporarily set the backup folder to a location that is accessible by the new server. Make sure that the location you choose has enough disk space to store the video archives of your Archiver.
   b) Using the following options, perform a manual backup:
      - For the type of backup, select **Backup**.
      - For the source, select the current Archiver role.
      - For the time range, select a range wide enough to include all of the video archives.
      - For the data, select **Everything since last transfer**.

   c) Return to the **Video** task.
4. In the **Server** drop-down list, select the new server that replaces the current one.
5. Based on the characteristics of the new server, make the necessary adjustments to the following:
   - The archive database
   - The archive storage settings

   IMPORTANT: If the new server is the same physical server as the old one (for example, same server but different GUID in Security Center), you do not need to modify the archive database and archive storage settings.

6. Click **Apply**.
7. To restore the video archives belonging to this Archiver role, consider the following:
   - If you performed a full backup in Step 3, restore this backup with the following options:
     - For the restore type, select **Archiver**.
     - For the Archiver, select your current Archiver.
     - For the time range, select the same start and end time used for the backup.
     - For the cameras you want to restore, select all.
     - Turn the option **Protect video from deletion** OFF.
   - If your previous server was broken and all you have are the backups taken prior to the server failure, restore all the video archives up to the archive retention period of the Archiver.

   - If both the archive database and the archive storage remained at the same location (on a third server), you do not need to restore the video archives.

8. If you temporarily changed the Backup folder to a new location (see step 3), set the folder back to its original location.
9. Click **Apply**.

About video units

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

Video units are created manually, or automatically by the Archiver if the unit supports *automatic discovery*.

Adding video units manually

To monitor video in Security Center, you must add video units to an Archiver.

Before you begin

You must know the manufacturer, the product type (model or series), the IP address, and the login credentials (username and password) for the units you plan to add.

TIP: If you do not know your unit’s IP address, you can use the *Unit enrollment tool* to discover it.

What you should know

If you are enrolling a Sharp camera running SharpOS 11.3 or earlier under the Archiver (to access the camera’s video streams, or if LPR Processing Unit input/output control is required), you must configure the AutoVu™ extension to allow basic authentication. In Config Tool, from the Archiver's *Extensions* tab, select the Genetec™ AutoVu™ extension, and turn off **Refuse Basic Authentication**.

To add a video unit:

1. From the Config Tool home page, open the *Video* task.
2. Click **Add an entity** (+) > **video unit**.

   The **Manual add** dialog box opens.
3. If you have multiple Archiver roles, select the Archiver role to manage the unit from the **Archiver** drop-down list.
4. Select the unit’s manufacturer and product type.
5. Enter the IP address and HTTP port of the unit.

   Use a range of IP addresses to add multiple units in a single operation.
6. Select which credentials the Archiver should use to connect to the unit.
   - **Default login :** Use the default login credentials defined in the manufacturer’s extension for this Archiver. If the extension has not yet been defined, blank credentials are used.
   - **Specific:** Enter the specific login credentials used by this unit. This can be changed to **Use default login** later during video unit configuration.
7. If the video unit is configured to use HTTPS, turn on **HTTPS** and enter the HTTPS port of the unit.
8. Complete all other settings as necessary, and click **Add**.

   If the manufacturer’s extension does not exist, it is created for you.

   If the added camera is an encoder with multiple streams available, each stream is added with the *Camera - n* string appended to the camera name, *n* representing the stream number. For an IP camera with only one stream available, the camera name is not modified.

   NOTE: If the manufacturer supports *automatic discovery*, all other units present on your system that share the same *discovery port* are automatically added to the same Archiver in addition to those being added manually.
9. To refresh the **Role view**, press **F5**.

The new video units are added under the selected Archiver entity.

After you finish

If necessary, change the default settings of the video units from their configuration tabs.

If you are experiencing issues adding a video unit, then you can troubleshoot the problem.

Related Topics

Video unit - Identity tab on page 847
Video unit - Properties tab on page 848
Video unit - Peripherals tab on page 849

Configuring default camera settings

You can use the **Camera default settings** tab to configure the default video quality and recording settings for all cameras controlled by an Archiver.

What you should know

- Any recording settings that are configured in the Security Center installer assistant are carried over to the **Camera default settings** tab.
- Recording settings affect your disk space.
- Recording settings defined on the **Recording** tab of an individual camera overwrite the settings defined on the **Camera default settings** tab.

To configure default camera recording settings:

1. From the Config Tool home page, open the *Video* task.
2. Select the Archiver to configure, and click the **Camera default settings** tab.
3. Under **Video quality** select a **Resolution**. You can choose from the following:
   - **High:** 1270x720 and greater.
   - **Standard:** Between 320x240 and 1280x720.
   - **Low:** 320x240 and less.
   - **Default:** Manufacturer default settings.
   - **Frame rate:** You can select a value between 1 and 30 fps. Does not apply to default settings.
4. From the **Recording modes** drop down list, select one of the following recording modes:
   - **Continuous:** Records continuously. Recording cannot be stopped by the user (🔴🔒).
   - **On motion/Manual:** Records when triggered by an action (such as *Start recording*, *Add bookmark*, or *Trigger alarm*) through motion detection, or manually by a user. In this mode, the *Record* button in Security Desk appears grey (●) when the Archiver is not recording, red (🔴) when it is recording but can be stopped by the user, or red with a lock (🔴🔒) when it is recording but cannot be stopped by the user (on motion or alarm recording).
   - **Manual:** Records when triggered manually by a user. In this mode, the *Record* button in Security Desk appears grey (●) when the Archiver is not recording, red (🔴) when it is recording but can be stopped by the user, or red with a lock (🔴🔒) when it is recording but cannot be stopped by the user (on motion or alarm recording).
   - **Custom:** Recording is specified by a custom schedule. You can use the custom schedule that you created with the installer assistant, or click ➕ to add a new custom recording schedule that you created using the *System* task. For more information about creating schedules using the *System* task, see Creating schedules on page 169.

     CAUTION: Recording schedules of the same type (for example, two daily schedules) cannot overlap, regardless of the recording mode configured for each. When a scheduling conflict occurs, the Archiver and the video units are displayed in yellow in the entity browser and they issue entity warning messages.
   - **Off:** Recording is off (●🔒), even when an alarm is triggered.
5. Configure the advanced recording settings. You can configure the following:
   - **Record audio:** Switch **ON** to record audio with your video. A microphone entity must be attached to your cameras. For more information, see Configuring camera settings on page 398.
   - **Record metadata:** Switch **ON** to record metadata with your video.

- **Redundant Archiving:** Switch **ON** to allow primary, secondary, and tertiary servers to archive video at the same time. This setting is effective only if failover is configured. For more information, see Setting up Archiver role failover on page 162.
- **Automatic cleanup:** Specify a retention period for recorded video (in days). Video archives older than this period are deleted.
- **Time to record before an event:** Use the slider to set the number of seconds that are recorded before an event. This buffer is saved whenever the recording starts, ensuring that whatever prompted the recording is also captured on video.
- **Time to record after a motion:** Use the slider to set the number of seconds that continue to be recorded after a motion event. During this time, the user cannot stop the recording.
- **Default manual recording length:** Use the slider to select the number of minutes the recording lasts when it is started manually by a user, or when the *Start recording* action is triggered.
- **Encryption:** Switch **ON** to enable *fusion stream encryption* for all cameras managed by the selected Archiver. Only users who have one or more of the listed **Certificates** installed on their workstations can view video.

  NOTE: In order to enable **Encryption**, you must add at least one *encryption certificate* to the Archiver role. For more information, see What is fusion stream encryption? on page 346.

6 Click **Apply**.

The recording settings are applied to all cameras controlled by the selected Archiver role.

Configuring the recording settings of cameras

To set the recording mode (continuous, on motion, and so on) or enable encryption for your cameras, you can do so through the **Recording** tab of each individual camera.

Before you begin

If you are using multiple disk groups for archive storage, temporarily set the *recording mode* to OFF, and then re-enable it at the end of the process. Doing this prevents you from creating the video files on the wrong disk group.

What you should know

- The recording settings of cameras affect your disk space.
- Recording settings defined on the **Recording** tab of an individual camera supersede the settings defined in the **Camera default settings** tab of the Archiver.

To configure the recording settings of cameras:

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

2 Select the camera to configure, and then click the **Recording** tab.

3 In the **Recording settings** option, select one of the following:

- **Inherit from Archiver:** The camera inherits the recording settings configured for the Archiver role in the **Camera default settings** tab.
- **Custom settings:** The camera uses its own settings.

4 From the **Recording modes** drop down list, select one of the following recording modes:

- **Continuous:** Records continuously. Recording cannot be stopped by the user (🔴🔒).
- **On motion/Manual:** Records when triggered by an action (such as *Start recording*, *Add bookmark*, or *Trigger alarm*) through motion detection, or manually by a user. In this mode, the *Record* button in Security Desk appears grey (⚫) when the Archiver is not recording, red (🔴) when it is recording but can be stopped by the user, or red with a lock (🔴🔒) when it is recording but cannot be stopped by the user (on motion or alarm recording).
- **Manual:** Records when triggered manually by a user. In this mode, the *Record* button in Security Desk appears grey (⚫) when the Archiver is not recording, red (🔴) when it is recording but can be stopped by the user, or red with a lock (🔴🔒) when it is recording but cannot be stopped by the user (on motion or alarm recording).
- **Custom:** Recording is specified by a custom schedule. You can use the custom schedule that you created with the installer assistant, or click ➕ to add a new custom recording schedule that you created using the *System* task. For more information about creating schedules using the *System* task, see Creating schedules on page 169.

  CAUTION: Recording schedules of the same type (for example, two daily schedules) cannot overlap, regardless of the recording mode configured for each. When a scheduling conflict occurs, the Archiver and the video units are displayed in yellow in the entity browser and they issue entity warning messages.
- **Off:** Recording is off (⚫🔒), even when an alarm is triggered.

5 Configure the advanced recording settings. You can configure the following:

- **Record audio:** Switch **ON** to record audio with your video. A microphone entity must be attached to your cameras. For more information, see Configuring camera settings on page 398.
- **Record metadata:** Switch **ON** to record metadata with your video.

- **Redundant Archiving:** Switch **ON** to allow primary, secondary, and tertiary servers to archive video at the same time. This setting is effective only if failover is configured. For more information, see Setting up Archiver role failover on page 162.
- **Automatic cleanup:** Specify a retention period for recorded video (in days). Video archives older than this period are deleted.
- **Time to record before an event:** Use the slider to set the number of seconds that are recorded before an event. This buffer is saved whenever the recording starts, ensuring that whatever prompted the recording is also captured on video.
- **Time to record after a motion:** Use the slider to set the number of seconds that continue to be recorded after a motion event. During this time, the user cannot stop the recording.
- **Default manual recording length:** Use the slider to select the number of minutes the recording lasts when it is started manually by a user, or when the *Start recording* action is triggered.
- **Encryption:** Switch this option **ON** to enable *fusion stream encryption* for this camera. Only users who have one or more of the listed **Certificates** installed on their workstations are able to view video.

  NOTE: To enable **Encryption**, at least one *encryption certificate* must be added to this camera. For more information, see What is fusion stream encryption? on page 346.

6 Click **Apply**.

The recording settings are applied to the selected camera.

Viewing recording states of cameras

You can view the *recording state* and statistics of each individual camera controlled by an Archiver or Auxiliary Archiver to verify whether each encoder is currently streaming video (and audio), and whether the role is currently recording the data.

To view the recording state of a camera:

1. From the Config Tool home page, open the *Video* task.
2. Click the **Resources** tab, and then click **Statistics** (◔).

   The Active cameras and Archiving cameras fields show you how many cameras are active, and how many have archiving enabled.
3. Click **See details**.

   In the **Archiving camera details** dialog box, the recording states of the cameras are listed. The possible recording states are as follows:

   - **Recording off:** Recording is enabled but the Archiver is currently not recording. If you suspect a problem, click the **Description** column. The possible causes are the following:
     - Database lost.
     - Disks full.
     - Cannot write to any drive.
   - **Recording on:** Recording was started by a user.
   - **Recording on (locked by system):** Recording is currently controlled by the Archiver (following an On Motion or Continuous schedule).
   - **Recording off (locked by system):** Recording is currently disabled on this camera by a schedule.
   - **Recording about to stop:** Recording was started by a user and is about to stop (within the last 30 seconds of recording).

Investigating Archiver events

You can search for events related to *Archiver roles*, using the *Archiver events* report.

What you should know

You can check the status of an Archiver by selecting it, setting the time range to one week, and making sure there are no critical events in the report. You can also troubleshoot an Archiver by searching for important events, such as *Disk load threshold exceeded* or *Cannot write to any drive*, and see when those events occurred.

To investigate Archiver events:

1. From the home page, open the **Archiver events** task.
2. Set up the query filters for the report. Choose from one or more of the following filters:
   - **Archiver:** Select the Archivers you want to investigate.
   - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
   - **Events:** Select the events of interest. The event types available depend on the task you are using.
   - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the last week or the last month.
   - **Description:** Restrict the search to entries that contain this text string.
3. Click **Generate report**.

   The Archiver events are listed in the report pane.

Report pane columns for the Archiver events task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Description:** Description of the event, activity, entity, or incident.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **Source (entity):** The name of the system the camera belongs to.

About Auxiliary Archivers

Auxiliary Archiver is the role that supplements the video archive produced by the Archiver. Unlike the Archiver, the Auxiliary Archiver is not bound to any particular *discovery port*, therefore, it can archive any camera in the system, including cameras federated from other Security Center systems. The Auxiliary Archiver depends on the Archiver to communicate with the video units. It cannot operate on its own.

The Auxiliary Archiver allows you to create a different set of video archives than the one produced by the Archiver roles, with different video quality settings and recording schedules.

Multiple instances of this role can be created on the system.

Auxiliary Archiver scenarios

The following are some sample scenarios where you would need Auxiliary Archivers:

- You need to create a high resolution off-site (outside your corporate LAN) copy of your video archive for selected cameras. In this scenario, you would run the Auxiliary Archiver from a secured location, probably on a server located in a separate building with large storage capabilities. The Auxiliary Archiver would record high quality video streams from specific cameras using different recording settings (mode, schedules, etc.) than the Archiver.
- You need to create a lower quality copy of your video archive to keep for a longer period of time. In this scenario, you would record the low quality video stream with the Auxiliary Archiver and set a longer retention period.
- You need to record more cameras (offering different viewing angles) during off-hours when there are no guards on duty. In this scenario, you would configure an Auxiliary Archiver to continuously archive cameras during off-hours that are also archived by the regular Archiver.

Limitations of Auxiliary Archivers

Auxiliary Archivers can record federated Security Center native cameras, but they cannot record cameras that are federated from an Omnicast™ 4.x system (through Omnicast™ Federation™, or through a remote Security Center system that federates an Omnicast™ 4.x system).

Differences between Archivers and Auxiliary Archivers

It is important to know the difference between the Archiver and the Auxiliary Archiver.

The following table highlights the differences between the Archiver and the Auxiliary Archiver.

Characteristics	Archiver role	Auxiliary Archiver role
Automatic unit discovery	Yes (on units that support it).	No.
Command and control of cameras/video units	Yes.	No (relies on the Archiver role).
Command encryption via secure protocols (such as HTTPS and *SSL*)	Yes (on units that support it).	Not applicable.
Recorded cameras	A camera can only be associated to one Archiver role.	A camera can be associated to multiple Auxiliary Archivers.

Characteristics	Archiver role	Auxiliary Archiver role
	Can only record cameras with which it has a direct connection (usually on the same LAN).	Can record any camera on the system, including federated cameras (but only from Security Center systems).
Recording settings	Each camera has the option to follow the default role settings or its own custom settings.	Each camera has the option to follow the default role settings or its own custom settings.
Recorded video stream	Can only record the stream designated for *Recording*.	Can record any video stream of your choice.
Manual recording	Yes, when Manual recording schedules are in effect.	No (although Manual recording schedules can be configured).
Event logging in database	Yes. The events can be searched and viewed with the *Archiver events* video maintenance task.	Yes. The events can be searched and viewed with the *Archiver events* video maintenance task.
Event logging to a flat file	Yes. Found in *ArchiverLogs* folder.	No.
Database backup and restore	Yes (*video files* are not included).	Yes (video files are not included).
Failover support	Yes. One *secondary server* can be added to the Archiver role.	Not applicable.
Multiple copies of the video archive	Yes, through *redundant archiving*, but the master and redundant copies are identical because they use the same recording settings.	Yes. Each Auxiliary Archiver produces a different set of video archives that follow unique recording settings.
Video file protection	Yes.	Yes.
Video watermarking	Yes.	Yes.

Creating Auxiliary Archivers

To create a set of video archives apart from those managed by the Archiver role, you must create an Auxiliary Archiver.

What you should know

The Auxiliary Archiver role is not created by default; it must be created manually.

NOTE: After you create the Auxiliary Archiver, you should not move the role to a different server unless both the database and the video storage are configured on a separate machine.

To create an Auxiliary Archiver role:

1 Open the **System** task, and click the **Roles** view.

2 Click **Add an entity** (+) > **Auxiliary Archiver**.

3 In the **Specific info** page, do the following:

a) (If you have multiple servers in your system) From the **Server** drop-down list, select the *server* where this role will be hosted

b) Enter the **Data server** name for the video archive database.

A default data server, called **(local)\SQLEXPRESS**, is installed on every computer where the Genetec™ Server service is installed. You can use it or use another data server on your network.

c) Enter the **Database** name of the video archive database.

CAUTION: The default name is *AuxiliaryArchiver*. If the selected server is already hosting another instance of Auxiliary Archiver, you must choose a different name. Otherwise, the new role will corrupt the existing database.

TIP: You should use a different database name for every instance of Auxiliary Archiver regardless of whether there is a conflict or not, to avoid confusion.

d) Click **Next**.

4 In the **Basic information** page, enter a name and description for the role.

5 Select a **Partition** this role is a member of, and click **Next**.

Partitions determine which Security Center users have access to this entity. Only users that are part of the partition can view or modify the Auxiliary Archiver.

6 Click **Next** > **Create** > **Close**.

A new Auxiliary Archiver role (🎥) is created. Wait a few seconds for the role to create the database on the selected data server.

7 Select the **Resources** tab, and configure the server and database for this Auxiliary Archiver.

NOTE: Every newly created Auxiliary Archiver is assigned the default value of 558 for its RTSP port. This port value must be unique for all archiving roles hosted on the same machine.

8 Configure the archive storage settings.

9 Click the **Camera recording** tab, and configure the default recording settings for all cameras recorded by this Auxiliary Archiver. See Configuring camera recording settings for an Auxiliary Archiver on page 387.

10 Click the **Cameras** tab, and select the cameras you want to archive.

Related Topics

Auxiliary Archiver - Resources tab on page 867

Adding cameras to Auxiliary Archivers

For the Auxiliary Archiver to create video archives, you must add cameras to be controlled by the role.

What you should know

- You cannot add federated cameras from Omnicast™ 4.x systems to the Auxiliary Archiver.
- If you are using Windows Server 2008 or earlier, you can greatly improve your system performance by assigning a different multicast port to each camera.

To add a camera to the Auxiliary Archiver:

1. From the Config Tool home page, open the *Video* task.
2. Select the Auxiliary Archiver, click the **Cameras** tab, and click **Add an item** (✚).
3. In the dialog box that appears, select the cameras you want and click **OK**.

   NOTE: It takes a few seconds for the selected cameras to be added. If the role is unable to add a camera in the given time, a failed status is indicated, and the camera is removed.

4. Click **Apply**.
5. To override the default recording settings on a camera:

   a) Select the camera from the list and click **Jump to** (→).

   The camera configuration page is selected.

   b) From the **Recording** tab of the camera, select the tab that corresponds to the current Auxiliary Archiver.
   c) Under **Recording settings**, click **Custom settings**, and make the necessary changes.
   d) Click **Apply**.

Removing cameras from Auxiliary Archivers

You can remove a camera from the Auxiliary Archiver, so it is no longer recorded by the Auxiliary Archiver.

What you should know

CAUTION: Removing a camera from the Auxiliary Archiver instantly deletes the associated *video archive* from the Auxiliary Archiver's database.

To remove a camera from an Auxiliary Archiver:

1. From the Config Tool home page, open the *Video* task.
2. Select the Auxiliary Archiver, click the **Cameras** tab and click **Delete the item** (✖).
3. In the confirmation dialog box that appears, click **Delete**.

   All records of this camera's video archive are deleted from the role's database.

4. In the second confirmation dialog box, do one of the following:
   - Click **No** if you want to keep the *video files* on disk.

     This allows you to play the video files with the *Video file player* in Security Desk, but you will no longer be able to query the video archive with the *Archives* task.

   - Click **Yes** if you do not want to keep the video files.

Configuring camera recording settings for an Auxiliary Archiver

You can use the **Camera recording** tab to configure the recording settings for all cameras controlled by an Auxiliary Archiver.

Before you begin

- If you are using multiple disk groups for archive storage, temporarily set the *recording mode* to OFF, and then re-enable it at the end of the process to avoid creating the video files on the wrong disk group.

What you should know

- The recording settings of cameras affect your disk space.
- Recording settings defined on the **Recording** tab of an individual camera supersede the settings defined on the **Camera default settings**tab of the Auxiliary Archiver.

To configure recording settings for cameras managed by an Auxiliary Archiver:

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

2 Select the Auxiliary Archiver to configure, and click the **Camera recording** tab.

3 From the **Video stream** drop-down list, select the default video stream that the Auxiliary Archiver should record for each camera. The video streams are configured for each individual camera.

4 From the **Recording modes**, select one of the following:

- **Continuous:** Records continuously. Recording cannot be stopped by the user (●).
- **Custom:** Recording is specified by a custom schedule. You can use the custom schedule that was created with the installer assistant, or click ➕ to add a custom recording schedule that was created using the *System* task. For more information about creating schedules using the *System* task, see Creating schedules on page 169.

  CAUTION: Recording schedules of the same type (for example, two daily schedules) cannot overlap, regardless of the recording mode configured for each. When a scheduling conflict exists, the Archiver and the video units are displayed in yellow in the entity browser and issue entity warning messages.
- **Off:** Recording is off (●), even when an alarm is triggered.

5 (Optional) Click **Show advanced settings** to configure advanced recording settings. You can configure the following:

- **Record audio:** Switch **ON** to record audio with your video. A microphone entity must be attached to your cameras for this option to work. For more information, see Configuring camera settings on page 398.
- **Record metadata:** Switch **ON** to record metadata with your video.
- **Automatic cleanup:** Specify a retention period for recorded video (in days). Video archives older than this period are deleted.

6 Click **Apply**.

The recording settings are applied to the cameras managed by the Auxiliary Archiver.

About the Media Router

Media Router is the central role that handles all stream (audio and video) requests in Security Center. It establishes streaming sessions between the stream source (camera or Archiver) and its requesters (client applications). Routing decisions are based on the location (IP address) and the transmission capabilities of all parties involved (source, destinations, networks, and servers).

It ensures all video streams use the best route to get to their destinations, while performing any necessary transformation (for example, from unicast to multicast, or from IPv4 to IPv6).

The Media Router role has a default RTSP port of 554, its redirectors have a default RTSP port of 560, and an Archiver role has a default RTSP port of 555. These ports must be unique on the same server.

If multiple Archiver roles are created on the same server, they must all have a different RTSP port. Otherwise, the role entity will turn yellow and an *Entity warning* event will be generated.

Only a single instance of this role is permitted per system.

Configuring the Media Router role

You can configure the Media Router role settings to optimize the throughput and increase the security of your private network.

What you should know

When Omnicast™ is enabled by your license, the Media Router role is created by default and hosted on the *main server*. The default setup is usually sufficient, unless you have a complex system involving multiple private networks.

To configure the Media Router role:

1. From the Config Tool home page, open the *Video* task.
2. Select the **Media Router** role, and click the **Resources** tab.
3. (Optional) Change the role's primary server.
4. To configure failover for the Media Router, add a standby server.
5. Click the **Properties** tab.
6. If the default start multicast address and port settings conflict with other applications on your system, select a different IP address or port in the **Start multicast address** fields.

   In multicast, all audio and video sources are streamed to different multicast addresses while using the same port number, because multicast switches and routers use the destination IP address to make their routing decisions. Similarly, the Media Router assigns that same port number to all streaming devices (microphones and cameras), starting with the specified IP address, and adding 1 for every new device it encounters.

7. To secure and authenticate RTSP video requests in Security Center, turn on the **Use secure communication** option.

   When secure communication is enabled, all video communications use RTSP over TLS. If your network is configured for Multicast or Unicast UDP, only the RTSP control channel is encrypted (no impact on performance). If your network is configured for Unicast TCP, all video-related traffic (RTSP and video data) goes through the TLS channel. This impacts the performance of live video redirection. Video playback and video export always use RTSP over TCP, therefore the video data is always encrypted. Secure communication is enabled by default on new installations, but disabled if you upgraded from a version prior to 5.5.

   IMPORTANT: When secure communication is turned on, older Security Center systems cannot federate your Security Center system.

8. Add or change the redirector configurations.
9. Click **Apply**.

Related Topics

Adding networks on page 132

Adding redirectors to the Media Router

If you need to reach clients located on remote networks or balance the redirection workload between multiple servers, you can create redirector agents on additional servers.

What you should know

Redirectors are *servers* assigned to host *redirector agents*. A redirector agent is a software module launched by the Media Router to redirect data streams from one IP endpoint to another. The Media Router automatically creates a redirector agent on every server assigned to an Archiver role.

To avoid overloading a redirector server or the network bandwidth between the two endpoints, you can limit the number of live and playback streams that the server can redirect.

To add a redirector to the Media Router role:

1 Open the *System* task, and click the **Roles** view.

2 Select the Media Router, and click the **Properties** tab.

3 Click **Add an item** (➕).

4 In the *Redirector configuration* dialog box, set the redirector settings as follows:

- **Server:** Server selected to host the redirector agent.
- **Incoming UDP port range:** Range of ports used by the redirector agent to send video using *UDP*. If the redirector agent is running behind a firewall, make sure that these ports are unlocked for inbound packets for UDP connections.
- **Live capacity:** Use this option to limit the maximum number of live streams that this server (redirector) can redirect. This feature serves two purposes:
  - Avoid overloading the server with too many users trying to view video (that needs redirection) at the same time.
  - Avoid overloading the network with too many video streams coming from a remote site that has limited bandwidth.

  When the limit is reached, an error message is displayed on the client application requesting the live video that the live stream capacity is exceeded.
- **Playback capacity:** Same idea as *Live capacity* for playback streams.
- **Redirection strategy:** Use this option if you have multiple network cards and want to specify the actions each network card will perform. For example, you may want to specify that export and video transfer only be performed by your Wireless network card. For more information, see Configuring network card usage for a redirector on page 391.

  NOTE: By default, all actions are performed on all available network cards.
- **Multicast interface:** Network adaptor to use for streaming data in multicast mode.
- **RTSP port:** Port used by the redirector agent to receive TCP commands. The same port is used to stream data using TCP.

  NOTE: If you are configuring the redirector agent on the same server that is hosting the Media Router, the RTSP port cannot be the same as the one used by the Media Router.

5 Click **Save** > **Apply**.

Configuring network card usage for a redirector

You can configure a redirector to use different network cards for specific actions. For example, you may want to specify that export and video transfer only be performed by your Wireless network card. You can also list the network cards in order of priority.

To configure the network card use for a redirector:

1 Open the *System* task, and click the **Roles** view.

2 Select the Media Router, and click the **Properties** tab.

3 From the **Redirectors** list, select the redirector you want to configure and click **Edit the item** (✎).

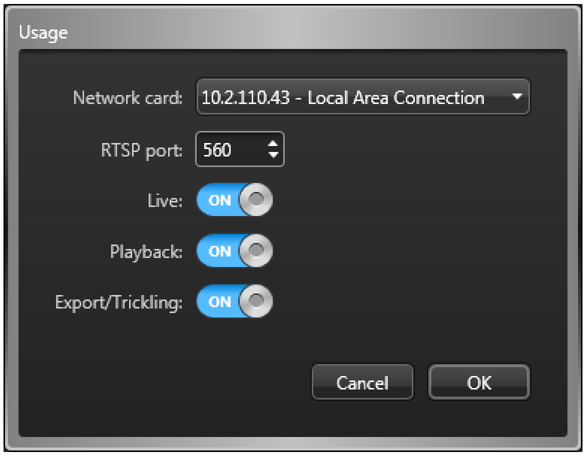
The *Redirector configuration* window opens.

4 Beside *Redirection strategy*, click **Advanced** (⚙).

5 Click **Add** (➕).

6 In the *Usage* dialog box, select the network card you want to configure.

7 Enter an **RTSP port**.



Network card: 10.2.110.43 - Local Area Connection

RTSP port: 560

Live: ON

Playback: ON

Export/Trickling: ON

8 Enable the actions you would like to assign to the selected network card. You can choose from the following:

- **Live**
- **Playback**
- **Export/Trickling**

IMPORTANT: You cannot add the same network card and port combination twice, the network card and port number combination must be unique.

9 Click **OK**.

10 (Optional) Change the network card priority.

a) In the *Redirector configuration* window, select a card from **Network card** list.

b) Click the ⌄ or ⌃ buttons to move it to the top or bottom of the list.

11 Click **Save** > **Apply**.

- To edit the settings for a network card, select it from the **Network card** list and click **Edit the item** (✎).
- To delete a network card, select it from the **Network card** list and click **Delete** (✖).

Video options

Once you are familiar with how to work with video in Security Center, you can customize how video is handled by the system from the *Video* tab in the *Options* dialog box.

Advanced video settings

The advanced video settings apply to the local workstation and affect Security Desk and Config Tool for all users.

NOTE: After changing the Advanced setting options, you must restart Security Desk.

- **Enable deinterlacing:** Select this option to help reduce the jagged effect around straight lines during movement in interlaced video streams.
- **Hardware acceleration:** Turn this option on to allow Security Desk to offload video decoding from the main CPU to the video cards. To see what video cards are installed on your computer, click **Show hardware information**. There are also tips about how to achieve the best video decoding performance.

About the Media Gateway

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

There are many uses for raw (not decoded) video streams. For example, an external system can use the raw video streams to perform video analytics and trigger events. Another application can display video in a web page using an off-the-shelf viewer that supports the camera's specific encoding.

The Media Gateway includes the following features:

- It supports the standard RFC 2326.
- It requires a valid license that provides one or more RTSP streams, as indicated by the *Number of RTSP streams* license option.
- A single instance of this role is permitted per system.
- The role can be assigned to multiple servers for load balancing.
- Live and playback video can be requested, but non-video streams such as audio, PTZ commands, overlays, and metadata are not supported.
- The default RTSP port is 654.

Creating the Media Gateway role

If you want to request live and playback video and receive raw video streams using the RTSP protocol, you must first add the Media Gateway in Config Tool.

Before you begin

Make sure of the following:

- The Media Gateway role does not already exist in your system.
- The *Number of RTSP streams* option in your Security Center license supports at least one stream.
- The *Media Router* role is active in your system.

To add the Media Gateway role:

1. From the Config Tool home page, open the *Video* task.
2. Click the arrow next to **Video unit**, and then click **Media Gateway**.
3. In the *Basic information* page, enter an **Entity name**, and (optional) an **Entity description**.
4. Select an existing **Partition**, or create a new one.
   The Media Gateway role is created under the selected partition.
5. Click **Next** > **Create** to add the Media Gateway role in your system.
6. Click **Close** after the role has been added.

After you finish

Configure the Media Gateway role.

Configuring the Media Gateway role to receive video requests

If you want to request live and playback video and receive raw video streams using the RTSP protocol, you must configure the Media Gateway in Config Tool.

Before you begin

Create the Media Gateway role in your system.

To configure the Media Gateway role:

1. From the Config Tool home page, open the *Video* task.
2. In the entity tree, select the Media Gateway role, and click the **Resources** tab.
3. (Optional) Change the role's primary server.
4. To configure load balancing for the Media Gateway, add servers to the role.
   a) Under the **Servers** list, click **Add an item** (➕).

      A dialog box that lists all remaining servers on your system not assigned to the role, appears.

   b) Select the server you want to add, and then click **Add**.

   The RTSP requests are now load balanced between the listed servers.
5. Click the **Properties** tab.
6. Make sure that the default **Start multicast address** and port settings do not conflict with other roles, such as Archivers, redirectors, and so on, and applications on your system.

   In multicast, all video sources are streamed to different multicast addresses while using the same port number, because multicast switches and routers use the destination IP address to make their routing decisions. Similarly, the Media Gateway assigns that same port number to all streaming cameras, starting with the specified IP address, and incrementing the IP address by 1 for every new camera it encounters.
7. If the default **RTSP port** conflicts with other roles or applications on your server, select a different port number.

   NOTE: The default RTSP port is 654.
8. (Optional) Disable the **User authentication** option if needed.

   NOTE: It is recommend that you keep this option enabled (default) for security purposes; however, you can disable it if you know that your network is secure.
9. If **User authentication** is enabled, configure the users that can be used to authenticate video requests made by RTSP client applications.

   NOTE: The cameras that an RTSP client application can view in the system depend on the user account the client uses to log on to Security Center. Assign a password to each user account added to the list, preferably a different password than the one used in Security Center.
10. Click **Apply**.

The Media Gateway role is now ready to receive RTSP video stream requests.

After you finish

See the *Security Center SDK Documentation* for details about sending RTSP video requests.

24

Cameras

This section includes the following topics:

About cameras (video encoders)

A camera is a type of entity that represents a single video source in the system. The video source can either be an IP camera, or an analog camera that is connected to the video encoder of a video unit. Multiple video streams can be generated from the same video source.

A video encoder is the device that converts an analog video source to a digital format using a standard compression algorithm (H.264, MPEG- 4, or M-JPEG). The video encoder is one of the many devices found on a video unit.

Each video encoder can generate one or multiple video streams using different compression schemes and formats for different usages. In the case of an IP camera, the camera and the video encoder form an inseparable unit. Because of the relationship between the camera and the video encoder, the two terms are often used interchangeably.

Cameras (or video encoders) are automatically created when you add the video units they are part of to Security Center.

Configuring camera settings

For optimal performance, configure your camera settings after the video units have been added in Security Center.

What you should know

Security Center provides default settings; however, it is recommended that you carefully go through the configuration of each entity in order to get the best results.

NOTE: For federated cameras, only the settings in the *Identity* and *Visual tracking* tabs are configurable.

To configure a camera:

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

2 Select the camera to configure.

3 Configure the video streams that the encoder should generate.

4 Configure specific recording settings for this camera.

   If you do not configure specific settings for the camera, it follows the recording settings for the archiving roles (Archiver and Auxiliary Archivers) that control it.

   NOTE: If a camera has been configured for archive transfer, recording can only be configured using its web page.

5 Configure the motion detection settings for the camera.

6 Adjust the camera's video attributes (brightness, contrast, hue, saturation) to account for different times of the day.

7 Configure Visual tracking so users can switch to adjacent cameras by clicking a camera in a Security Desk tile.

8 Click the **Hardware** tab, and associate hardware devices to the camera if they are not built-in on the same video unit.

   - **PTZ motors:** Configure the PTZ motor.
   - **Microphones:** Select a microphone from the **Microphone** drop-down list.
   - **Speakers:** Select a speaker from the **Speaker** drop-down list.

9 Click **Apply**.

10 Test the video settings you have configured so far: video quality, color and brightness, PTZ controls, and so on.

After you finish

You can copy the settings you just configured for this camera to other cameras of the same model.

About video streams

Most *video encoders* and IP cameras supported by Security Center can generate multiple video streams from the same video source.

When a camera has multiple video streams, it allows you to define different video quality settings for the live monitoring stream and the recording stream. Additional streams can also be configured for other needs, such as remote access (low bandwidth) or low resolution versus high resolution streams.

Each video stream is defined by the following settings:

- **Video quality:** The quality of the video stream, made up of parameters such as image resolution, *bit rate*, frame rate, and so on, that varies depending on the manufacturer. The video quality can have multiple configurations based on different *schedules*. For example, lower resolution might be required for regular hours when there is a lot of activity in the office, while higher resolution might be used during off-hours when less activity occurs. Video quality directly affects your bandwidth and archiving disk space.
- **Stream usage:** The purpose of the video stream, and when it is used (for live video, recordings, and so on).
- **Network settings:** Specific connection type and *multicast* address that is configured for the stream, based on its usage and your network configuration.

Automatic stream selection

Displaying high resolution video requires a lot of CPU power. In order to display the maximum number of live video streams simultaneously in Security Desk, CPU use should be optimized.

You can configure Security Desk to use *Automatic* video stream mode. When this mode is selected, Security Desk displays the *Low resolution* or *High resolution* stream, depending on the size of the selected canvas tile. The video stream that has an image resolution equal to, or lower than, the display area of the tile is selected.

The video stream also changes dynamically when the user resizes the Security Desk window, or changes the *tile pattern*.

NOTE: When *Automatic* mode is selected as the default viewing stream in Security Desk, the *High resolution* stream is always used when a tile is maximized, or when the digital zoom is in use.

For more information about changing the default live stream in Security Desk, see the *Security Desk User Guide*.

Configuring video streams of cameras

Before you start monitoring video in Security Desk, you should decide how you want to use each video stream, and configure the appropriate settings for it.

What you should know

Every video stream setting affects your bandwidth and archive storage. You must find a balance between quality, CPU usage, and disk space.

Security Desk only switches to a higher resolution when it makes a visual difference to the users. Therefore, make sure the *Live* stream has a better resolution than the *Low resolution* stream, and that the *High resolution* stream has a better resolution than the *Live* stream.

To configure a camera's video streams:

1. From the Config Tool home page, open the *Video* task.
2. Select the camera to configure, and then click the **Video** tab.
3. If the camera supports multiple video streams, select a video stream tab at the bottom of the **Video** tab.
4. In the **Video quality** section, set the video quality settings (resolution, frame rate, and so on) for the selected video stream.
5. In the **Stream usage** section, specify the purpose for the selected video stream.

   NOTE: A stream can be assigned all, some, or none of the usage options. A stream that has no usage assigned is not generated by the video encoder, which conserves CPU on the unit.

   - **Live:** Default stream used for viewing live video in Security Desk.
   - **Recording:** Stream recorded by the Archiver for future investigation.

     TIP: The quality of the recording stream can be temporarily boosted when the recording is triggered by certain types of events.
   - **Remote:** Stream used for viewing live video when the bandwidth is limited.
   - **Low resolution:** Stream used instead of the *Live* stream when the tile used to view the stream in Security Desk is small.
   - **High resolution:** Stream used instead of the *Live* stream when the tile used to view the stream in Security Desk is large.
6. From the **Connection type** drop-down list in the **Network** section, select how communication between the Archiver and the camera is established for sending or receiving video streams:
   - **Best available:** Lets the Archiver select the best available connection type for the stream. The best available types rank in this order, according to availability:
     - Multicast (not available for the recording stream).
     - UDP
     - TCP
     - RTSP over HTTP
     - RTSP over TCP
   - **Unicast UDP:** Forces the stream to be sent in UDP to the Archiver. The stream must be formatted using the RTP protocol.
   - **Unicast TCP:** Forces the stream to be sent in *TCP* to the Archiver. Here, TCP is taken in the broad sense. For some types of cameras, the Archiver establishes a TCP connection to the unit and receives the stream in a proprietary protocol. For others, the stream is sent over HTTP. Typically, the stream is not formatted according to the RTP protocol by the unit. The Archiver has to convert the stream to the RTP protocol to be archived or retransmitted to the system.

- **RTSP stream over HTTP:** This is a special case of TCP connection. The Archiver uses the RTSP protocol to request the stream through an HTTP tunnel. The stream is sent back through this tunnel using the RTP protocol. This connection type is used to minimize the number of ports needed to communicate with a unit. It is usually the best way to request the stream when the unit is behind a NAT or firewall, because requests sent to HTTP ports are easily redirected through them.
- **RTSP stream over TCP:** This is another special case of TCP connection. The Archiver uses the RTSP protocol to request the stream in TCP. The request is sent to the RTSP port of the unit.

7 Click **Apply**.

8 Configure the other video streams available on the camera.

Related Topics

Camera - Video tab on page 803

Boosting video recording quality on important events on page 402

Boosting video recording quality on important events

To provide adequate support for future investigations of video footage, you can increase the video quality of the recording stream when important events occur.

What you should know

Typically, the video stream used for recording is of a lower quality (lower frame rate or lower image resolution) than the stream used for live viewing to save storage space.

Boost quality on event recording settings have priority over the *Boost quality on manual recording* settings. The length of the video quality boost depends on the event type, and the camera's recording settings.

To boost video recording quality on important events:

1. From the Config Tool home page, open the *Video* task.
2. Select the camera to configure, and then click the **Video** tab.
3. Turn **ON** one or both of the automatic boost quality settings:
   - **Boost quality on manual recording:** Temporarily boosts video quality when the recording is started manually by a Security Desk user when they click the *Record* (●) button or the *Add bookmark* (🔖) button.
   - **Boost quality on event recording:** Temporarily boosts video quality when the recording is triggered by a *system event* (the *Start recording* action was executed, an *alarm* was triggered, or because of a motion event).
4. In the *Video quality* section, configure the boost quality settings.
5. Click **Apply**.

Any time the manual actions or the system events are triggered, the video quality is boosted for the selected camera.

Boosting video recording quality manually

You can boost the video quality of the recording stream using a manual action.

Before you begin

The video quality settings for the recording stream during *Boost quality on manual recording* and *Boost quality on event recording* must be configured in the camera **Video** tab.

What you should know

Once the video quality is boosted through an action, the custom boost quality settings override the general settings for event recording until you trigger another action, or until the Archiver restarts.

To boost video recording quality manually:

1. In the Security Desk notification tray, click **Hot actions** (📣).
2. In the **Hot actions** dialog box, click **Manual action**.
3. In the **Configure an action** window, select one of the following action types, and select a camera:
   - **Override with manual recording quality:** Turn the **Boost quality on manual recording** option to **ON**.
   - **Override with event recording quality:** .Turn the **Boost quality on event recording** option to **ON**.
4. Click **OK**.

The custom boost quality settings for video recording are applied to the selected camera.

5 To return to the normal recording video quality settings:

a) In the notification tray, click **Hot actions** (📢).

b) In the **Hot actions** dialog box, click **Manual action**.

c) Select the **Recording quality as standard configuration** action, and select a camera.

d) Click **OK**.

Changing multicast addresses of cameras

If you are short of multicast addresses, you can use the same multicast address for multiple cameras, and assign a different port number to each.

What you should know

Since a multicast address and port number are automatically assigned to a video unit when it is discovered, you only need to edit the multicast addresses when you do not have enough of them (certain switches are limited to 128).

NOTE: Using the same multicast address on multiple encoders is less efficient than using a different address for each encoder, because it causes more network traffic.

To change the multicast address of a video encoder:

1. From the Config Tool home page, open the *Video* task.
2. Select the camera to configure, and click the **Video** tab.
3. In the **Network settings** section, type the **Multicast address** and port number you want to use.

   NOTE: All multicast addresses must be between the range 224.0.1.0 and 239.255.255.255.
4. Click **Apply**.
5. To restart the video unit, select the unit in the roles and units view, and click **Reboot** (⟲) in the toolbar at the bottom of the workspace.

Related Topics
Changing multicast ports of cameras on page 405

Changing multicast ports of cameras

If you are using Windows Server 2008 or earlier, and you have a large number of cameras streaming in multicast, you can greatly improve your system performance by assigning a different multicast port number to each camera on your system.

What you should know

Windows Server 2008 and earlier uses a lot of CPU to process multicast packets when they are on the same port. By default, the system only increments the multicast address assigned to every video encoder it discovers. You need to change the port number as well if you frequently use multicast. That can happen if you use Auxiliary Archivers or if everything is recorded in multicast.

To change the multicast port of a video encoder:

1. From the Config Tool home page, open the *Video* task.
2. Select the camera to configure, and click the **Video** tab.
3. In the **Network settings** section, besides the **Multicast address**, set the port number you want to use.
4. Click **Apply**.
5. To restart the video unit, select the unit in the roles and units view, and click **Reboot** (↺) in the toolbar at the bottom of the workspace.

Related Topics

Changing multicast addresses of cameras on page 404

Testing video settings of cameras

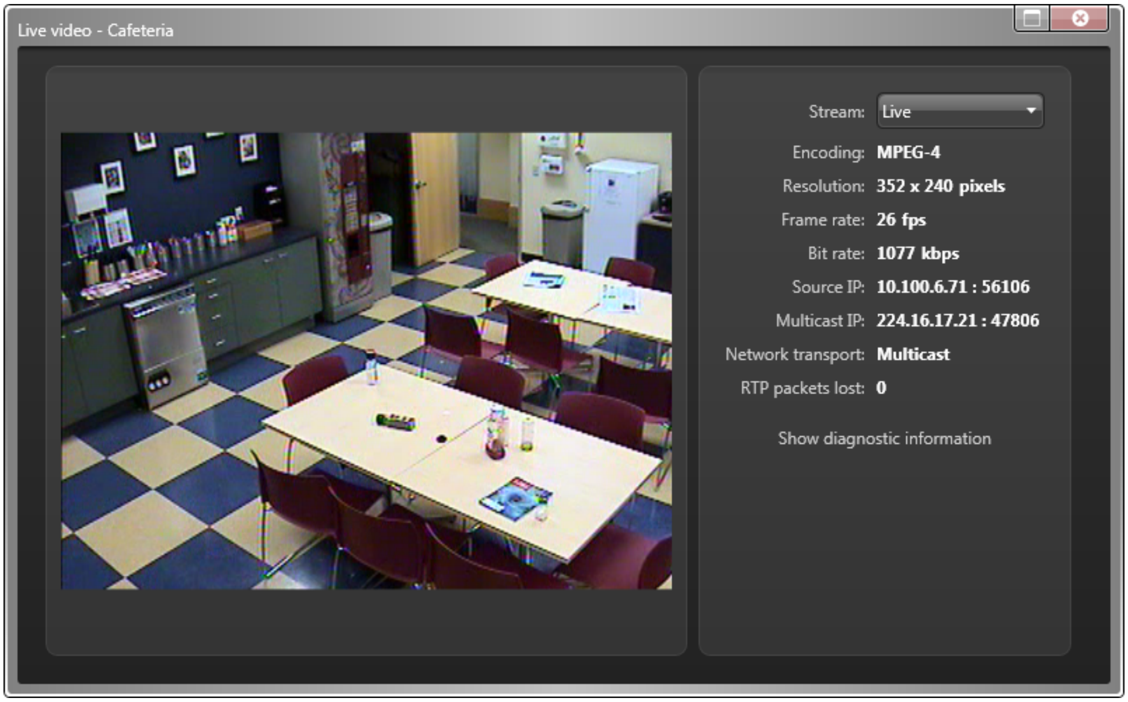
After configuring your cameras, test that the video settings are correct, and make sure that you can view the camera properly.

To test a camera’s video settings:

1 Open the **Video** task, and do one of the following:

- Double-click the camera you want to test.
- Select the camera, and then in the toolbar at the bottom of the workspace, click **Live video** (▶).

The **Live video** dialog box opens and shows you live statistics about the video stream that is coming from the video encoder.



Live video - Cafeteria

Stream: Live

Encoding: MPEG-4

Resolution: 352 x 240 pixels

Frame rate: 26 fps

Bit rate: 1077 kbps

Source IP: 10.100.6.71 : 56106

Multicast IP: 224.16.17.21 : 47806

Network transport: Multicast

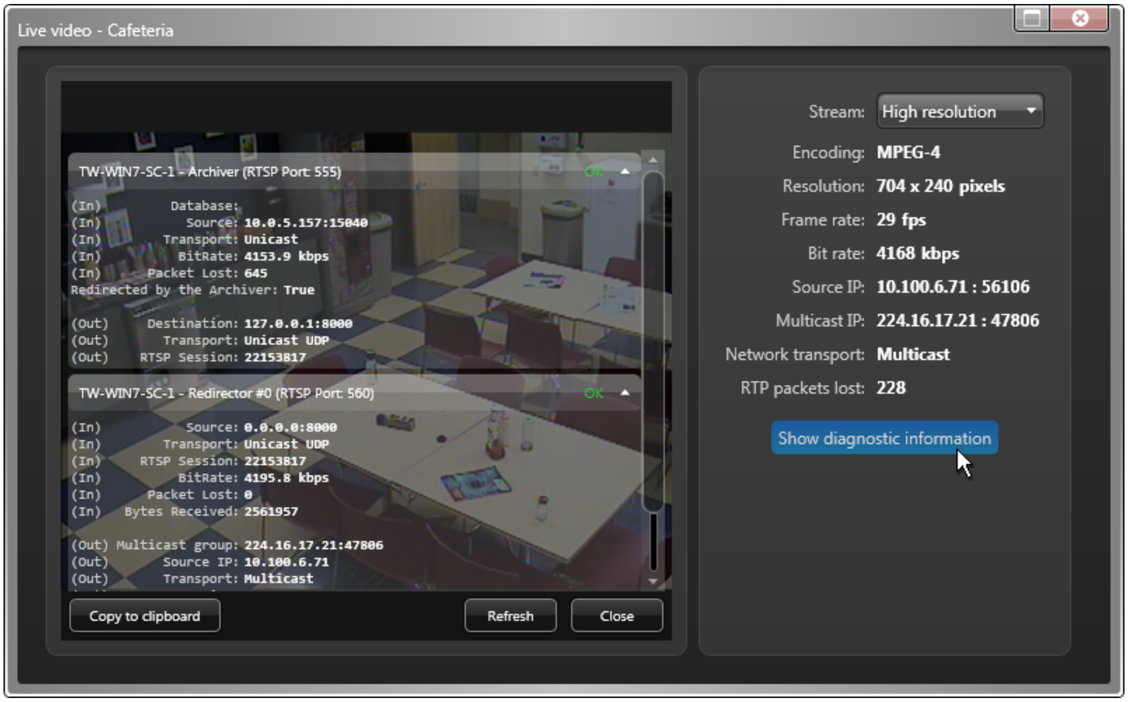
RTP packets lost: 0

Show diagnostic information

2 If you have configured multiple video streams, click the **Stream** drop-down list to select a different stream to view (live, recording, and so on).

3 If you have configured separate **High resolution** and **Low resolution** streams, select **Automatic** from the **Stream** drop-down list, and resize the **Live video** dialog box to test if the stream selection automatically changes.

4 If you are experiencing streaming problems, click **Show diagnostic information** to display diagnostic information as a transparent overlay on the video.



```
TW-WIN7-SC-1 - Archiver (RTSP Port: 555)                    OK
(In)         Database:
(In)           Source: 10.0.5.157:15040
(In)        Transport: Unicast
(In)          BitRate: 4153.9 kbps
(In)      Packet Lost: 645
Redirected by the Archiver: True

(Out)     Destination: 127.0.0.1:8000
(Out)       Transport: Unicast UDP
(Out)    RTSP Session: 22153817

TW-WIN7-SC-1 - Redirector #0 (RTSP Port: 560)               OK
(In)           Source: 0.0.0.0:8000
(In)        Transport: Unicast UDP
(In)     RTSP Session: 22153817
(In)          BitRate: 4195.8 kbps
(In)      Packet Lost: 0
(In)   Bytes Received: 2561957

(Out) Multicast group: 224.16.17.21:47806
(Out)       Source IP: 10.100.6.71
(Out)       Transport: Multicast
```

Stream: High resolution
Encoding: MPEG-4
Resolution: 704 x 240 pixels
Frame rate: 29 fps
Bit rate: 4168 kbps
Source IP: 10.100.6.71 : 56106
Multicast IP: 224.16.17.21 : 47806
Network transport: Multicast
RTP packets lost: 228

5 To capture that information to send it to Technical Support, click **Copy to clipboard**.

6 To hide the diagnostic information, click **Close.**

About motion detection

Motion detection is the feature that watches for changes in a series of video images. The definition of what constitutes motion in a video can be based on highly sophisticated criteria.

There are two types of motion detection:

- **Software motion detection:** Motion detection is executed by the *Archiver* on the video stream set for recording and motion events are generated by Security Center.
- **Hardware motion detection:** Motion detection is executed by the *video unit*, and motion events are generated by the unit and transmitted to Security Center.

Supported capabilities differ between the two types as shown in the table below.

Capability	Software	Hardware
Configuring motion detection settings	Config Tool	Unit's proprietary configuration tool[1]
Supports Motion search task in Security Desk	Yes	See the Supported Device List[2]
Shows motion indicators (green bars) in the timeline during video playback	Yes	See the Supported Device List[2]
Supports multiple motion detection zones	Yes	Camera specific[3]
Requires additional server resources	Yes	No
Auto calibration of the sensitivity[4]	Yes	No

IMPORTANT:

1 When configuring hardware motion detection, the motion blocks shown in Config Tool are the result of software motion detection. Because the unit does not report motion levels to Security Center and the results between software and hardware motion detection are similar enough, motion blocks are shown to ease the configuration of the hardware motion detection.

2 Some cameras support motion detection as part of their video analytic capabilities. To see if a camera supports video analytics, check the Supported Device List.

3 Not all units support multiple motion detection zones. If you switch motion detection from **Archiver** to **Unit**, the existing zone configurations not supported by the unit are lost.

4 The unit might not interpret the sensitivity the same way as the Archiver does. Therefore, when testing your motion zones in Config Tool, the results might not accurately reflect the behavior of the unit.

To configure motion detection, you must specify how motion is detected on a video stream, and when the motion detection settings apply based on a schedule. Every camera has a default motion detection configuration based on the **Always** schedule. The default motion detection configuration can be modified but not deleted.

When an *H.264* stream is selected as the recording stream, the **Advanced settings** button becomes available. Clicking this button opens the **H.264 advanced motion detection settings** dialog box that can be used to refine the motion detection settings.

Motion block

A *motion block* is when motion is detected inside one of the blocks you configure on the video image. There is positive motion in a video image when the area covered by the block detects motion in two consecutive video frames. The number of motion blocks detected represents the amount of motion. A motion block is represented by a semi-transparent green square overlay on the video image.

Positive motion detection

Simply seeing motion blocks on the video does not necessarily mean that the system will generate a motion related event. It could simply be noise. To determine when motion actually started (*Motion on* event) and when it stopped (*Motion off* event), the *Sensitivity* and *Consecutive frame hits*, *Motion on threshold*, and the *Motion off threshold* parameters must be adjusted to achieve the best results in the specific environment.

Best practices for configuring motion detection

The main purpose for using motion detection is to reduce the amount of video recordings that must be saved on storage devices to minimize the storage requirements, and to reduce the time needed for performing video searches. However, configuration of motion detection must be done carefully. In most cases, the same motion settings cannot be used on all cameras at once if you want to achieve the optimal motion detection for each camera. When configuring motion detection, consider the following:

- Depending on the environment in which the camera is installed, it can be normal to receive false motion events. It is preferable to have more sensitive settings that might trigger more false events than being not sensitive enough, in which case expected recordings would be missing.
- Because all motion settings are stored in the Directory database, make sure to backup your database when changes are made.
- Motion detection is the most basic video analytic capability. Due to possible false motion events, it should not be used to trigger alarms in critical situations, for example in replacement to a specialized intrusion detection system.
- Be careful not to set the **Time to record before an event** parameter to a value that is too large. The higher the value and the more memory (RAM) resources are required by the Archiver. This reduces the camera count allowed on the Archiver. Cameras with a higher resolution also have the same effect on the memory resources required.

  For example, buffering a 2 Mbps stream for 5 minutes will require 75 MB of RAM.

When configuring software motion detection:

- It is always possible to use MJPEG streams.
- It is possible to use MPEG-4 streams.
- It is also possible to use H.264 streams but because of the notion of *profiles*, some cameras must be configured through the additional **H.264 advanced motion detection settings** dialog box.

For pre-configuration instructions or any additional configuration steps required to enable motion detection in Security Center for specific video units, see the *Security Center Video Unit Configuration Guide*.

Configuring motion detection

If you want to monitor and report on motion detected in a camera image, you must configure motion detection for the video unit.

Before you begin

Make sure the unit supports motion detection.

What you should know

Motion detection can be performed by the Archiver or by the unit, on the entire video image (default) or only on certain areas (motion zones).

BEST PRACTICE: For H.264 and MPEG-4 streams, software motion detection is performed by analyzing P-frames. Ensure that your video stream is not made up of only key frames when configuring the *Key frame interval* and *Frame rate* settings of the camera.

To learn more about configuring advanced motion detection, watch our GTAP Webinar.

To configure motion detection:

1. From the Config Tool home page, open the *Video* task.
2. Select the camera to configure, and click the **Motion detection** tab.
3. Turn the **Motion detection** option to **ON**.
4. From the **Detection is done on** option, select whether motion detection is performed by the Archiver or the video unit.
5. In **Sensitivity** option, select how much of a difference must be detected in a *block* between two consecutive frames before it is highlighted as a *motion block*.

   A plain image, such as viewing an empty wall, is more prone to generate noise than an image containing a lot of detail.

   TIP: First set a high value, and then slowly lower it until you are only receiving a few false motion reads in the image.

   You can also calibrate the sensitivity automatically.

6. In the **Consecutive frame hits** option, select how many frames in a row the *Motion on threshold* must be reached for a positive motion hit to be generated.
7. Define the motion detection zones.
8. Set the motion detection criteria for each motion zone as follows:

   If these values are too low, then motion will be detected too often. If these values are too close together, then you might receive many consecutive *Motion on* and *Motion off* events.

   - **Motion on threshold:** Indicates the minimum number of *motion blocks* that must be detected before the motion is significant enough to be reported. Together with the *Consecutive frame hits*, a positive motion detection is made.
   - **Motion off threshold:** Detects the end of motion. Motion is considered to have ended when the number of motion blocks drops below the *Motion off threshold* for at least 5 seconds.

9. Select the event types you want to generate when motion is detected for each motion zone.

Related Topics

Camera - Motion detection tab on page 808
Troubleshooting: Axis P1428-E camera sensitivity issue on page 481
Motion detection is not working in Security Center on page 482
KBA: Axis cameras do not have a Motion detection tab on page 483

Automatically calibrating motion detection sensitivity

You can determine what constitutes positive motion detection by automatically calibrating the sensitivity value.

Before you begin

Make sure there is no motion in the camera’s field of view (0 motion blocks).

What you should know

If your camera is located outdoors, the accuracy of this test might be affected due to wind, moving trees, and so on.

To automatically set the motion detection sensitivity:

1 Open the **Video** task.
2 Select the camera to configure, and click the **Motion detection** tab.
3 Select one of the following options from the **Auto calibrate** drop-down list:

- **Current zone:** Calibrate the sensitivity for motion detected in the currently selected motion zone on the video image.
- **All zones:** Calibrate the sensitivity for motion detected in all the motion zones on the video image.
- **All motion:** Calibrate the sensitivity for motion detected on the whole video image.

Different sensitivity values are tested to find the highest value without detecting motion in the image. This test accounts for any unwanted background noise that your camera may pick up and consider as motion.

Defining motion detection zones

To define the areas of the video image where motion is meaningful, you can draw motion detection zones, or *blocks* (blue rectangles) on the image.

To define a motion detection zone:

1 Open the **Video** task.
2 Select the camera to configure, and click the **Motion detection** tab.
3 Under **Motion zone 1**, use the following tools to define the motion detection zone:

TIP: For cameras that are positioned near a window or door, make sure that the motion detection zone covers that important area.

- To cover the entire image with motion detection blocks, use the**Fill** (🟩) tool.
- To draw a group of motion detection blocks, use the **Rectangle** (▦) tool.
- To draw single motion detection blocks, use the **Pen** (✎) tool.
- To interchange the area with motion detection blocks and the area without any selected blocks, use the **Invert** (▦) tool.
- To erase all the motion detection blocks in the image, use the **Clear all** (☒) tool.
- To erase the motion detection blocks that are not needed, use the **Eraser** (▱) tool.

4 To remove the blocks where motion typically occurs so they do not generate false motion reads, click **Learning mode** (💡).

You should only use this option if the video image is displaying what it normally does. If there is usually a lot of motion in the image, but you use the *Learning mode* in the middle of the night, it is not helpful.

The affected areas where motion typically occurs are turned off.

5 If necessary, add additional motion detection zones to the image.
6 Click **Apply**.

Selecting which events are triggered on motion

When motion is detected on a motion zone, you can select which event is triggered when the motion period starts, and which one is triggered when it stops.

What you should know

The default events that are triggered when motion detection is generated are the following:

- **Motion on:** Default event triggered at the beginning of the motion period.
- **Motion off:** Default event triggered at the end of the motion period.

Using custom events is useful when you have multiple motion zones. Each zone can be configured to detect motion in a different area of the camera’s field of view and generate different events. Having different events allows you to program different actions to respond to different situations.

To select which events are triggered on motion:

1 Open the **Video** task.
2 Select the camera to configure, and click the **Motion detection** tab.
3 Under **Motion zone 1**, click **Events**.
4 In the **Motion events** dialog box, select which events will be triggered for the **Motion on event** and the **Motion off event**.
5 Click **OK**, and then click **Apply**.
6 If you have more than one motion zone configured, repeat the steps for each zone.

Testing motion detection settings

After modifying the motion detection settings for a camera, test your new settings to make sure that you get the expected results.

What you should know

There are limitations with hardware motion detection. If motion detection is performed on the unit, then the test might not be completely accurate.

CAUTION: Light reflections on windows, switching lights on/off, and light level changes caused by cloud movement can cause undesirable motion detection responses, and generate false alarms. Therefore, carry out a number of tests for different day and night conditions to make sure the motion detection is interpreted correctly. For surveillance of indoor areas, ensure there is consistent lighting of the areas during the day and at night. Uniform surfaces without contrast can trigger false alarms even with uniform lighting.

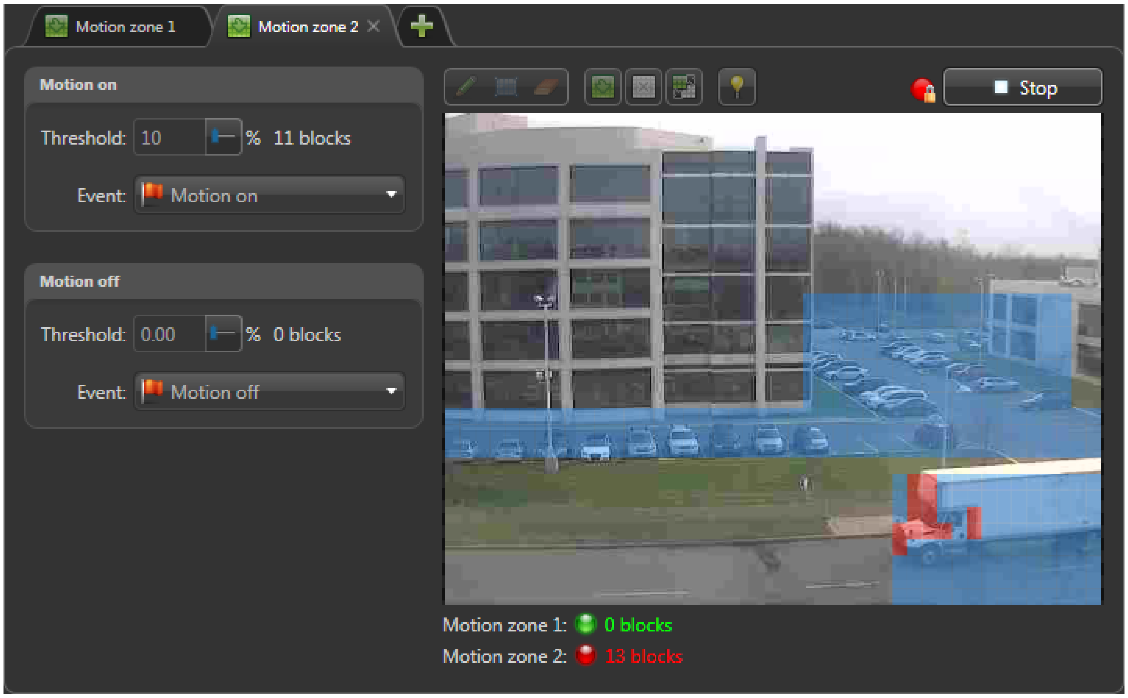
To test your motion detection settings:

1 From the Config Tool home page, open the *Video* task.
2 Select the camera to configure, and click the **Motion detection** tab.
3 Under **Motion zone**, select one of the following test modes from the **Test zone** drop-down list:

- **Test zone:** The motion zone is displayed as blue overlays. The *motion blocks* are displayed as green overlays. The number of motion blocks is updated in real time. When the number of motion blocks reaches the *Motion threshold*, it is displayed in red.

  NOTE: If the camera is configured to record on motion, the recording state (●) will turn red when the ***Motion threshold*** is reached.

- **Test all zones:** In this mode, all *motion zones*are displayed at once, with the number of motion blocks in each displayed separately.



Motion on
Threshold: 10 % 11 blocks
Event: Motion on

Motion off
Threshold: 0.00 % 0 blocks
Event: Motion off

Motion zone 1: 0 blocks
Motion zone 2: 13 blocks

- **View all motion:** In this mode, the entire video image is tested for motion. All motion anywhere on the image is displayed as motion blocks (green overlays). The total number of motion blocks is updated in real time. Use this mode to test the sensitivity setting for this camera.

Related Topics

About motion detection on page 408

Adjusting camera color settings

You can adjust the video attributes such as brightness, contrast, hue and saturation for a camera based on schedules, to account for different times of the day.

Before you begin

Schedules must be created before you set the video attributes for that schedule.

What you should know

These settings are helpful for twilight schedules since the ambient lighting is different at dawn and dusk.

To adjust the color settings of a camera:

1. From the Config Tool home page, open the *Video* task.
2. Select a camera, and then click the **Color** tab.
3. Adjust the **Brightness**, **Contrast**, **Hue**, and **Saturation** for the video image.
4. To add a new color configuration, click **Add schedule**.
5. Select a previously created schedule, and click **Add**.
6. Adjust the **Brightness**, **Contrast**, **Hue**, and **Saturation** for the video image during that schedule.
7. To reset all parameters to their default values, click **Load default**.
8. Click **Apply**.

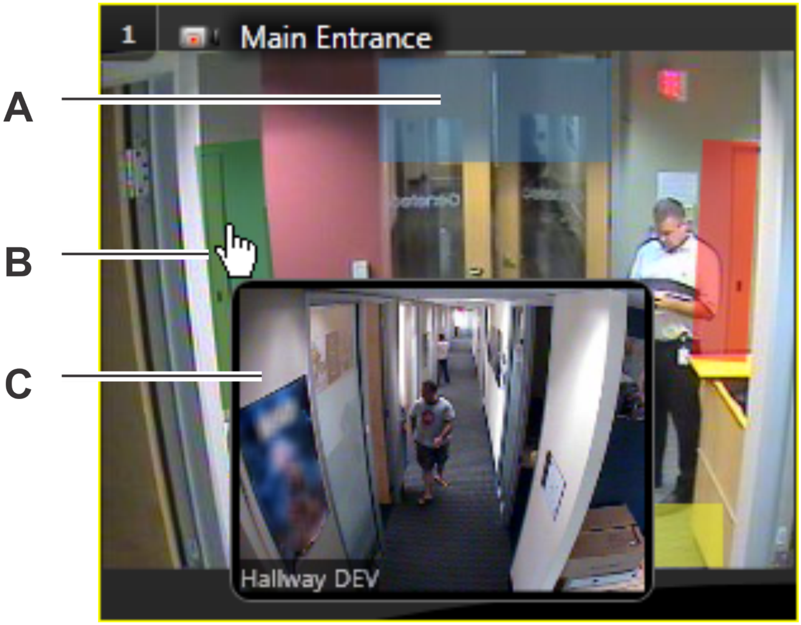
Related Topics
About twilight schedules on page 167

About visual tracking

Visual tracking is a Security Desk feature that allows you to follow an individual across different areas of your company without ever losing sight of that individual, as long as the places this person goes through are monitored by cameras.

Visual tracking works with both live and playback video. When visual tracking is turned on, semi-transparent overlays (colored shapes drawn over the video) appear in the tile where the camera is displayed. Each overlay corresponds to one or more adjacent cameras that you can jump to.

In addition, when more than one camera is associated to a given overlay, a list of camera names is shown instead of the video preview. You must pick a camera name to switch to that camera. The video stream displayed in the tile switches to the next camera, as determined by the visual tracking configuration.



A	Semi-transparent overlays on the video image signify a visual tracking link to another camera.
B	Click on colored overlay to switch to the next camera.
C	Hovering your mouse pointer over the overlay produces a preview of the next camera.

Configuring visual tracking

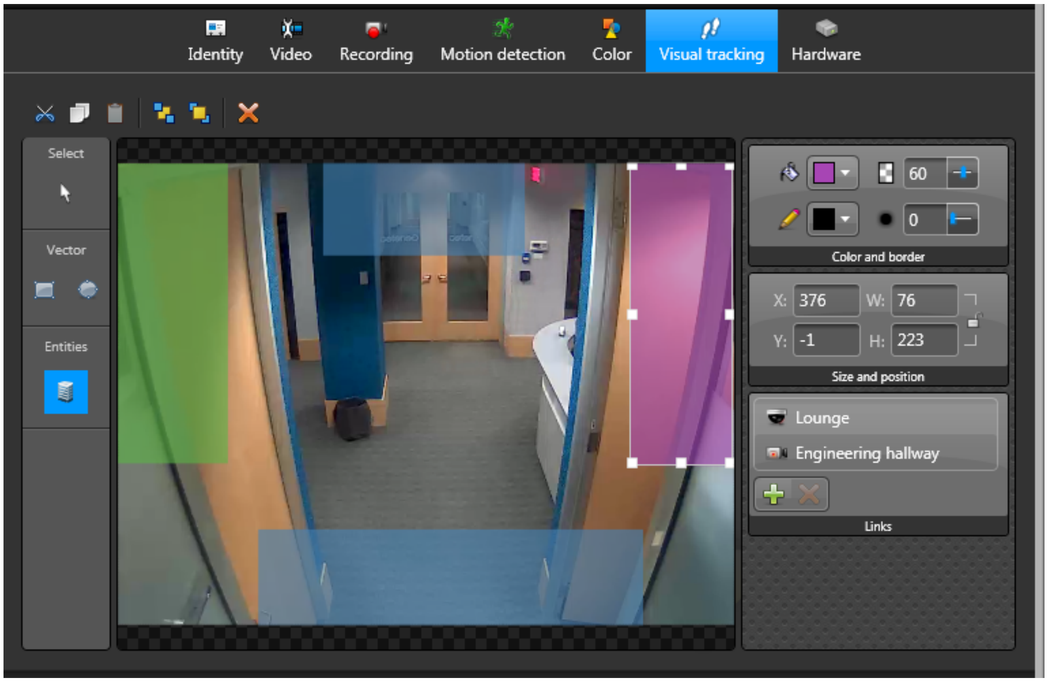
To jump to adjacent cameras from a displayed camera in Security Desk, you must configure visual tracking by creating on-video overlays (colored shapes) for a camera.

What you should know

Visual tracking is supported for PTZ cameras only if they are used as fixed cameras.

To configure visual tracking:

1 Open the **Area view** task.
2 Select a camera, and click the **Visual tracking** tab.
3 Select one of the **Rectangle** or **Ellipse** drawing tool, and draw a shape over the live video displayed to the right.
4 Resize, reposition, and rotate the shape using your mouse, or using the **Size** and **Position** parameters.



Size and position: X: 376, W: 76, Y: -1, H: 223; opacity 60; border 0

5 Select the fill color and opacity for the overlay.

TIP: Setting the opacity at 60 percent is a good balance between transparency and visibility.

6 Set a border color and a border thickness.
7 From the area view inside the **Visual tracking** tab, drag the cameras you want to jump to onto the colored shape.

NOTE: If the area view is not shown inside the **Visual tracking** tab, click **Entities** ( ) in the toolbar to display it.

The camera names appear in the **Entities** box. If more than one camera is associated with the same overlay, the Security Desk user must select a camera before jumping to that camera, instead of just clicking on the colored overlay.

8 Add as many overlays as necessary.
9 Click **Apply**.

Viewing camera settings

At a glance, you can view a list of all the local and federated Security Center cameras that are part of your system and their settings, using the *Camera configuration* report.

What you should know

The Camera configuration report is helpful for comparing camera settings, and making sure that your cameras are configured properly according to your requirements. If the camera has multiple video streams or multiple streaming schedules set, each stream and schedule is displayed as a separate result item.

This report is not supported with Security Center 5.0-5.2 federated cameras or Omnicast™ federated cameras.

NOTE: This report might take a few minutes to generate, depending on how many cameras you are querying.

To view the settings of cameras in your system:

1 Open the **Camera configuration** task.

2 Set up the query filters for the report. Choose one or more of the following filters:

- **Cameras:** Select the camera to investigate.
- **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.

3 Click **Generate report**.

The following camera settings are listed in the report pane:

- **Bit rate:** Bit rate setting for the camera.
- **Camera:** Camera name.
- **Description:** Entity description.
- **Edge transfer:** Whether the camera is configured for edge transfer or not (yes or no).
- **Entity path:** List of all parent areas, starting from the system entity. If the camera has multiple parent areas, "*\" is shown as the path.
- **Frame rate:** Frame rate setting for the camera.
- **Image quality:** Image quality setting for the camera.
- **Key frame interval:** Key frame interval setting for the camera.
- **Logical ID:** Logical ID of the camera.
- **Manufacturer:** Manufacturer of the unit.
- **Multicast address:** Multicast address of the camera.
- **Network setting:** Connection type used by the camera.
- **Owner:** Archiver that manages the camera.
- **Port:** Connection port of the video unit.
- **Product type:** Model or series of the video unit.
- **Recording mode:** Recording settings for the camera.
- **Resolution:** Resolution of the camera's video stream.
- **Stream:** The video stream of the camera.
- **Stream usage:** Purpose of the video stream (for live video, recordings, and so on).

- **Streaming schedule:** Schedule when the camera streams video.
- **Type:** Type of camera (fixed camera or PTZ camera).

4. To modify the settings of a camera, right-click an item in the report pane, and then click **Configure entity** (⚙) to jump to that entity’s configuration page in Config Tool.

   NOTE: You need the user privilege to modify entities to use this command.

Configuring PTZ motors

If the PTZ motor is not integrated with your camera on the video unit, you need to configure the PTZ motor separately before you can control it in Security Desk.

What you should know

Some PTZ motors support the following additional commands:

- **Zoom-box:** Zoom in on an area by drawing a box on the video image using your mouse. This works like the digital zoom for fixed cameras.
- **Center-on-click:** Center the camera on a point of the video image with a single click.
- **Enhanced zoom:** Zoom in or out to a specific zoom factor (absolute value) using the slider available in the tile. For example, you can move the slider to 10x and it will keep its position when released. When **Enhanced PTZ** is disabled, the zoom factor is not available and the slider returns to its center position when released, similar to a joystick used to pan and tilt a camera.

When these commands are enabled, they replace the normal pan, tilt, and zoom commands when controlling the PTZ in Security Desk.

To configure PTZ motors:

1. From the Config Tool home page, open the *Video* task.
2. Select the camera to configure, and click the **Hardware** tab.
3. Switch the **PTZ** option to **ON**.
4. From the **Protocol** drop-down list, select the protocol used by the PTZ motor.
5. Beside the **Protocol** field, click ✎ to set the **Idle delay**, **Idle command**, and **Lock delay** options.
6. From the **Serial port** drop-down list, select the serial port used to control the PTZ motor.
7. In the **PTZ address** box, select the number that identifies the PTZ motor on the serial port.

   This number is important because it is possible to connect more than one PTZ motor on the same serial port. This number must correspond to the dip switch settings on the PTZ hardware.
8. To enable the enhanced PTZ commands (zoom-box, center-on-click and enhanced zoom), switch the **Enhanced PTZ** option to **ON**, and calibrate the PTZ coordinates.
9. Click **Apply.**

After you finish

- Test the PTZ motor.
- Define which users have priority to control the PTZ motor.

Related Topics
Camera - Hardware tab on page 812

Calibrating PTZ coordinates

For most cameras, you need to calibrate the limits of the PTZ movement in order to use the zoom-box, center-on-click and enhanced zoom commands properly in Security Desk.

What you should know

Not all cameras require PTZ calibration. For example, Axis cameras do not require calibration.

To calibrate the PTZ coordinates:

1 Open the **Video** task.
2 Select the camera, and click the **Hardware** tab.
3 Next to the **Enhanced PTZ** option, click **Calibrate**.
4 To set the PTZ coordinates automatically, click **Calibration assistant**, and follow the on-screen instructions.
5 To set the PTZ coordinates manually, move the PTZ motor around in the live video image, and enter the corresponding values on the right:

   - **Max zoom factor:** Zoom in to the maximum level you want Security Desk users to reach, and enter the **Zoom** value from the **Coordinates** section.
   - **Horizontal field of view:** Enter the horizontal field of view specified by the camera manufacturer. If you do not have this information, zoom out until the **Zoom** value indicates 1x, and estimate the angle of the horizontal field of view from the image you see on screen.
   - **Vertical field of view:** Enter the vertical field of view specified by the camera manufacturer. If you do not have this information, zoom out until the **Zoom** value indicates 1x, and estimate the angle of the vertical field of view from the image you see on screen.
   - **Minimum pan angle:** Turn the camera to the left-most position of the area under surveillance, and enter the **Pan** value from the **Coordinates** section.
   - **Maximum pan angle:** Turn the camera to the right-most position of the area under surveillance, and enter the **Pan** value read from the **Coordinates** section.
   - **Minimum tilt angle:** Turn the camera to the bottommost position of the area under surveillance, and enter the **Tilt** value read from the **Coordinates** section.
   - **Maximum tilt angle:** Turn the camera to the topmost position of the area under surveillance, and enter the **Tilt** value read from the **Coordinates** section.

6 If you want to flip the camera image at any point, select one of the following from the **Flip camera** drop-down list:

   - **Minimum tilt:** Flips the camera image when the PTZ motor reaches the minimum tilt coordinate.
   - **Maximum tilt:** Flips the camera image when the PTZ motor reaches the maximum tilt coordinate.

7 If you see that the **Minimum pan angle** value is higher than the **Maximum pan angle** value, select the **Invert pan axis** option.
8 If you see that the **Minimum tilt angle** value is higher than the **Maximum tilt angle** value, select the **Invert tilt axis** option.

After you finish

Test the zoom-box, center-on-click and enhanced zoom commands from a Security Desk tile. If needed, adjust the calibration, and test the PTZ camera again.

Testing PTZ controls

After you set up your PTZ motor, you should test if the controls are working properly.

What you should know

Every time you change a PTZ parameter, you must remove the camera from the tile and drag it back to the tile for your changes to take effect.

To test PTZ controls:

1 Open the **Video** task, and do one of the following:

   - Double-click the camera you want to test.
   - Select the camera, and then in the toolbar at the bottom of the workspace, click **Live video** (🎥).

2 In the **Live video** dialog box, test the PTZ controls in the video image using the PTZ widget.

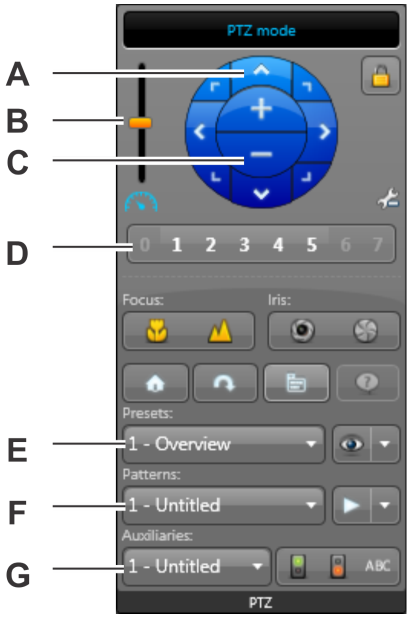
Related Topics

PTZ widget on page 423

PTZ widget

The *PTZ* widget is used to perform pan, tilt, and zoom operations on the displayed camera. It appears in the dashboard when the selected tile is displaying a PTZ-enabled camera (📷).

IMPORTANT: Not all PTZ cameras support all PTZ commands. If one or more of the PTZ buttons are greyed out, it means that the PTZ camera you are working with does not support that command.



Button/Letter	Command	Description
A	**Direction arrows**	Pan the PTZ motor using the eight direction arrows.
B	**Speed slider**	Adjust the speed of the PTZ motor.
C	**Zoom in/out**	Zoom in and out using the plus (+) and minus (-) commands.
D	**Quick access buttons**	Move the PTZ motor to one of the eight quick access PTZ presets.
E	**Presets**	Select a preset from the drop-down list to move the PTZ motor to that preset, save a new preset position, or rename the preset.
F	**Patterns**	Select a PTZ pattern from the drop-down list to start a PTZ pattern (series of presets or recorded PTZ movements), record a new pattern, or rename the pattern.
G	**Auxiliaries**	Select an auxiliary from the drop-down list to start or stop an auxiliary command, or rename the auxiliary command.
🔒	**Lock PTZ**	Lock the PTZ motor so only you have control of the PTZ.
🔧	**Toggle to advanced mode**	Open the PTZ Advanced mode menu.

Button/Letter	Command	Description
✿	**Focus near**	Focus the PTZ near.
⛰	**Focus far**	Focus the PTZ far.
◉	**Open iris**	Manually control the iris (open iris).
⊛	**Close iris**	Manually control the iris (close iris).
⌂	**PTZ home**	Go to the PTZ home (default) position.
↷	**Flip**	Flip the PTZ motor 180 degrees.
▤	**Menu on/off**	Open the PTZ menu. This option is only for analog PTZ cameras.
?	**Specific commands**	Use commands that are specific to that camera model.
👁	**Go to preset**	Jump to the preset position selected in the drop-down list. • **Save:** Save the preset selected in the drop-down list, using the current PTZ position. • **Clear preset:** Clear the PTZ position from the preset.
▶	**Start pattern**	Start the PTZ pattern selected in the drop-down list. You can click any preset of PTZ button to stop the pattern. • **Rename:** Rename the selected preset, pattern, or auxiliary. • **Record pattern:** Record a new PTZ pattern. • **Clear pattern:** Clear the pattern.
🟢	**Start auxiliary command**	Start a PTZ auxiliary command (for example, a wiper blade).
🔴	**Stop auxiliary command**	Stop the PTZ auxiliary command.
ABC	**Rename**	Rename the selected preset, pattern, or auxiliary.

Defining user levels for controlling PTZ motors

You can select which users or user groups have priority to control different PTZ cameras, by overriding their general user level for specific areas or cameras.

What you should know

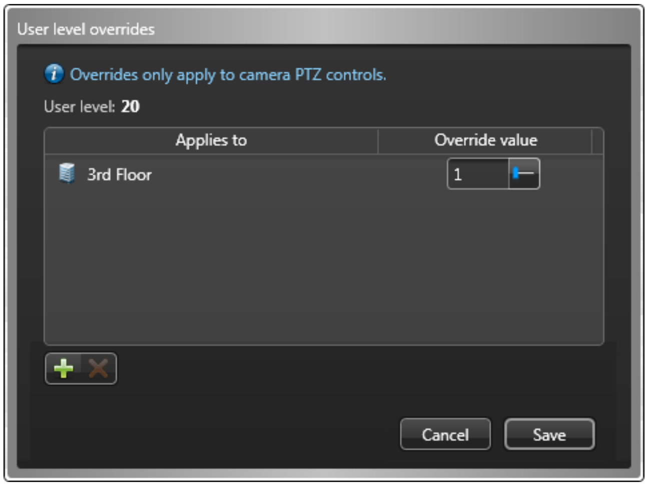
By default, priority to control PTZ cameras is determined by a user's general *user level*, which is set individually or inherited by their parent user group. However, user level overrides take precedence over their general user level for controlling PTZ motors. You can create an override for PTZ controls by area or camera. If you override a user level for an area, it applies to all PTZ cameras in that area.

Setting user level overrides for PTZ controls is helpful if you have multiple user groups who all have access to the same cameras. For example, if a user has a general user level of 30, you can promote them to a user level of 2 for a camera that they should always be able to control.

To define user levels for controlling a PTZ motor:

1 From the Config Tool home page, open the *User management* task.
2 Select the user or user group to configure, and click the **Properties** tab.
3 Set the **User level** option to **Override**, and then click **Configure PTZ overrides**.
4 In the **User level overrides** dialog box, click **Add an item** (✚).
5 Select the camera or area to create the override for, and click **OK**.
6 In the **Override value** column, select a user level that applies to the camera or area.
7 Click **Save** > **Apply**.

Example: Paul is a member of the Operator user group in his company, and he is in charge of monitoring the third floor of their building. As part of the Operator user group, by default he has a user level of 20. Because he is in charge of monitoring the third floor, he needs to have the highest priority to control all the PTZ cameras on that floor. Therefore, a user level override with the value of 1 is created for him for the third floor.



User level overrides

Overrides only apply to camera PTZ controls.

User level: **20**

Applies to	Override value
3rd Floor	1

About camera sequences

A camera sequence is a type of entity that defines a list of cameras that are displayed one after another in a rotating fashion within a single tile in Security Desk.

When displayed in a Security Desk, the camera sequence can be paused (stop cycling) and unpacked (showing all cameras at the same time).

The cameras composing the sequence can be fixed, PTZ enabled, or federated. Each camera is given a preset amount of display time. PTZ cameras can be configured to point to a preset position, to run a pattern, or to turn on/off an auxiliary switch.

Creating camera sequences

You can group fixed, PTZ-enabled, and federated cameras into a camera sequence, so they are displayed one after another in Security Desk tiles.

What you should know

The cameras in the camera sequence list are displayed in the same order in Security Desk.

To create a camera sequence:

1 Open the **Area view** task.

2 Click **Add an entity** (➕) > **Camera sequence**.

A new camera sequence entity (📹) appears in the area view.

3 Type a name for the camera sequence, and press **ENTER**.

4 Click the **Cameras** tab, and click **Add an item** (➕).

5 From the **Camera** drop-down list, select a camera to be part of the sequence.

6 In the **Dwell time** box, set the amount of time the camera is displayed when cycling through the sequence.

7 From the **PTZ command** drop-down list, choose what action the PTZ camera will perform when it is displayed in the sequence.

This option is only for PTZ-enabled cameras.

- **Preset:** Move the PTZ camera to a preset position.
- **Position:** Start a PTZ pattern.

8 From the **PTZ auxiliary** drop-down list, configure the switch number and the state to set it to.

This option is only for PTZ-enabled cameras that support auxiliary switches.

9 Click **Save** > **Apply**.

10 If necessary, add additional cameras to the sequence.

11 To change the order of the cameras in the sequence, use the ⌃ and ⌄ buttons.

12 To remove a camera from the sequence, select the camera, and click **Remove the item** (✖).

13 Click **Apply**.

Related Topics
About camera sequences on page 426

About analog monitors

An analog monitor is a type of entity that represents a monitor that displays video from an analog source, such as a video decoder or an analog camera. This term is used in Security Center to refer to monitors that are not controlled by a computer.

A video decoder is a device that converts a digital video stream into analog signals (NTSC or PAL) for display on an analog monitor. It is one of the many devices found on a video decoding unit. A video decoding unit can have multiple video decoders, each connected to an analog monitor. Each video decoder found on a video decoding unit is represented by an analog monitor entity in Security Center.

The *monitor group* entity is used to configure the properties of a group of analog monitors.

Configuring analog monitors

To achieve optimal performance with your analog monitor, configure its settings.

What you should know

Analog monitor entities are automatically created when the video decoding units they are connected to are added to your system. Although Security Center provides workable default settings when analog monitor entities are added, we recommend that you configure each analog monitor.

To configure analog monitors:

1. Add a video decoding unit to your system.

   Analog monitors that are connected to the video decoding unit are automatically added as analog monitor entities.
2. From the Config Tool home page, open the *Video* task.
3. Select an analog monitor to configure, and then click the **Properties** tab.
4. Configure the video settings, network settings, and the hardware connected to the analog monitor.
5. Click **Apply**.
6. Configure each analog monitor connected to the decoder.

Related Topics
Analog monitor - Properties tab on page 797

Adding analog monitors as alarm recipients

To receive alarms on your physical analog monitors, you must create a monitor group, and then add that group as recipient of the alarm.

What you should know

When you receive alarms on an analog monitor, high priority alarms do not replace lower priority alarms that are displayed on the monitor. For more information about viewing video or receiving alarms in analog monitors in Security Desk, see the *Security Desk User Guide*.

IMPORTANT: If you add more than one analog monitor to a monitor group, the first analog monitor in the list will receive the highest priority alarm, the second analog monitor will receive the second highest priority alarm, and so on. The last analog monitor in the monitor group list will receive all the other alarms.

To add analog monitors as alarm recipients:

1. Open the **Alarms** task, and click the **Monitor groups** view.
2. Click **Monitor group** (➕), and type a name for your monitor group.
3. Select the monitor group, and click the **Monitors** tab.
4. At the bottom of the page, click ➕, select the analog monitors to be part of the monitor group, and then click **OK**.

   You can select multiple analog monitors by holding the **SHIFT** or **CTRL** keys.
5. Click **Apply**.
6. In the **Alarms** task, click the **Alarms** view, select an alarm, and then click the **Properties** tab.
7. In the **Recipients** section, click ➕, select the monitor groups to be recipients of the alarm, and then click **OK**.
8. Click **Apply**.

Analog monitors that are part of the monitor group are now recipients of the alarm. When the alarm is triggered, the video associated with the alarm is shown on the physical analog monitor.

Testing analog monitor settings

After configuring your analog monitors, you should always test to make sure you can view video on the analog monitors.

Before you begin

Make sure the cameras you want to test viewing video with are supported (same manufacturer as the decoder, and use the same video format).

What you should know

For more information about viewing video in an analog monitor in Security Desk, see the *Security Desk User Guide*.

To test analog monitor settings:

1 Open Security Desk.

2 In the Monitoring task, display an analog monitor in a canvas tile, and then add a supported camera to the tile.

25

Video archives

This section includes the following topics:

About video archives

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

Each Archiver is responsible for the video archives of the *cameras* it controls. The video archives are divided into the archive database, and the archive storage.

Archive database

The archive database is a database in your Security Center system that stores video recordings and *events*. Each Archiver role and Auxiliary Archiver role in your system maintains an archive database.

The archive database stores the following types of information:

- A catalog of the recorded video footage.
- Events describing the recording activities, such as when recording started and stopped, and what triggered the event.
- Events associated with the recorded video footage, such as motion detected, *bookmarks*, and occasionally, metadata.
- Events related to the archiving process, such as *Disk load is over 80%* and *Cannot write to any drive.*

For Archiver roles, the default name of the database is *Archiver*; for Auxiliary Archiver roles, the default name of the database is *AuxiliaryArchiver* .

IMPORTANT: A separate archive database must be configured for each server assigned to the Archiver role or Auxiliary Archiver role. Because of this requirement, the archive database is often hosted locally on each server. When two or more Archiver roles are hosted on the same server, you must assign a different database to each role instead of using the default one.

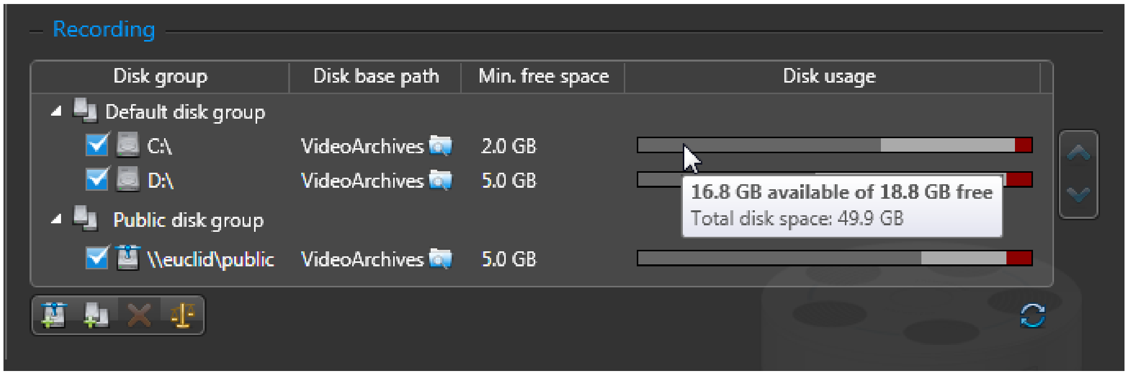
Related Topics
Databases on page 117

Archive storage

In Security Center, your video recordings are not stored in a database. Recordings are stored on disk, in small files with a G64 extension called *video files*. Each video file contains one or many short sequences of video. Similar to the archive database, the archive file storage is also specific to each server.

The location of the video files and the description of the *video sequences* they contain (source camera, beginning and end of sequence) are stored in the database catalog managed by the *Archiver* or *Auxiliary Archiver*. For each Archiver role, you can set the maximum size limit of the video files.

Both local drives and network drives can be used to store video. In the Archiver's **Resources** tab, all local drives found on the host server are listed by default and grouped under *Default Disk Group*, as shown in the following image.



Recording

Disk group	Disk base path	Min. free space	Disk usage
Default disk group			
☑ C:\	VideoArchives	2.0 GB	
☑ D:\	VideoArchives	5.0 GB	
Public disk group			
☑ \\euclid\public	VideoArchives	5.0 GB	

16.8 GB available of 18.8 GB free
Total disk space: 49.9 GB

Disk space cannot be allocated in advance for archiving purpose. Instead, the Archivers can use a certain limit of the available disk space. This limit is defined by the *minimum free space* that must be left on each disk.

IMPORTANT: You must make sure that the service user running the Archiver or Auxiliary Archiver role has write access to all the archive root folders that are assigned to the role.

Archive storage requirements

Because the Archiver role and Auxiliary Archiver role can control a different number of cameras, you must evaluate the storage requirements for each of these roles separately.

The storage requirements are affected by the following factors:

- The number of cameras that need archiving.
- The number of days you need to keep the archive online.
- The percentage of recording time. The percentage of recording time depends on the selected archiving mode. You can configure your recordings for specific times during the day, and the archiving mode can be continuous, triggered by motion and user request, only upon user request, or off. Continuous recording consumes disk space faster than each of the other archiving modes.
- Frame rate. The higher the frame rate, the more storage space the recording needs.
- Image resolution. The higher the image resolution, the more storage space the recording needs. The image resolution is determined by the video data format that is being used.
- The expected percentage of movement. Instead of storing the whole image for every single frame, most video encoding schemes compress data by storing only the image changes between consecutive frames. As a result, recording a scene with plenty of movement requires more storage than recording a scene with little movement.
- Audio and metadata recordings. Audio and metadata, if recorded, can also add to the amount of storage required.

TIP: Checking the disk usage statistics regularly is the best way to estimate future storage requirements, and it also allows you to make adjustments quickly.

Related Topics
Camera - Video tab on page 803
Freeing up storage space for video files on page 438
Configuring the recording settings of cameras on page 379
Monitoring disk space available for video files on page 436

Protecting video archives

Since the video archives are the most important part of your video surveillance system, you must protect them.

To protect your video archives:

1. Check your archive storage requirements to make sure you have a disk with enough room to store your footage.
2. If one disk is not enough, then create multiple disk groups to store the archives.
3. Make sure your camera recording settings are correct.

   If your cameras are recording continuously, your disk space is filled up faster.
4. Regularly monitor how much disk space you have left.
5. Free up disk space by deleting older video files, setting retention periods for cameras, and so on.
6. Regularly backup your archive database.
7. Regularly backup your video archives.
8. Set up Archiver failover in case the server hosting the Archiver role goes offline.
9. Protect important video files from being deleted.
10. Protect important video files from being tampered with by adding watermarks.

Related Topics

About video archives on page 432

Distributing archive storage over multiple disks

To avoid a bottleneck on the Archiver or Auxiliary Archiver due to disk throughput, you can enable the role to write simultaneously to multiple disks.

What you should know

The Archiver and Auxiliary Archiver roles can write to multiple disks by spreading the video archive over several *disk groups*. Each disk group must correspond to a separate disk controller. By splitting the video archive from different cameras over different disk groups, you can effectively attain the maximum throughput in terms of disk access.

CAUTION: There is nothing that prevents other applications from using up the disk space set aside for the Archiver or Auxiliary Archiver. For this reason, it is recommended that you assign a disk that is not shared with other applications to this role. In the case where multiple Archivers share the same server, use a separate disk for each.

To distribute the archiving cameras over multiple disk groups:

1. From the Config Tool home page, open the *Video* task.
2. Select the Archiver role, and click the **Resources** tab.
3. To create a new disk group, click **Add group** ().
4. In the **Disk group** column, click the **New disk group**, and type a name for the group.
5. Click **Camera distribution** (⚖).
6. In the **Camera distribution dialog** box, divide the cameras between the disk groups by selecting them one at a time and moving them with the arrow buttons.
7. Click **Close** > **Apply**.

Monitoring disk space available for video files

Given the importance of your video archives, you should regularly monitor how much disk space you have left, so archiving does not suddenly stop.

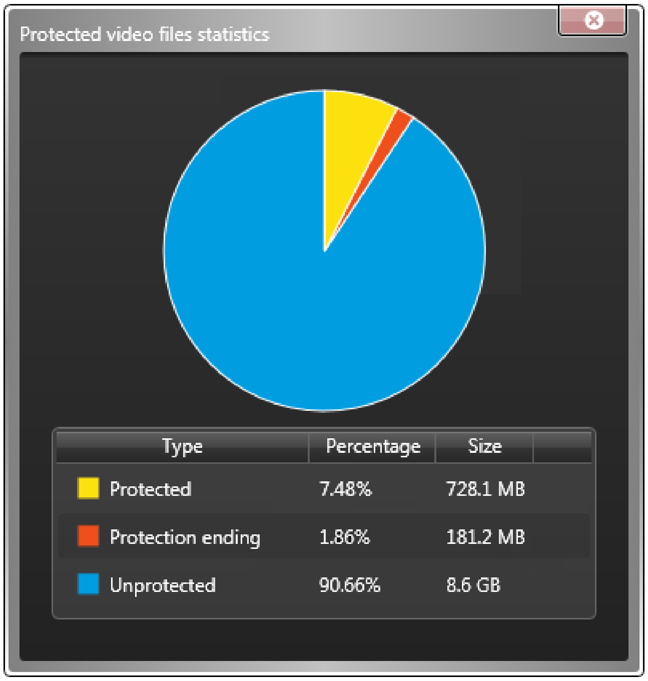
What you should know

Too many protected *video files* on a disk can take away valuable storage space for new video files. When regularly checking your disk space, you should also check the percentage of protected video files on each disk.

You can also create an *event-to-action* to alert you when an Archiver or Auxiliary Archiver is running out of disk space, or has stopped archiving.

To monitor the disk space available for video files:

1. Open the **Video** task, and select the Archiver or Auxiliary Archiver role.
2. Click the **Resources** tab, and then click **Statistics** (●).
3. In the **Statistics** dialog box, check the following statistics:
   - **Available Space:** Disk space available for video archives.
   - **Average disk usage:** Average space used per day (first line) and average space used per camera per day (second line).
   - **Estimated remaining recording time:** Number of days, hours, and minutes of recording time left based on the average disk usage and the current load.
   - **Active cameras:** Number of cameras that are currently active.
   - **Archiving cameras:** Number of cameras for which archiving is enabled.
4. Select a disk group, and click Protected video file statistics (●).



Protected video files statistics

Type	Percentage	Size
🟨 Protected	7.48%	728.1 MB
🟧 Protection ending	1.86%	181.2 MB
🟦 Unprotected	90.66%	8.6 GB

The pie chart indicates the status of video files on the disk, as follows:

- **Protected:** Percentage of video files on the disk that are currently protected.

- **Protection ending:** Percentage of video files on the disk that a user has decided to unprotect. When a user decides to manually remove the protection on a video file, the Archiver waits 24 hours before actually removing the protection, giving the user enough time to change their mind if necessary. During this time, the status indicates *Protection ending*.
- **Unprotected:** Percentage of video files on the disk that are not protected.

After you finish

If the disk is getting full, consider reviewing the video archives to see if there are any that you can delete. Also, you can configure the Archiver settings to free up as much disk space as possible.

Freeing up storage space for video files

Within each disk group, you can free up storage space to make room for new video files.

What you should know

The following are different ways to free up storage space for video files:

- Delete the oldest video files when the disk space starts to run out. This is recommended if most of your video footage is equally important, and you want to keep as much footage as possible. This maximizes disk usage.
- Set up archiving retention periods for cameras (number of days the recorded footage must be kept online). When the retention period expires, the video is automatically deleted. This allows you to keep more important video footage for a longer period of time.
- Limit the size and length of video files.
- Limit the amount of space that protected video files are allowed to occupy on disks, since they are not deleted during normal cleanup procedures.

NOTE: If you do not instruct the Archiver to delete any video files, archiving is stopped when disk space runs out.

To free up storage space for video files:

1. Open the **Video** task, and select the Archiver or Auxiliary Archiver to configure.
2. Click the **Resources** tab, and click **Advanced settings**.
3. Switch the **Delete oldest video files when disks are full** option to **ON**.
4. In the **Protect video threshold** option, set a maximum percentage of space that protected video files can occupy on the disks.

   When this threshold is exceeded, the Archiver generates a *Protected video threshold exceeded* event once every 15 minutes, so you can review the video files and delete the ones that are no longer needed. The Archiver does not delete the protected files itself.

5. In the **Video files** section, set a **Maximum length** for video sequences, in minutes.
6. In the **Maximum size** option, select **Specific**, and set a maximum size for the video files, in gigabytes.
7. Click **OK** > **Apply**.
8. To set a retention period for the video footage of all cameras recorded by the role, do one of the following:
   - For an Archiver role, click the **Camera default settings** tab.
   - For an Auxiliary Archiver role, click the **Camera recording** tab.
9. In the **Automatic cleanup** option, set a number of days, and click **Apply**.
10. To set a retention period for a specific camera managed by this role, expand the role entity tree, and select the camera.

    This is helpful for cameras that have more important video footage.

    TIP: You might want to set a shorter retention period for PTZ cameras, because PTZ cameras often use more storage due to the increased movement.

11. Click the **Recording** tab.
12. In the **Automatic cleanup** option, set a number of days, and click **Apply**.

Archive transfer

Archive transfer is the process of transferring your video data from one location to another. The video is recorded and stored on the video unit itself or on an Archiver storage disk, and then the recordings are transferred to another location.

With archive transfer, you can do the following:

- Retrieve video archives from edge recording units to their main Archiver
- Duplicate video archives from one Archiver on another Archiver
- Backup video archives from an Archiver to a G64x file
- Restore video archives from a G64x file to an Archiver

Archive transfers can be performed manually or on a schedule. You can configure the same transfer settings for multiple cameras or Archivers by creating a *Transfer group*.

NOTE: Only system administrators can configure archive transfer settings.

Within the same transfer group, only video sequences that occurred after the last video time frame that was transferred are backed up.

Example: If the last frame retrieved for a unit is ‘7/30/2014 3:44:40' and you try to retrieve video between 3:40:00 and 3:50:00, only video between 3:44:40 and 3:50:00 is retrieved and stored in the Archiver.

When you perform an archive transfer, the following information is preserved in the copy:

- Audio and metadata
- Video watermarks
- Camera blocking settings
- Protection settings

When video is restored to an Archiver, it acquires the retention period of that Archiver.

Limitations of archive transfer

Only original files can be backed up. For example, archives can only be duplicated from the Archiver where the video was originally recorded.

Archive transfer troubleshooting

If your Archiver goes offline during an archive transfer and the process is stopped, the transfer must be restarted after the Archiver reconnects.

- If you were performing a manual archive transfer, then you must restart the process manually.
- If the archive transfer was set to run on a schedule, then the transfer restarts at the next scheduled time.

NOTE: The archive transfer restarts at the last successfully transferred frame.

Retrieving video archives from units

To store video archives on your video units using edge recording and then periodically retrieve those archives in Security Center, you must enable edge recording on the unit and then configure the cameras to transfer video to their main Archiver using archive transfer.

Before you begin

You must determine whether or not the video unit is capable of edge recording and supports archive transfer. To find out which edge devices are currently supported, contact Genetec™ Technical Assistance.

What you should know

You can configure the archives to be retrieved automatically when the unit connects to the Archiver.

You can continue to record video on the Archiver, even if the camera is configured for archive transfer. Cameras can only be added to one transfer group for retrieving archives from units.

To retrieve video archives from units:

1 Enable edge recording on the video unit.
2 Select which cameras will transfer video archives to the Archiver, and define the transfer settings.
3 To retrieve archives from the video unit apart from the scheduled transfer time, then transfer the video manually.

Example

Archive transfer from units to Archivers is helpful in the following scenarios:

- For remote sites connected to a central site with limited bandwidth: Typically, a server is deployed at the remote site to host the recording. However, with archive transfer you can simply retrieve the video directly from the cameras on demand without requiring a server.
- For city wide surveillance using edge recording cameras: Cameras are always recording. Recordings are only retrieved on demand for investigation purposes, or outside of peak hours.
- If there is a network failure, the portions of video that are missing from the Archiver recordings can be retrieved from the video unit.

Related Topics
Archive transfer on page 439
Duplicating archives on another Archiver on page 443

Enabling edge recording on video units

Before you can transfer video from video units to an Archiver, you must enable edge recording on the video units.

What you should know

You can set the recording on the device to be continuous, or triggered by specific events (inputs, motion, analytics, and so on). Edge recording can only be enabled from the unit's web page.

NOTE: Bosch units support edge recording on a separate device from the video units. For information about enabling edge recording on Bosch units, see the *Security Center Video Unit Configuration Guide*.

To enable edge recording on a video unit:

1. Open the **Video** task.
2. Select the video unit to configure, and click **Unit** > **Unit's web page** (🌐) in the toolbar at the bottom of the workspace.
3. In the web browser window that appears, follow the instructions from the unit's manufacturer to enable recording on that unit.
4. Close the web browser window when you are done.

Configuring video transfer settings for cameras

To retrieve video archives that were recorded on the video units in Security Center, you must configure the video transfer settings for those cameras, such as what type of video data you want to download, and when.

Before you begin

Enable edge recording on all cameras selected for archive transfer.

To configure video transfer settings for cameras:

1. In the Config Tool home page, open the *Archive transfer* task.
2. Click **Add an item** (➕) > **Retrieve from edge**.
3. In the **Transfer group properties** dialog box, type a name for this archive transfer scenario.
4. In the **Sources** section, click **Add an item** (➕), select the cameras you want, and then click **Add**.

   TIP: Hold **CTRL** or **SHIFT** to select multiple cameras.

5. In the **Recurrence** option, set a schedule for the archive transfer:

   Transferring archives on a schedule is recommended for fixed cameras with limited network bandwidth. The transfer can be scheduled for a time when the network demand is the lowest.

   - **Manual:** Transfer archives manually only.
   - **Minutes:** Transfer archives every x number of minutes.
   - **Hourly:** Transfer archives every x number of hours.
   - **Daily:** Transfer archives once a day, for a set duration of time (optional).
   - **Weekly:** Transfer archives on specific days during the week, for a set duration of time (optional).

   If you set a duration for the *Daily* or *Weekly* schedule, then the transfer stops at the end of the set duration, and the next transfer starts from the last successfully transferred video frame. If you do not set a duration and the transfer is still in progress at the beginning of the next scheduled transfer, then the new transfer starts as soon as the current transfer is completed.

6. To retrieve archives upon connection to the network, set the **Upon reconnection** option to ON, and specify how many seconds the Archiver will wait to determine if a unit is online before transferring the video.

   This option is recommended for cameras connected to mobile units that regularly move in and out of Wi-Fi coverage. It is also helpful if you have an unstable network where your cameras frequently go on and offline.

7. In the **Data** option, select whether to transfer everything since the last successful transfer or specific sequences based on event filters.
8. If you select **Specific**, then select the different types of data to transfer:

   - **All archives when the camera was offline:** Transfer video segments that span between a *Unit lost* and a *Unit discovered* event.
   - **Alarms:** Transfer video segments related to alarm events. The record of the alarm itself is not transferred.

- **Video analytics events:** Transfer video segments that contain video analytics events.
- **Motion events:** Transfer video segments that span between a *Motion on* and *Motion off* event. This option only applies to unit motion detection.
- **Bookmarks:** Transfer video segments that contain bookmarks.
- **Input triggers:** Transfer video segments that contain input events.
- **Time range:** Transfer video segments recorded during a specific period of time. You can specify a specific time range or a relative time range (last *n* days, hours, minutes).

9 (Event-based transfer only) If you selected specific data, specify how many seconds of video should be transferred before and after the event occurs.

Example: If you select the **Motion events** filter, this setting indicates how many seconds of video are transferred before the *Motion on* event occurred, and how many seconds are transferred after the *Motion off* event occurred.

10 Click **Save**.

Duplicating archives on another Archiver

If you want to periodically duplicate video archives from one Archiver on another Archiver, you must configure the transfer settings to the second Archiver, such as what types of video data you want to transfer, and when.

What you should know

When you duplicate video from an Archiver on another Archiver, the archives are also kept on the storage disk of the original Archiver until the retention period ends.

To duplicate archives on another Archiver:

1. From the Config Tool home page, open the **Video** task, and select the Archiver you want to configure.
2. Click the **Resources** tab, and then click **Advanced** settings.
3. In the **Max archive transfer throughput** option, set the maximum bandwidth available to the Archiver for archive transfer.

   This setting is useful to ensure that network bandwidth is available for live video and playback requests.
4. In the Config Tool home page, open the *Archive transfer* task.
5. Click **Add an item** (✚) > **Duplicate archives**.
6. In the **Transfer group properties** dialog box, provide a name for this archive transfer scenario.
7. In the **Sources** section, click **Add an item** (✚), select the cameras or Archivers you want, and then click **Add**.

   If you select cameras as your source, video that was recorded from those cameras on all Archivers are transferred.

   TIP: Hold **CTRL** or **SHIFT** to select multiple cameras or Archivers.
8. From the **Destination** drop-down list, select the Archiver you want to transfer the video to.
9. In the **Recurrence** option, set a schedule for the archive transfer:

   Transferring archives on a schedule is recommended for fixed cameras with limited network bandwidth. The transfer can be scheduled for a time when the network demand is the lowest.

   - **Manual:** Transfer archives manually only.
   - **Minutes:** Transfer archives every x number of minutes.
   - **Hourly:** Transfer archives every x number of hours.
   - **Daily:** Transfer archives once a day, for a set duration of time (optional).
   - **Weekly:** Transfer archives on specific days during the week, for a set duration of time (optional).

   If you set a duration for the *Daily* or *Weekly* schedule, then the transfer stops at the end of the set duration, and the next transfer starts from the last successfully transferred video frame. If you do not set a duration and the transfer is still in progress at the beginning of the next scheduled transfer, then the new transfer starts as soon as the current transfer is completed.
10. In the **Coverage** option, select whether to transfer all the data that has been accumulated since the last transfer, or only for a set range of days.
11. In the **Data** option, select whether to transfer everything that has been accumulated since the last successful transfer, or specific sequences based on event filters.
12. If you select **Specific**, then select the type of data to transfer:
    - **Alarms:** Transfer video segments related to alarm events. The record of the alarm itself is not transferred.
    - **Video analytics events:** Transfer video segments that contain video analytics events.

- **Motion events:** Transfer video segments that span between a *Motion on* and *Motion off* event. This option only applies to unit motion detection.
- **Bookmarks:** Transfer video segments that contain bookmarks.
- **Input triggers:** Transfer video segments that contain input events.
- **Time range:** Transfer video segments recorded during a specific period of time. You can specify a specific time range or a relative time range (last n days, hours, minutes).

13 (Event-based transfer only) If you selected specific data, specify how many seconds of video should be transferred before and after the event occurs.

Example: If you select the **Motion events** filter, this setting indicates how many seconds of video are transferred before the *Motion on* event occurred, and how many seconds are transferred after the *Motion off* event occurred.

14 Click **Save**.

Example

Archive transfer between Archivers is helpful in the following scenarios:

- For multi-tiered storage solutions: High quality video is recorded in real-time on the first Archiver, which uses a high performance, costly storage device. Periodically, you duplicate the important video on the second Archiver, which uses a slower device but is better for long-term storage.
- If you moved video units to a new Archiver using the Move unit tool and you also want to transfer the video archives from those cameras to the new Archiver.
- Transferring video recordings from a federated site to a central system for long-term storage, local investigations, and to manage bandwidth.

Related Topics
Archive transfer on page 439
Retrieving video archives from units on page 440

Backing up video archives on a schedule

To save important video on a regular basis, you can back up specific archives to a file server or a network drive on a schedule using archive transfer.

What you should know

The video is saved to a G64x backup file, which can be restored at a later time. Backed up archive files are not searchable in Security Desk unless they are restored; however, the original video is still searchable.

You can also backup video archives manually if you need the backup to be done right away.

To back up video archives on a schedule:

1. From the Config Tool home page, open the *Video* task.
2. Select the Archiver to configure, and click the **Resources** tab.
3. In the **Archive transfer** section, set the following options:
   - **Backup folder:** Location where the backed up archives saved as a G64x file.
   - **Delete oldest files when disks are full:** Turn this option on to delete the oldest video archives when the disk is full.
   - **Automatic cleanup:** Turn this option on to specify a retention period for the backed up video archives (in days). If you do not enable this option, the backed up video archives are not deleted by the system, and you must manually delete them.
4. Click **Advanced settings**.
5. In the **Max archive transfer throughout** option, set the maximum bandwidth available to the Archiver for archive transfer.
6. Click **OK** > **Apply**.
7. In the Config Tool home page, open the *Archive transfer* task.
8. Click **Add an item** (➕) > **Backup**.
9. In the **Transfer group properties** dialog box, type a name for this archive transfer scenario.
10. In the **Sources** section, click **Add an item** (➕), select the cameras or Archivers you want, and then click **Add**.

    If you select cameras as your source, video that was recorded from those cameras on all Archivers are transferred.

    TIP: Hold **CTRL** or **SHIFT** to select multiple cameras or Archivers.
11. In the **Recurrence** option, set a schedule for the archive transfer:

    Transferring archives on a schedule is recommended for fixed cameras with limited network bandwidth. The transfer can be scheduled for a time when the network demand is the lowest.
    - **Manual:** Transfer archives manually only.
    - **Minutes:** Transfer archives every x number of minutes.
    - **Hourly:** Transfer archives every x number of hours.
    - **Daily:** Transfer archives once a day, for a set duration of time (optional).
    - **Weekly:** Transfer archives on specific days during the week, for a set duration of time (optional).

    If you set a duration for the *Daily* or *Weekly* schedule, then the transfer stops at the end of the set duration, and the next transfer starts from the last successfully transferred video frame. If you do not set a duration and the transfer is still in progress at the beginning of the next scheduled transfer, then the new transfer starts as soon as the current transfer is completed.
12. In the **Coverage** option, select whether to transfer all the data that has been accumulated since the last transfer, or only for a set range of days.

13 In the **Data** option, select whether to transfer everything since the last successful transfer or specific sequences based on event filters.

14 If you select **Specific**, then select the type of data to transfer:

- **Alarms:** Transfer video segments related to alarm events. The record of the alarm itself is not transferred.
- **Video analytics events:** Transfer video segments that contain video analytics events.
- **Motion events:** Transfer video segments that span between a *Motion on* and *Motion off* event. This option only applies to unit motion detection.
- **Bookmarks:** Transfer video segments that contain bookmarks.
- **Input triggers:** Transfer video segments that contain input events.
- **Time range:** Transfer video segments recorded during a specific period of time. You can specify a specific time range or a relative time range (last n days, hours, minutes).

15 (Event-based transfer only) If you selected specific data, specify how many seconds of video should be transferred before and after the event occurs.

Example: If you select the **Motion events** filter, this setting indicates how many seconds of video are transferred before the *Motion on* event occurred, and how many seconds are transferred after the *Motion off* event occurred.

16 Click **Save**.

The video archives are backed up at the scheduled time.

Example

Backing up your video archives is helpful in the following scenarios:

- If you are performing maintenance on the server and need to temporarily store the archives in a secure location.
- If your Archiver fails and you need to restore the video to another Archiver.
- For multi-tiered storage solutions, if you have an Archiver that is dedicated to managing backups of several Archiver databases. High quality video is recorded in real-time on the first Archiver, which uses a highperformance, costly storage device. Periodically, you back up the important video on the second Archiver, which uses a slower device but is better for long-term storage.

Related Topics

Archive transfer on page 439
Restoring video archives on page 447
Transferring video archives manually on page 448

Restoring video archives

If you are done performing maintenance on a server that is hosting an Archiver or if you have a new Archiver, you can restore video archives that were backed up to a disk.

What you should know

By default, the restore process looks for archives in the default backup folder of the Archivers, which is specified in their **Resources** tab when you back up video archives on a schedule. However, you can also select a backup G64x file from a different folder.

You can only restore archives to an Archiver known to your Security Center system.

Only the types of video data that were backed up are restored. Once you restore the archives, the video is searchable using Security Desk reports.

To restore video archives:

1. In the Config Tool home page, open the *Archive transfer* task.
2. At the bottom of the window, click **Restore archives**.
3. In the **Restore type** option, select what you want to restore:
   - **Camera:** Restore video from specific cameras that was recorded and stored in the Archiver database, and then backed up to the default backup folder. If you select **Camera**, then select which cameras to restore video for.
   - **Archiver:** Restore video from specific Archivers that was backed up to the default backup folder. If you select **Archiver**, then select which Archivers to restore video for.
   - **Custom:** Restore video from a backup file that is not in the default location (for example, a USB storage device or a different folder). If you select **Custom**, then select which Archiver to restore the video to and the backup file to load from.
4. In the **When** section, select the time range for the search.
5. Click **Find archives**.
6. Select the archives you want to restore.

   TIP:

   Hold **CTRL** or **SHIFT** to select multiple cameras or Archivers.
7. To protect the archives from being deleted by the system when its retention period has ended, turn on the **Protect archive from deletion option**.

   BEST PRACTICE: If you are restoring old video sequences, it is best practice to protect your video files from being deleted.
8. Select how long to protect the archives for, from one of the following options:
   - **Indefinitely:** No end date. You must remove the protection status manually.
   - **For x days:** The video file is protected for the number of days that you select.
   - **Until:** The video file is protected until the date that you select.
9. Click **Restore**.

Related Topics

Backing up video archives on a schedule on page 445

Transferring video archives manually

To safeguard your video archives before a major operation such as a software upgrade or the replacement of a server, you can transfer specific archives manually without creating a *transfer group*.

What you should know

For recurrent video archive transfers, you can transfer the video archives on a schedule.

To transfer video archives manually:

1. In the Config Tool home page, open the *Archive transfer* task.
2. At the bottom of the window, click **Transfer now**.
3. In the **Transfer group properties** dialog box, select the type of transfer you want to perform:
   - **Backup:** Backup video archives from an Archiver to a G64x file.
   - **Duplicate archives:** Duplicate video archives from one Archiver on another Archiver.
4. In the **Sources** section, click **Add an item** (✚), select the cameras or Archivers you want, and then click **Add**.

   If you select cameras as your source, video that was recorded from those cameras on all Archivers are transferred.

   TIP: Hold **CTRL** or **SHIFT** to select multiple cameras or Archivers.
5. If you selected **Duplicate archives**, then select from the **Destination** drop-down list the Archiver to which you want to transfer the video.
6. In the **Time range** option, select the start and end date and time of the video archives you want to transfer.
7. In the **Data** option, select whether to transfer everything since the last successful transfer or specific sequences based on event filters.
8. If you select **Specific**, then select the type of data to transfer:
   - **Alarms:** Transfer video segments related to alarm events. The record of the alarm itself is not transferred.
   - **Video analytics events:** Transfer video segments that contain video analytics events.
   - **Motion events:** Transfer video segments that span between a *Motion on* and *Motion off* event. This option only applies to unit motion detection.
   - **Bookmarks:** Transfer video segments that contain bookmarks.
   - **Input triggers:** Transfer video segments that contain input events.
   - **Time range:** Transfer video segments recorded during a specific period of time. You can specify a specific time range or a relative time range (last n days, hours, minutes).
9. (Event-based transfer only) If you selected specific data, specify how many seconds of video should be transferred before and after the event occurs.

   Example: If you select the **Motion events** filter, this setting indicates how many seconds of video are transferred before the *Motion on* event occurred, and how many seconds are transferred after the *Motion off* event occurred.
10. Click **Start**.

    The video archives are transferred immediately.

Related Topics

Archive transfer on page 439

Backing up video archives on a schedule on page 445

Bypassing archive transfer schedules

If you need to retrieve the video recordings from a video unit, copy archives to another Archiver, or backup your video archives right away rather than waiting until the next scheduled transfer, you can execute an archive transfer manually.

Before you begin

The archive transfer settings for the transfer group must be configured.

To bypass an archive transfer schedule:

1. In the Config Tool home page, open the *Archive transfer* task.
2. Select one or more of the transfer groups in the list.

   TIP:

   Hold **CTRL** or **SHIFT** to select multiple cameras or Archivers.
3. Click **Start transfer for selected transfer groups (**▶).

Archive transfer status and details

You can monitor and review the status of your archive transfers in the Archive transfer task.

The following information is provided for each transfer group:

- **Transfer group:** Group of cameras or Archivers with the same video transfer settings.
- **Type:** Video transfer type. Either *Retrieve from edge*, *Duplicate archives*, or *Backup*.
- **Recurrence:** How often the video transfer reoccurs, based on the defined schedule.
- **Status:** State of the current transfer. The status can be one of the following:
  - **Idle:** The transfer is waiting to start.
  - **Pending:** The transfer will start as soon as a spot opens in the download queue.
  - **Active:** The transfer has started. The progression and bit rate are shown.
  - **Error:** Some cameras could not be processed successfully, but others are still active.
  - **Success:** The transfer was successfully completed.
- **Transferred data size:** How much video data was transferred.
- **Last transfer start:** Date and time the last transfer was started.
- **Last transfer end:** Date and time the last transfer finished.
- **Last transfer status:** The status of the last transfer.
- **Next transfer:** Date and time when the next transfer is set to start.
- **Show transfer details (◔):** Transfer information about each camera in the transfer group.
  - **Source:** Name of the camera.
  - **To:** Destination of the transfer (an Archiver or the Archiver's backup folder).
  - **Status:** State of the transfer.
  - **Transferred data size:** Number of bytes that were transferred.
  - **Last transfer start:** Date and time the last transfer was started.
  - **Last transfer end:** Date and time the last transfer finished.
  - **Last transfer status:** The status of the last transfer.
  - **Result:** Displays errors about the transfer.

Protecting video files from being deleted

You can protect important video footage from being deleted by the system when the Archiver's disk space becomes full, or when its normal retention period has ended.

What you should know

The Archiver cannot protect partial files; therefore, you might protect a larger segment than the one you select.

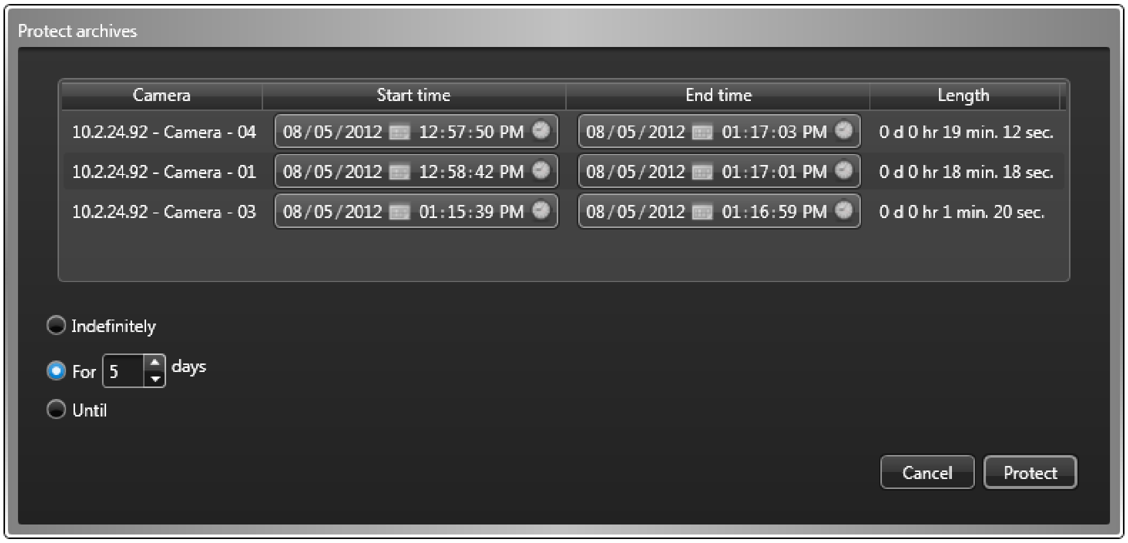
CAUTION: Too many protected video files on a disk can waste storage space for new video files. To avoid wasting storage space, regularly check the percentage of protected video files on each disk.

To protect a video file:

1. Open the **Archive storage details** task
2. Generate your report.

   The video files associated with the selected cameras are listed in the report pane.
3. From the report pane, select the video file to protect, and then click **Protect** (🔒).

   To select multiple video files, hold the **CTRL** or **SHIFT** keys.
4. In the **Start** and **End** columns in the *Protect archives* dialog box, set the time range of the video file to protect.



Protect archives

Camera	Start time	End time	Length
10.2.24.92 - Camera - 04	08/05/2012 12:57:50 PM	08/05/2012 01:17:03 PM	0 d 0 hr 19 min. 12 sec.
10.2.24.92 - Camera - 01	08/05/2012 12:58:42 PM	08/05/2012 01:17:01 PM	0 d 0 hr 18 min. 18 sec.
10.2.24.92 - Camera - 03	08/05/2012 01:15:39 PM	08/05/2012 01:16:59 PM	0 d 0 hr 1 min. 20 sec.

○ Indefinitely

● For 5 days

○ Until

5. Select how long to protect the video file for, from one of the following options:
   - **Indefinitely:** No end date. You must remove the protection status manually by selecting the video file in the report pane, and then clicking **Unprotect** (🔓).

     NOTE: When you unprotect a video file, it is not immediately deleted. You have 24 hours to change your mind.
   - **For x days:** The video file is protected for the number of days that you select.
   - **Until:** The video file is protected until the date that you select.
6. Click **Protect**.

The video file is protected.

Related Topics

Archive storage on page 432

Protecting video files against tampering

If you want to use your video evidence in court, you can enable video watermarking on the Archiver, to protect the video against tampering and prove that it was not altered.

What you should know

Video watermarking is the process by which a digital signature (watermark) is added to each recorded video frame to ensure its authenticity. If anyone later tries to make changes to the video (add, delete or modify a frame), the signatures will no longer match, which shows that the video has been tampered with.

To protect your video files against tampering:

1. Open the **System** task, and click the **Role view**.
2. Select the Archiver role, click the **Resources** tab, and click **Advanced settings**.
3. Switch the **Video watermarking** option to **ON**, and click **OK** > **Apply**.
4. Set up an encryption key for the watermarking fingerprint..

Setting up an encryption key for video files

You can generate your own encryption key and set the Archiver to use it for the watermark fingerprint.

To set up an encryption key for video files:

1. Run the program called *EncryptionKeyGenerator.exe* found in the Security Center Server installation folder.

   The program will generate two 1 kB files named *fingerprint.bin* and *private.bin*. The first file contains a random 20 Byte initial fingerprint used for the encryption. The second file contains an RSA 248-bit encryption key. These two files will be different every time the program is executed.
2. Keep a copy of these files in a safe place.
3. Place another copy of these files in the Security Center Server installation folder.
4. In Config Tool, open the **System** task, and click the **Role view**.
5. Select the Archiver role, and restart the role.
6. If you have a secondary server assigned to the Archiver role, copy the same custom encryption files into the Security Center Server installation folder on that server.

The next time the Archiver records video to disk, the video files are watermarked, and the fingerprint is encrypted using the new encryption key.

Viewing the properties of video files

You can find the *video files* used to store *video archives* from cameras, and view the properties of the video files (file name, start and end time, file size, protection status, and so on), using the *Archive storage details* report. You can also change the protection status of the video files.

To view the properties of a video file:

1. From the home page, open the **Archive storage details** task.
2. Set up the query filters for the report. Choose from one or more of the following filters:
   - **Cameras:** Select the camera to investigate.
   - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
   - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the last week or the last month.
   - **Media type:**

     Select the type of media your are looking for:

     - **Video:** Files that contain video recordings.
     - **Audio:** Files that contain audio recordings.
     - **Metadata:** Files that contain metadata, such as overlays.
   - **Origin type:**

     Refine your search by selecting the origin of the files:

     - **Downloaded from the unit's internal storage:** Files created by the camera, downloaded from it by an Archiver, and currently stored on the Archiver's disk.
     - **Duplicated from another Archiver:** Files created by an Archiver and transferred to another one.
     - **On the unit's internal storage:** Files created by the camera and currently stored on it.
     - **Recorded by the Archiver:** Files created and currently stored by an Archiver.
     - **Restored from a backup:** Files restored from an offline backup set; that is, a backup file containing archives that were not accessible from Security Center prior to restoring them.
   - **Source:** The name of the system the camera belongs to.
   - **Status:**

     Select the video file status you want to investigate:

     - **Unprotected:** Video files that are not protected against the Archiver’s routine cleanup. These files can be deleted once their retention period expires, or when the Archiver runs out of disk space, depending on your Archiver role settings.
     - **Protection ending:** Video files that you unprotected less than 24 hours ago.
     - **Protected:** Video files that are protected. They are not deleted even when the disk is full. For these files, you can also specify a protection end date.
3. Click **Generate report**.

   The video files associated with the selected cameras are listed in the report pane, along with their file properties.
4. To view a video sequence in a tile, double-click or drag a video file from the report pane to the canvas.

   The selected sequence immediately starts playing.

After you finish

- To export a video archive, select the item in the report pane, and then click **Export video** (💿).
- To remove a video file from the database, select the item in the report pane, and then click **Delete** (✗).
- To protect a video archive from automatic deletion, select the item in the report pane, and then click **Protect** (🔒).

Related Topics
Protecting video files from being deleted on page 451

Report pane columns for the Archive storage details task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Camera:** Camera name.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Drive:** The drive on the server where the Archiver role is running.
- **End time:** End of the time range, playback sequence, or video sequence.
- **File name:** Name of the video file.
- **File size:** Size of the video file.
- **Length:** Length of the video sequence contained in the video file, in hours, minutes, and seconds.
- **Media type:** Type of media (video, audio, metadata) contained in the file.
- **Origin type:**

  The origin of the file:

  - **Downloaded from the unit's internal storage:** Files created by the camera, downloaded from it by an Archiver, and currently stored on the Archiver's disk.
  - **Duplicated from another Archiver:** Files created by an Archiver and transferred to another one.
  - **On the unit's internal storage:** Files created by the camera and currently stored on it.
  - **Recorded by the Archiver:** Files created and currently stored by an Archiver.
  - **Restored from a backup:** Files restored from an offline backup set; that is, a backup file containing archives that were not accessible from Security Center prior to restoring them.
- **Protection status:** Protection status of the video file.
- **Server:** Name of the server where the Archiver role is running.
- **Source (entity):** The name of the system the camera belongs to.
- **Start time:** Beginning of the time range, playback sequence, or video sequence.

Effects of Daylight Saving Time on video archives

Time changes that occur every year, to or from Daylight Saving Time (DST), can affect the way video archives are viewed and queried in Security Center.

Time changes do not prevent recording of video data from your cameras. The *Archiver* always records using the Coordinated Universal Time (UTC), which never changes according to the seasons, and archives queries are always transmitted to the server using UTC timestamps. This isolates the archives from the effects of time changes. However, because Security Desk and Config Tool can be configured to use (and display) a time zone other than UTC, and for which DST may apply, different behaviors can be observed whether the time is adjusted backward or forward.

NOTE: The Eastern Standard Time (EST) time zone is used as an example, however this applies to all time zones that are also subjected to DST.

Effects of time adjusted backward

When time is adjusted backward, it changes from DST to EST.

Before 2:00 AM, Security Center uses the DST (UTC-4), while starting from 2:00 AM, it uses the EST (UTC-5), as illustrated below.

	DST		Time change	EST	
Local time	12:00 AM	1:00 AM	2:00 AM = 1:00 AM	2:00 AM	3:00 AM
Offset (hours)	-4	-4	-5	-5	-5
UTC	4:00 AM	5:00 AM	6:00 AM	7:00 AM	8:00 AM

Due to the time being adjusted backward, the following behaviors can be observed when playing back or exporting archives:

- The time jumps back by one hour in the timeline. At 1:59:59 AM, the time displayed returns to 1:00:00 AM.
- The end time of a video sequence can be earlier than the start time.
- Exporting archives between 1:00 AM and 2:00 AM always include an additional hour of video. For example, when exporting archives from 1:50 AM to 2:00 AM, the exported sequence will include 1 hour and 10 minutes of video instead of the 10 minutes expected, because the query is made from 5:50 AM to 7:00 AM UTC.

If you do not want to see the time jumping back by one hour during video playback, or if you want to export video without the additional one-hour period, you must configure Security Desk to use UTC. After the sequence is exported, you can revert to the previous time zone to view the sequence relatively to your local time reference.

Effects of time adjusted forward

When time is adjusted forward, it changes from EST to DST.

Before 2:00 AM, Security Center uses the EST (UTC-5), while starting from 2:00 AM, it uses the DST (UTC-4), as illustrated below.

	EST		Time change	DST	
Local time	12:00 AM	1:00 AM	2:00 AM = 3:00 AM	4:00 AM	5:00 AM
Offset (hours)	-5	-5	-4	-4	-4
UTC	5:00 AM	6:00 AM	7:00 AM	8:00 AM	9:00 AM

Due to the time being adjusted forward, the following behaviors can be observed when playing back or exporting archives:

- The time jumps forward by one hour in the timeline. Instead of showing 2:00 AM, it shows 3:00 AM.
- There are no archives to export between 2:00 AM and 3:00 AM, because this period corresponds to 7:00 AM UTC.

If you do not want to see the time jumping forward by one hour during video playback, you must configure Security Desk to use UTC.

Changing the time zone to UTC

If you are viewing or querying archives that were recorded during a time change to or from Daylight Saving Time (DST), and you want to remove the impacts on the timeline, you can set the time zone to Coordinated Universal Time (UTC) in Security Desk prior to performing your task.

What you should know

Client applications (Security Desk, Config Tool) display time relatively to the selected time zone. For example, if you select *Eastern Time*, the client application will display all timestamps relatively to this time zone. However, because the server always uses UTC, the client application must convert the server's timestamps into the application's time zone.

NOTE: Time and date settings apply only to the client application you configure. Each application must be configured separately.

To change the time zone to UTC:

1. From the home page, click **Options** > **Date and time**.
2. If you want to show the time zone, select **Display time zone abbreviations**.

   The time zone is added next to the time displayed in the notification tray.
3. Click **Display time based on the following time zone**, and then select **(UTC) Coordinated Universal Time**.
4. Click **Save**.

The client application now displays current time and archive timestamps relatively to the UTC time zone.

Importing movie files to Security Center

To view MOV, AVI, and MP4 movie files in Security Center, you must import them using an offline camera.

Before you begin

You must configure the date on the device you are using to record your movie files. Failure to do so might prevent the movie files from being imported.

What you should know

The files you import must be named using the following format: *XXXX_YYYY.MM.DD_HH.MM.SS.AVI*. Whereby *XXXX* is the filename, and the other values represent the date and time.

To import a movie file:

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

2 Select the Archiver role to manage the unit.

3 Click (➕) **Video unit**.

The **Manual add** dialog box opens.

4 From the **Manufacturer** drop-down list, select **Offline device**.

5 Beside **Product type** drop-down list, select **Network share**.

6 Enter a **Unit Name**.

This is the default name for the camera, and will be used to generate a unique ID (GUID) for it.

7 Enter the **Path** for the folder where you will place the movie files you want to import.

The path can be a local path or a shared network path. The user must have read and write access to the shared network folder.

8 Ignore the **Authentication** setting.

9 Select the **Location**, and click **Add**.

10 Select the Archiver managing the new unit, and click the **Camera default settings** tab.

11 Make sure that the **Automatic cleanup** setting is higher than the oldest movie file you want to import.

For example, if your oldest movie file is thirty days old, set the **Automatic cleanup** option to at least 32 days so your oldest movie file does not get deleted right after it is imported.

IMPORTANT: The **Automatic cleanup** option is also used as the retention period for recorded video of all the cameras that are managed by the selected Archiver. Make sure that this does affect your camera recording settings.

12 Copy the movie files to the folder **Path** you created in step 7.

As the files are processed they will disappear from the folder. This may take up to thirty seconds or more depending on the number of files and their size.

NOTE:

- If a file does not disappear from the folder, the import failed.
- If you see a *FailedAudioImports* folder, then the video files were imported but the audio was not. You can find the original file in this folder.

After you finish

View your video file using the Archives report. For more information, see the *Security Desk User Guide*.

26

Troubleshooting video

This section includes the following topics:

Moving video units to a different Archiver

If you want a different Archiver role to manage and control a video unit, for load balancing or another purpose, you can move the unit to another Archiver using the *Move unit* tool.

Before you begin

- The Archiver role must be on the same LAN as the video unit it controls.
- If you are using custom settings for the unit manufacturer extension, such as custom logon credentials, you must configure the same extension settings on the new Archiver role.

What you should know

The video archives are not moved with the video unit to the new Archiver role. They remain under the old Archiver until their retention period ends.

To move a video unit to a different Archiver:

1. From the home page, click **Tools** > **Move unit**.
2. From the **Unit type** drop-down list, select **Video unit**.
3. Select the units you want to move.
4. Under **Archiver**, select the new Archiver role to control the unit.
5. Click **Move** > **Close**.

After you finish

If you have important video archives, you should move them over to the new Archiver at a non-crucial time.

Related Topics
Archiver: Extensions tab on page 859

Replacing video units

If a video unit fails and is offline in Security Center (red in the area view), you can replace the unit with a compatible one.

Before you begin

Make sure that the new video unit is the same brand and model as the old one, or you will receive the following error message: *Units' extension does not match*.

IMPORTANT: The configuration settings are not copied over during the replacement. You must copy over the configuration settings to the new video unit and all the cameras it controls before replacing the unit using the *Unit replacement* tool.

What you should know

This process copies the *video archives* and event logs associated with the old unit to the new one, so that the video archives are not lost.

To replace a video unit:

1 Add a new video unit to the Archiver controlling the old unit.

2 Copy the configuration settings of the old video unit to the new video unit, using the **Copy configuration tool**.

3 Copy the configuration settings of the cameras controlled by the old video unit to the new cameras, using the **Copy configuration tool**.

4 Click the home tab, and then click **Tools** > **Unit replacement tool**.

5 In the **Unit type** option, select **Cameras**.

6 Select the **Old** and the **New** cameras.

7 Click **Swap**.

   The video archives and event logs of the old video unit are copied to the new one.

8 Verify that the video archives are now associated with the new video unit, as follows:

   a) In Security Desk, open the **Archives** task.

   b) Select a camera that is controlled by the new video unit.

      All days that include video archives for the selected camera are listed in the **All available** tab.

   c) Click **Generate report**.

9 Once everything is verified, return to the Config Tool **Video** task.

10 In the area view, right-click the old unit, and click **Delete** (✖).

11 In the confirmation dialog box that opens, click **Continue**.

Upgrading video unit firmware

You can upgrade the firmware on your video unit directly from Config Tool.

Before you begin

- Download a supported firmware version for the unit from the Supported Devices List.
- Take note of the unit's configuration settings. For some manufacturers, the unit is reset to its default settings after the firmware upgrade.
- If Config Tool was installed with Basic Authentication turned OFF (default option), it is not possible to upgrade the firmware. Turn Basic Authentication ON before performing the upgrade.

What you should know

For some manufacturers, you cannot upgrade the unit's firmware from Config Tool. For manufacturer-specific information, see your manufacturer documentation.

To upgrade a video unit's firmware:

1 From the Config Tool home page, open the *Video* task.
2 Select the video unit to upgrade, and click the **Identity** tab.
3 Click **Upgrade** (☢).
4 In the file browser, select the firmware file that you downloaded from GTAP, and click **Open**.

The unit restarts.

After you finish

If the unit was reset to its default settings after the firmware upgrade, re-configure its settings.

Finding orphan files on your system

To find video files that are no longer referenced by your Archiver database, you can use the *VideoFileAnalyzer.exe* tool found in the Security Center installation folder.

What you should know

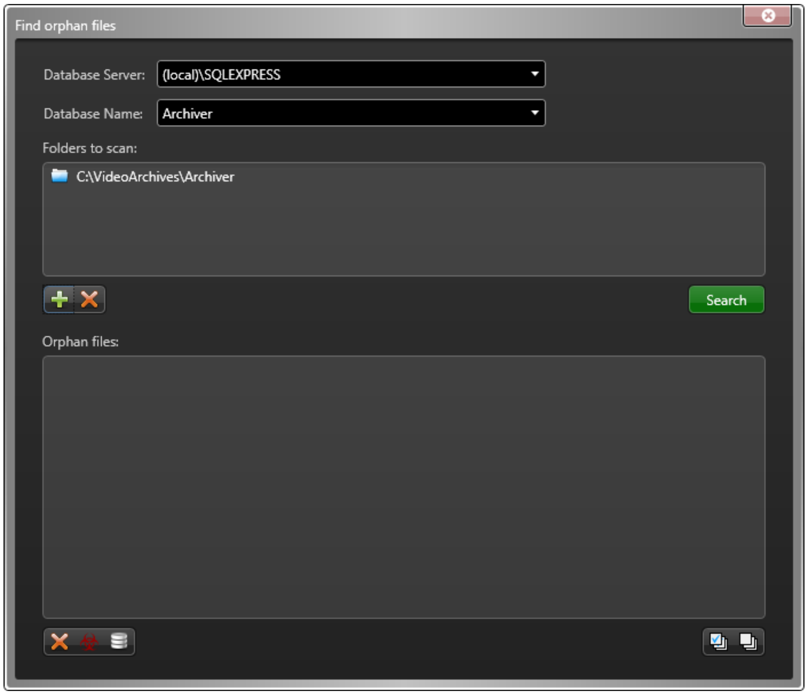
An *orphan file* is a video file that is no longer referenced by a designated Archiver database. Because the Archiver can only delete files that are referenced by its database, orphan files remain on the disk forever if they are not deleted manually. This situation can arise if the Archiver database is changed inadvertently, creating a mismatch between the number of video file entries in the database and the actual number of video files on disk. You can avoid this problem by performing a full archives backup before changing the database, and restoring the backup after changing the database.

To find orphan files on your system:

1. Open the *VideoFileAnalyzer.exe* tool.

   This tool is found in *C:\Program files (x86)\Genetec Security Center 5.5* on a 64-bit computer, and in *C:\Program files\Genetec Security Center 5.5* on a 32-bit computer.
2. At the bottom of the *Video File Analyzer* dialog box, click **Find orphan files**.
3. In the *Find orphan files* dialog box, specify which Archiver database you want to check the video files against.

   You can find the database server and database name in the *Resources* tab of the Archiver role in the Config Tool.
4. Under the *Folders to scan* section, click (➕) to add the folders you want to search through, and then click **OK**.



Find orphan files

Database Server: (local)\SQLEXPRESS

Database Name: Archiver

Folders to scan:

C:\VideoArchives\Archiver

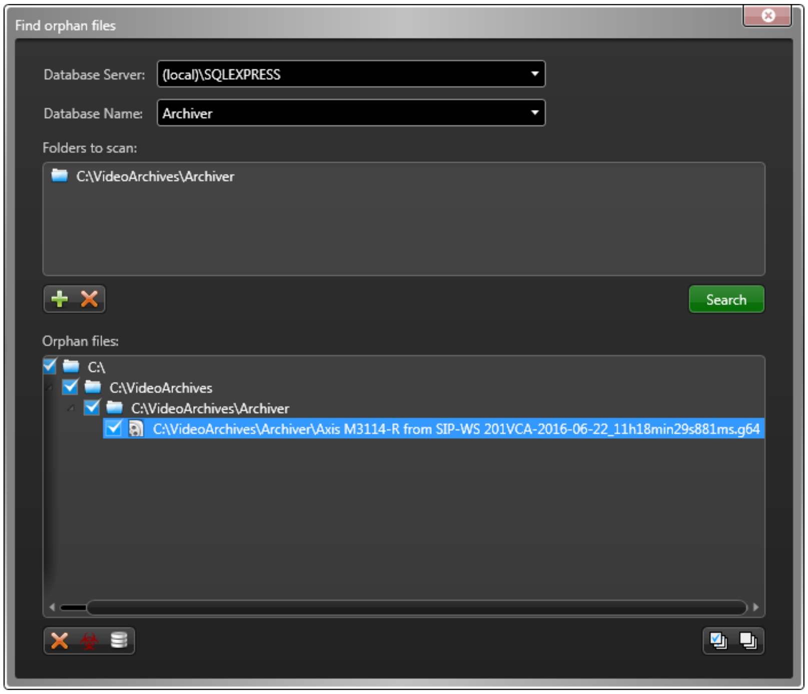
Orphan files:

5. Click **Search**.
6. Select files from the *Orphan files* list, and do one of the following:
   - To permanently remove the selected files from your system, click **Delete files** (✖).
   - To move the selected files to another location and free up storage space on the Archiver, click **Move files to another folder** (☣).

By moving the files, you can examine them and decide what to do with them later without affecting the Archiver's operation.

- To re-index the selected files in the Archiver database so that they can be found again using video reporting tasks in Security Center, such as the *Archives* report, click **Add files to the database** (🗄).

  NOTE: Only the basic information (recording start time and end time) is retrieved. This operation should only be used as an emergency measure; therefore, it is recommended to back up your database before you re-index the files.



Database Server: (local)\SQLEXPRESS

Database Name: Archiver

Folders to scan:

C:\VideoArchives\Archiver

Orphan files:

☑ C:\
☑ C:\VideoArchives
☑ C:\VideoArchives\Archiver
☑ C:\VideoArchives\Archiver\Axis M3114-R from SIP-WS 201VCA-2016-06-22_11h18min29s881ms.g64

Related Topics

Backing up databases on page 127

Finding missing files on your system

To find video files that are still referenced by your Archiver database but are no longer accessible from the storage device, you can use the *VideoFileAnalyzer.exe* tool found in the Security Center installation folder.

What you should know

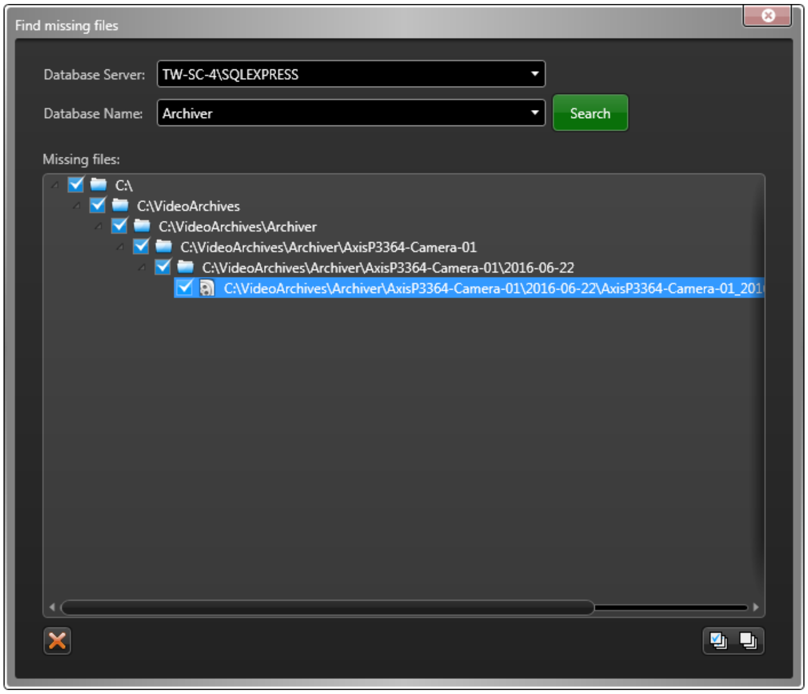
A *missing file* is a video file that is still referenced by a designated Archiver database but cannot be accessed anymore. This situation can arise if video files are deleted manually without using the *Archive storage details* task, creating a mismatch between the number of video file entries in the database and the actual number of video files on disk.

To find missing files on your system:

1. Open the *VideoFileAnalyzer.exe* tool.

   This tool is found in *C:\Program files (x86)\Genetec Security Center 5.5* on a 64-bit computer, and in *C:\Program files\Genetec Security Center 5.5* on a 32-bit computer.
2. At the bottom of the *Video File Analyzer* dialog box, click **Find missing files**.
3. In the *Find missing files* dialog box, specify the **Database Server** and the **Database Name** you want to check for missing video files.

   You can find the database server and database name in the *Resources* tab of the Archiver role in the Config Tool.
4. Click **Search**.
5. Once the scan has been completed, select files from the *Missing files* list, and then click **Delete files** (✖).



Find missing files

Database Server: TW-SC-4\SQLEXPRESS

Database Name: Archiver

Missing files:

- ☑ C:\
  - ☑ C:\VideoArchives
    - ☑ C:\VideoArchives\Archiver
      - ☑ C:\VideoArchives\Archiver\AxisP3364-Camera-01
        - ☑ C:\VideoArchives\Archiver\AxisP3364-Camera-01\2016-06-22
          - ☑ C:\VideoArchives\Archiver\AxisP3364-Camera-01\2016-06-22\AxisP3364-Camera-01_201

The selected file indexes are permanently removed from your Archiver database.

Troubleshooting: Video stream issues

In Security Desk, you can diagnose the status of video streams displayed in the canvas.

What you should know

Diagnosing the video stream helps you to determine at what point the flow of information is broken along the network path. Each component is displayed with information about the incoming and outgoing traffic, which tells you whether there is a potential problem with the video unit, the Archiver, the redirection to Security Desk, and so on.

To troubleshoot why there are issues with a video stream:

1 In Security Desk, display a camera in a tile.

2 Press `Ctrl+SHIFT+R`.

Diagnostic information about the video stream is overlaid in the tile.

3 Click **OK** to view information about each of the following video stream connections:

- **Archiver or Auxiliary Archiver or Federation™ redirector:** The streaming status from the source camera to the Archiver role, Auxiliary Archiver role, or Federation™ redirector initially providing the stream.
- **Redirector:** The streaming status from the Archiver role, Auxiliary Archiver, or Federation™ redirector to the redirector routing the stream to the next hop.

  NOTE: All redirectors involved in the routing will be listed.
- **Media player:** The streaming status from the last redirector involved in the routing to your Security Desk workstation.

4 Click **Close**.

Troubleshooting: Hardware acceleration issues

Security Desk can detect and use compatible hardware to accelerate video decoding. Hardware acceleration provides enhanced performance, especially when viewing multiple high-definition H.264 streams.

What you should know

For information on recommended video cards and performance benchmarks, see the Security Center 5.5 System Requirements document.

NOTE: Security Desk does not support hardware acceleration under Windows XP.

To ensure optimal video decoding performance with your computer:

1. To optimize the operation with NVIDIA video cards, make sure of the following:
   - The video card is of a compatible model.
   - The monitor or projector used to display video is plugged into this video card.
   - The installed driver is the latest available from NVIDIA's official web site.
2. To optimize the operation with Intel Quick Sync, make sure of the following:
   - Your CPU supports Quick Sync (see http://ark.intel.com)
   - The integrated video card on your CPU is of a compatible model.
   - A monitor is plugged into the motherboard's integrated output.
   - The Intel integrated graphics is enabled in the BIOS.
   - The installed driver is the latest available from Intel's official site.

   NOTE: On high performance computers, NVIDIA GPU decoding works better when Quick Sync is disabled.
3. To troubleshoot problems with multiple screens and multiple GPUs, make sure of the following:
   - If "SLI" mode is available, disable it.
   - If you have multiple NVIDIA video cards, connect each monitor to a different card to use them in parallel.
   - If you have video cards using different drivers (AMD, NVIDIA, Intel), set a monitor connected to a NVIDIA card as the primary monitor.
   - If both integrated and discrete video cards are available, and if your NVIDIA video card meets the recommended requirements, disable your integrated video card in the BIOS. Having the integrated card available actually hinders the discrete video card performance.
   - On laptops using NVIDIA OPTIMUS technology (combined Intel and NVIDIA GPUs), you need to launch each video intensive application (Security Desk, Genetec™ Video Player, and so on) a first time, after you installed Security Center, to allow the application to register itself as an application that requires NVIDIA GPU. After the initial run, the application will always use the NVIDIA GPU thereafter.

Related Topics

Hardware information dialog box on page 253

Video units are offline in Security Center

When a camera is red in the area view, it means that either the video unit is offline, or the communication with the Archiver has been lost.

What you should know

When a unit drops offline in Security Center, it usually coincides with a *Unit lost* event in Security Desk. This can be caused by an unstable network connection, or issues with the unit itself.

If you do not have access to both Security Desk and Config Tool you will not be able to perform every troubleshooting step.

To troubleshoot why a unit is offline:

1. Make sure you can ping the unit, as follows:
   - a) In the Config Tool **Video** task, select the red video unit.
   - b) At the bottom of the **Video** task, click **Ping** ().

   If there is no reply, the unit is offline (the unit might be broken, unplugged, and so on), or there is a problem with your network.
2. Make sure that you can connect to the unit's web page by typing its IP address in a web browser.
3. Restart the unit, as follows:
   - a) In the Config Tool **Video** task, select the red video unit.
   - b) At the bottom of the **Video** task, click **Reboot** ().
4. Make sure the unit is supported by Security Center, and that it is running the certified firmware.

   For a list of video units supported by Security Center, see the Supported Devices List.
5. Restart the Archiver role controlling the unit, as follows:

   IMPORTANT: Perform this step at a non-crucial time, since all the units connected to the Archiver will temporarily go offline.

   - a) In the Config Tool **Video** task, select the Archiver.
   - b) At the bottom of the **Video** task, click **Deactivate role** ( ).
   - c) In the confirmation dialog box that opens, click **Continue**.

     The Archiver and all video units controlled by the role turn red.
   - d) At the bottom of the **Video** task, click **Activate role** ( ).
6. If the video unit is still offline, contact Genetec™ Technical Support.

Troubleshooting: Network trace capture

You can run a network trace directly from Config Tool, even if you do not have a network packet analyzer installed on your computer.

What you should know

Security Center uses WinPcap library to capture the network trace. In order to read the captured network packet data files (.pcap), you need to have a compatible network packet analyzer, such as Wireshark, installed.

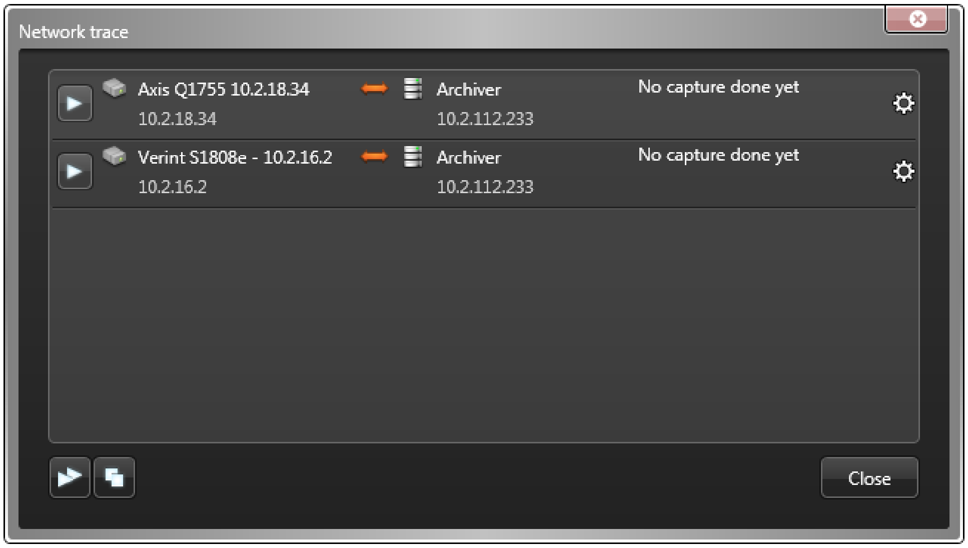
To capture the network packet data:

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

2 From the entity tree, select the video units you want to analyze.

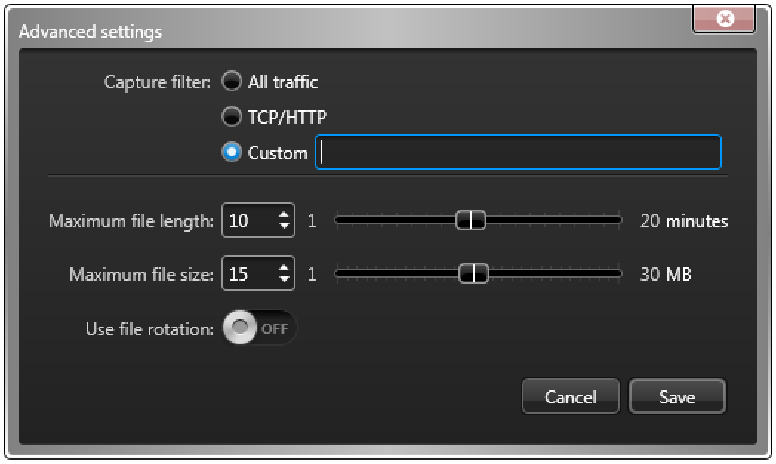
Hold the **CTRL** key to perform a multiple-selection.

3 Right-click your selection, and then click **Unit** > **Network trace**.



Axis Q1755 10.2.18.34 10.2.18.34	Archiver 10.2.112.233	No capture done yet
Verint S1808e - 10.2.16.2 10.2.16.2	Archiver 10.2.112.233	No capture done yet

4 (Optional) Click **Advanced settings** (⚙) to change the default settings of a particular capture.



Capture filter: ○ All traffic ○ TCP/HTTP ● Custom

Maximum file length: 10 (1 – 20 minutes)

Maximum file size: 15 (1 – 30 MB)

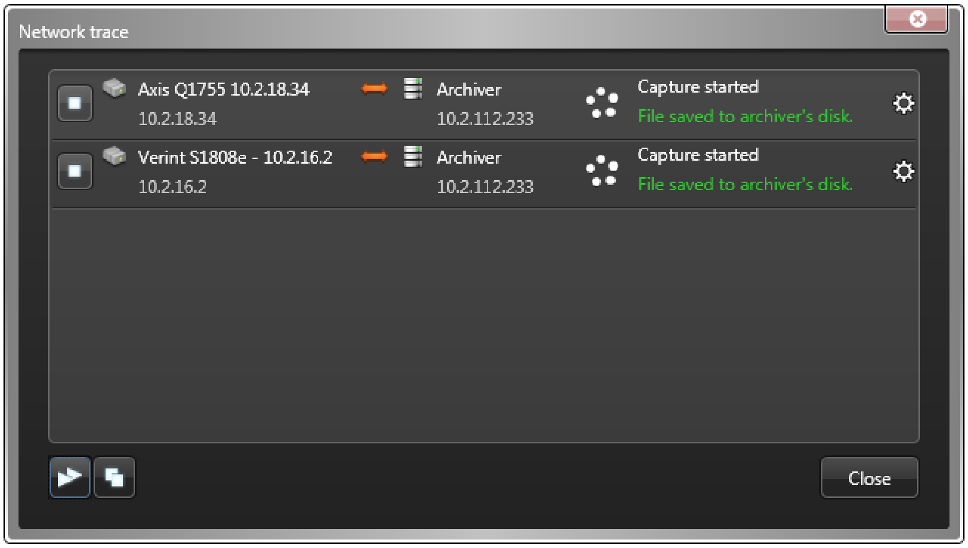
Use file rotation: OFF

- **Capture filter:** Select the type of traffic you want to capture.
  - **All traffic:** Capture everything that is between the video unit and the Archiver.
  - **TCP/HTTP:** Capture only TCP and HTTP traffic between the video unit and the Archiver (eliminates other traffic like UDP).

  - **Custom:** Custom filter. Use the same syntax as for Wireshark. Example: `host 10.1.1.1 and not udp`.
- **Maximum file length:** Maximum duration of the capture (default=10 minutes).
- **Maximum file size:** Maximum size of the captured data file (default=15 MB).
- **Use file rotation:** OFF (default): The capture stops when either the maximum file length or the maximum file size is reached, whichever comes first. ON: The capture lasts up to the maximum file length. A new file is created every time the maximum file size is reached, but only the last two are kept.

5 Do one of the following:

- Click **Start capture** (▶) to start a specific capture.
- Click **Start all captures** (▶) to start all configured captures.



Network trace

■	Axis Q1755 10.2.18.34 10.2.18.34	Archiver 10.2.112.233	Capture started File saved to archiver's disk.	⚙
■	Verint S1808e - 10.2.16.2 10.2.16.2	Archiver 10.2.112.233	Capture started File saved to archiver's disk.	⚙

If file rotation is turned off, a capture automatically stops when either the configured maximum file length or the maximum file size is reached, unless you stop it before hand.

6 Click **Close** when you finish.

The captured network packet data files are saved on the server hosting the Archiver role, in the folder *C:\Windows\Temp*.

The file names follow the format *genetec_capture_<address>_<date>_<time>_<sequence>.pcap*, where:

- *<address>* is the IP address of the video unit.
- *<date>* is the capture start date in the 'yy-mm-dd' format.
- *<time>* is the capture start time in hours, minutes, and seconds.
- *<sequence>* is the file sequence number. When file rotation is turned on, it indicates how many files were created during the capture event (only the last two are kept). Otherwise, it stays at '0001'.

Troubleshooting: "Impossible to establish video session with the server" errors

If you receive an *Error: Impossible to establish video session with the server* message, you can try to determine the cause.

What you should know

The *Error: Impossible to establish video session with the server* message could show up for multiple reasons. There could be a problem with your server, the Media Router role, the Federation™ role, the Archiver role, or the video unit itself.

If you do not have access to both Security Desk and Config Tool you will not be able to perform every troubleshooting step.

To diagnose an *Impossible to establish video session with the server* error:

1 Make sure your server is running.

2 Make sure the Archiver role is online, as follows:
   a) In the Config Tool **Video** task, select the Archiver.
   b) At the bottom of the **Video** task, click **Diagnose** (✚).
   c) If there are issues, try to fix them.

3 If you are trying to view a federated camera, make sure the Security Center Federation™ role or the Omnicast™ Federation™ role is online, as follows:
   a) In the Config Tool **System** task, click the **Roles** view.
   b) Select the Federation™ role, and at the bottom of the task, click **Diagnose** (✚).
   c) If there are issues, try to fix them.

4 If you are trying to view a federated camera, make sure the server of the federated Security Center system is online.

5 It might be a connection problem with the Media router. Make sure the Media Router role is online, as follows:
   a) In the Config Tool **System** task, click the **Roles** view.
   b) Select the Media Router role, and at the bottom of the task, click **Diagnose** (✚).
   c) If there are issues, try to fix them.

6 Restart the Media Router role, as follows:
   a) In the Config Tool **System** task, click the **Roles** view.
   b) Select the Media Router role, and at the bottom of the task, click **Deactivate role** (🚦).
   c) In the confirmation dialog box that opens, click **Continue**.

      The Media Router turns red.
   d) At the bottom of the **System** task, click **Activate role** (🚦).

7 Make sure that the unit is online.

   If the unit is red in the *Roles and units view*, then troubleshoot why the video unit is offline.

Cannot watch live video in Security Desk

If you cannot view video in Security Desk, you can try to troubleshoot the issue.

What you should know

Some of the reasons you could get a waiting signal error are the following:

- The network is slow.
- There is some sort of block due to your port connections.
- The video stream was dropped while it was being redirected to Security Desk.

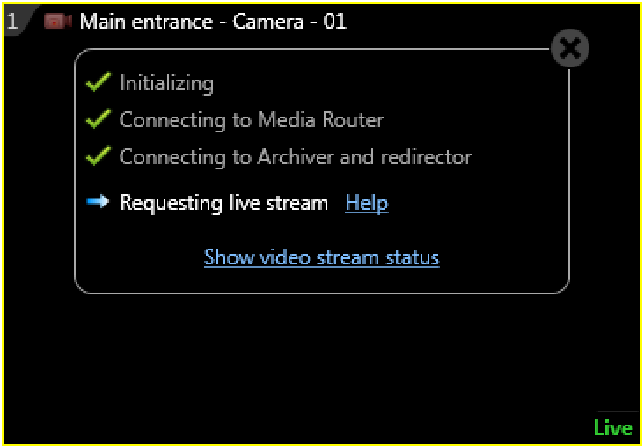
If you do not have access to both Security Desk and Config Tool you will not be able to perform every troubleshooting step.

To troubleshoot why you cannot view live video:

1 Wait to see if the camera connects.

2 If the problem persists for more than 10 seconds, then click **Show diagnosis** in the tile, or press `Ctrl+SHIFT+D`.

Information about the video stream is displayed. An arrow indicates the video stream issue that is occurring:



✓ Initializing
✓ Connecting to Media Router
✓ Connecting to Archiver and redirector
→ Requesting live stream

- **Initializing:** The media player is preparing the necessary resources to display the video as soon as the stream comes in.
- **Connecting to Media Router:** The media player is establishing connection with the Media Router in order to obtain the network location of the stream.
- **Connecting to Archiver and redirector:** The media player is currently establishing connection with the Archiver and the Redirector in order to request video.
- **Requesting live stream:** The connection is properly established between the Archiver and the Media Player. The Media Player is now requesting the live stream.
- **Analyzing the stream:** The stream was properly requested and received by the client workstation. The media player is analyzing the stream to detect the video format and the presence of key frames. Once the stream is validated, then the video will be decoded.

TIP: You can click the **Help** button for a quick reference list of things you can try to troubleshoot the issue.

3 Make sure that the unit is online.

If the unit is red in the *Roles and units view*, then troubleshoot why the video unit is offline.

4 Make sure you can ping the unit, as follows:

a) In the Config Tool **Video** task, select the red video unit.

b) At the bottom of the **Video** task, click **Ping** ().

If there is no reply, the unit is offline (the unit might be broken, unplugged, and so on), or there is a problem with your network.

5 Make sure that you can connect to the unit's web page by typing its IP address in a web browser.

6 Make sure the unit is supported by Security Center, and that it is running the certified firmware.

For a list of video units supported by Security Center, see the Supported Devices List.

7 Change the video unit's connection type to the Archiver, as follows:

a) In the Config Tool **Video** task, select the red camera.

b) Click the **Video** tab.

c) From the**Connection type** drop-down list in the *Network settings* section, select a different connection type.

d) Click **Apply**.

8 Try viewing playback video from the camera, as follows:

a) In the Security Desk Archives task, select the camera.

b) Select the most recent video archive available, and then click **Generate report**.

c) Once the report is generated, try to view the video from the archive.

- If you can view the video, continue with the next troubleshooting step.
- If you cannot view any video, contact technical support.

9 If you have an expansion server on your system running the Archiver role, try to view video from the expansion server, as follows:

a) Open Security Desk on the expansion server.

b) In the **Monitoring** task, drag the camera from the area view to a tile in the canvas.

- If you can view video, it might be a problem with the redirection from the Media Router to your Security Desk. Continue with the next troubleshooting step.
- If you cannot view any video, contact Genetec™ Technical Assistance.

10 Make sure the correct ports are open on your network so there is no firewall blocking the video stream.

11 Make sure each network on your system is configured properly, as follows:

a) In the Config Tool **Network view** task, select a network.

b) Click the **Properties** tab, and make sure all the settings are correct (IP prefix, subnet mask, routes, network capabilities, and so on).

c) Change the network settings if needed, and then click **Apply**.

12 Force Security Desk to use a different connection type, as follows:

a) From the Security Desk home page, click **Options** > **General**.

b) In the **Network options** section, next to the **Network** option, select **Specific**.

c) From the drop-down list, select a different network, and then click **Save**.

d) Restart Security Desk.

e) If changing the network connection does not work, repeat the steps to test using other networks.

13 If you still cannot view video, click **Show video stream status** in the tile, and then troubleshoot the video stream.

14 If the issue persists, contact Genetec™ Technical Assistance.

Cannot watch playback video in Security Desk

If you cannot view playback video or video archives in Security Desk, you can try to troubleshoot the issue.

What you should know

If you do not have access to both Security Desk and Config Tool you will not be able to perform every troubleshooting step.

To troubleshoot why you cannot view playback video:

1 Try viewing live video from the camera on the same workstation, by dragging the camera from the area view to a tile in the canvas in the Security Desk **Monitoring** task.

- If you can view live video, continue with the next troubleshooting step.
- If you cannot view any video, then it is probably a network issue. See Video units are offline in Security Center on page 468.

2 Try viewing playback video from the **Archives** task, as follows:

a) In the Security Desk **Archives** task, select a camera.
b) Search for video archives from the same camera at different dates and times, and then click **Generate report**.
c) Once the report is generated, try to view video from the archives.
d) Repeat the steps with other cameras that are connected to the same Archiver.

- If you can view the video from some of the video archives, continue with the next troubleshooting step.
- If you cannot view any video, skip the next troubleshooting step.

3 Make sure the unit is supported by Security Center, and that it is running the certified firmware.

For a list of video units supported by Security Center, see the Supported Devices List.

4 Try viewing playback video from the **Archives** task on another Security Desk, and on the server where the Archiver role is running.

- If you can view video, it might be a problem with the redirection from the Media Router to your Security Desk. Continue with the next troubleshooting step.
- If you cannot view any video, contact technical support.

5 Make sure the correct ports are open on your network so there is no firewall blocking the video stream.

6 If you still cannot view playback video, contact Genetec™ Technical Assistance.

Troubleshooting: Cameras are not recording

If you cannot record video, or there are missing video archives or gaps in the archives, you can try to determine the cause of the issue.

What you should know

If you can view live video from a camera but cannot record video, it might be due to the recording mode of the camera, the Archiving schedule, the Archiver role database, or even your CPU usage.

Some of the ways you can tell if the camera is not recording are the following:

- If you are viewing live video, the recording status of the camera is indicated in the lower-right corner of the tile. If the status indicates Live, the camera is currently not recording.
- You are trying to view playback video, but there is no video available for the date and time you selected, and you know that there should be.

If you do not have access to both Security Desk and Config Tool you will not be able to perform every troubleshooting step.

To troubleshoot why a camera is not recording:

1. Make sure the unit is supported by Security Center, and that it is running the certified firmware.

   For a list of video units supported by Security Center, see the Supported Devices List.
2. Verify the camera recording type to make sure the camera is set to record video on the correct schedule, as follows:
   a) In the Config Tool **Video** task, select the red camera.
   b) Click the *Recording* tab.
      - If the **Recording settings** option is set to **Custom settings**, then check that all the recording settings are correct, and then click **Apply**.
      - If the **Recording settings** option is set to **Inherit from Archiver**, then continue with the next substep.

   c) In the **Video** task, select the Archiver.
   d) Click the **Camera default settings** tab.
   e) In the *Recording modes* section, make sure the Archiver is set to record on the right **Schedule**, and that the recording **Mode** is not set to **Off**.
3. If the camera recording mode is set to **On motion/Manual**, then make sure the motion detection settings are configured properly, as follows:
   a) In the Config Tool **Video** task, select the red camera.
   b) Click the *Motion detection* tab.
   c) Verify the motion detection settings.
4. Check the status of the Archiver role database, as follows:
   a) In the Config Tool **Video** task, select the Archiver.
   b) Click the *Resources* tab.
      - If the Archiver database status is **Connected**, go to the next troubleshooting step.
      - If the Archiver database status is **Disconnected** or **Unavailable**, continue with the next substep.

   c) Click **Create a database** (+).

      CAUTION: Perform this step at a non-crucial time, since all the units connected to the Archiver will temporarily go offline. Give the database a new name. Do not overwrite the existing database, or your video archives will be deleted.

      NOTE: When you create a new database, the video archives from the old database are no longer included in Security Center searches, and will not be deleted by automatic database cleanups.

   - If the camera can record using the new Archiver database, you can continue to use the new database.

- If the camera is still not recording, revert back to the original database, and continue with the next troubleshooting step.

5 Check how much disk space is available for archiving, as follows:

a) In the Config Tool **Video** task, select the Archiver.

b) Click the *Resources* tab.

c) In the disk information table, make sure the **Min. free space** value is at least 0.2% of the **Total size** value.

The **Min. free space** is the minimum amount of free space that the Archiver must leave untouched on the disk.

d) If the **Min. free space** value is less than 0.2% of the **Total size**, click on the value, and then increase it.

6 Check for *Archiving stopped* and *Recording stopped* events that occurred on your system.

In Windows on the server where the Archiver role is running, open the *.log* files, located in *C:\ArchiverLogs*.

If there are *Archiving stopped* or *Recording stopped* events in the **Entry type** column, restart the Genetec™ Server service, as follows:

a) Open your Windows Control Panel.

b) Click **Administrative Tools** > **Services**.

c) Click the **Genetec Server** service, and then click **Restart**.

7 Check for *Transmission lost* and *RTP packets lost* events that occurred on your system.

In Windows on the server where the Archiver role is running, open the *.log* files, located in *C:\ArchiverLogs*.

- If there are many *Transmission lost* and *RTP packets lost* events in the **Entry type** column, then it might be a CPU usage or network issue. Continue with the next troubleshooting step.
- If there are not many *Transmission lost* and *RTP packets lost* events, then skip the next troubleshooting step.

8 Check your CPU usage, as follows:

a) Right-click in the Windows taskbar.

The *Windows Task Manager* opens.

b) Click the *Performance* tab, and make sure the **CPU Usage** is not over **60%**.

If the **CPU usage** is over **60%**, restart the server, and consider adding more CPU to the server.

c) Click the **Networking** tab, and make sure the network **Link speed** is not over **300 Mbps**.

9 If you are only experiencing recording problems with one video unit, try the following:

a) In the Config Tool **Video** task, right-click on the red video unit, and then click **Delete**.

b) In the confirmation dialog box that opens, choose if you want to keep the video archives from the unit.

The video unit is removed from the Archiver.

c) Add the video unit.

10 If you still cannot record video on the camera, contact Genetec™ Technical Assistance.

Troubleshooting: Video units cannot be added

If you are having trouble adding a video unit to an Archiver, you can try to determine the cause of the issue.

What you should know

When you cannot add a video unit, it might be due to network issues, user credential issues, and so on.

As a best practice, log on to Config Tool as an administrator.

To troubleshoot why a video unit cannot be added:

1 Make sure you can ping the unit, as follows:

a) In the Config Tool **Video** task, select the red video unit.

b) At the bottom of the **Video** task, click **Ping** (🖧).

If there is no reply, the unit is offline (the unit might be broken, unplugged, and so on), or there is a problem with your network.

2 Make sure that you can connect to the unit's web page by typing its IP address in a web browser.

This is also where you can determine if you have the correct credentials for the unit.

3 Restart the unit, as follows:

a) In the Config Tool **Video** task, select the red video unit.

b) At the bottom of the **Video** task, click **Reboot** (↺).

4 Try adding the unit again.

5 Make sure that you have a free camera connection in your Security Center license, as follows:

a) From the Config Tool home page, click the *About* page, and click the *Omnicast* tab.

b) In the **Number of cameras** license option, make sure there is a camera connection still available.

6 Make sure the unit is supported by Security Center, and that it is running the certified firmware.

For a list of video units supported by Security Center, see the Supported Devices List.

7 Make sure you are using the correct credentials when trying to add the unit, as follows:

For some manufacturers, you have to set the default credentials from the Archiver *Extensions* tab.

a) In Config Tool **Video** task, select the Archiver to which you are trying to add the video unit.

b) Click the *Extensions* tab.

c) To add the extension for the video unit, click **Add an item** (✚), select the extension type, and click **Add**.

d) Select the extension.

e) In the *Default logon* section, enter the username and password for the unit.

8 Make sure the Archiver is connected to the correct database, as follows:

a) In the Config Tool **Video** task, select the Archiver.

b) Click the *Resources* tab.

- If the Archiver database status is **Connected**, go to the next troubleshooting step.
- If the Archiver database status is **Disconnected** or **Unavailable**, continue with the next substep.

c) Click **Create a database** (✚).

CAUTION: Perform this step at a non-crucial time, since all the units connected to the Archiver will temporarily go offline. Give the database a new name. Do not overwrite the existing database, or your video archives will be deleted.

NOTE: When you create a new database, the video archives from the old database are no longer included in Security Center searches, and will not be deleted by automatic database cleanups.

9 Make sure the Media Router is connected to the correct database, as follows:

NOTE: If the camera was previously added in Security Center and the IP address or name was changed, you can also re-create the Media Router database.

a) In Config Tool **Video** task, select the Media Router.

b) Click the *Resources* tab.

- If the Media Router database status is **Connected**, go to the next troubleshooting step.
- If the Media Router status is **Disconnected**, or **Unavailable**, continue with the next substep.

c) Click **Create a database** (➕).

10 Try adding the unit with the firewall turned off.

For information about how to disable Windows firewall, see KBA00596: "Recommended Windows Firewall Settings" on the Genetec™ Technical Information Site.

IMPORTANT: Do not turn off the firewall permanently. Reactivate it after your tests are complete.

11 Make sure each network on your system is configured properly, as follows:

a) In the Config Tool **Network view** task, select a network.

b) Click the **Properties** tab, and make sure all the settings are correct (IP prefix, subnet mask, routes, network capabilities, and so on).

c) Change the network settings if needed, and then click **Apply**.

12 Make sure the Archiver, Media Router, and all redirectors are using the correct NICs (network interface cards), as follows:

a) In the Config Tool **System** task, click the **Roles** view.

b) Select the **Archiver** role, and click the *Resources* tab.

c) From the **Network card** drop-down list, select the appropriate NIC.

d) In the entity tree, select the **Media Router** role, and click the *Resources* tab.

e) Under the *Servers* section, click **Advanced** (⚙).

f) Select the appropriate **Network card** for each server, and click **Apply**.

g) Click the *Properties* tab.

h) Select a **Redirector**, and click **Edit the item** (✎).

i) From the **Multicast interface** drop-down list, select the appropriate NIC.

j) Repeat the last two substeps for each redirector.

13 Try adding the unit.

14 Verify the NICs priority in Windows, as follows:

a) In Windows, click **Start** > **Run**, and type `ncpa.cpl`.

The *Network Connections* window opens.

b) Click the **Advanced** menu above and select **Advanced Settings**.

c) Note which NIC on your server is configured as network priority one (at the top of the Connections list), and which is configured as priority two.

d) If needed, use the arrow buttons on the right side to move the different connections up and down in the list.

15 Try adding the unit.

16 It might be a connection problem with the Media router. Make sure the Media Router role is online, as follows:

a) In the Config Tool **System** task, click the **Roles** view.

b) Select the Media Router role, and at the bottom of the task, click **Diagnose** (✚).

c) If there are issues, try to fix them.

17 Make sure the Archiver role is online, as follows:

a) In the Config Tool **Video** task, select the Archiver.

b) At the bottom of the **Video** task, click **Diagnose** (✚).

c) If there are issues, try to fix them.

18 If you still cannot add the video unit, contact Genetec™ Technical Assistance.

Troubleshooting: Video units cannot be deleted

If you cannot delete a video unit, you can temporarily deactivate the Archiver.

To delete a video unit:

1 In the Config Tool **Video** task, select the Archiver.

2 At the bottom of the **Video** task, click **Deactivate role** ( ).

3 In the confirmation dialog box that opens, click **Continue**.
The Archiver and all video units controlled by the role turn red.

4 Select the video unit, and at the bottom of the **Video** task, click **Delete** (✖).

5 Select the Archiver, and at the bottom of the **Video** task, click **Activate role** ( ).

Troubleshooting: H.264 video stream issues

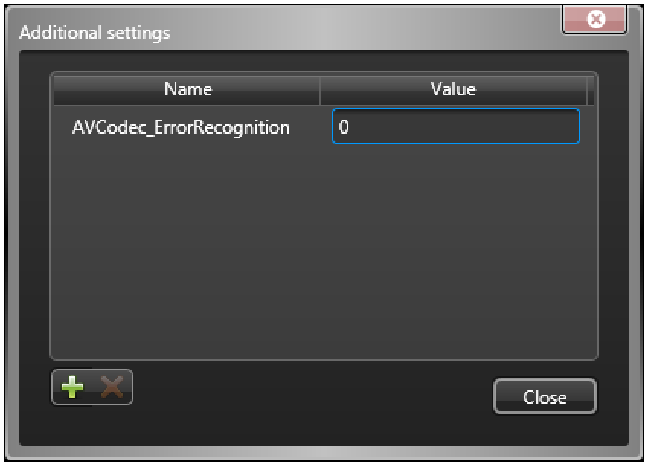
If you are having problems viewing H.264 video streams, you can disable the *AVCodec_ErrorRecognition* advanced Archiver role setting.

What you should know

If you do not have access to both Security Desk and Config Tool you will not be able to perform every troubleshooting step.

To troubleshoot H.264 video stream issues:

1 In the Config Tool **Video** task, select the Archiver to configure.
2 Click the *Resources* tab.
3 At the bottom of the *Resources* tab, click **Advanced settings**.
4 Click **Additional settings**.
5 In the **Additional settings** dialog box, click **Add an item** (➕).



Name	Value
AVCodec_ErrorRecognition	0

6 In the **Name** column, type `AVCodec_ErrorRecognition`.
7 In the **Value** column, type 0.
8 Click **Close**.
9 In the *Advanced settings* dialog box, click **OK**.
10 In the *Resources* tab, click **Apply**.
11 When you are asked to restart the Archiver, click **Yes**.

You should see improvement with the video stream. If there is no change, you can try other values (1-4).

Troubleshooting: Axis P1428-E camera sensitivity issue

If you are unable to lower the sensitivity of the Axis P1428-E camera to get a reliable motion detection performed by the Archiver on its H.264 video stream, you can lower the value of the *Vectors weight* in the *Advanced settings*.

What you should know

The Axis P1428-E camera encodes the motion vectors differently from most cameras, causing the Archiver's motion detection algorithm to be hyper-sensitive.

To lower the motion detection sensitivity on the Axis P1428-E camera:

1. From the Config Tool home page, open the **Video** task.
2. Select the camera you want to configure and click the *Motion detection* tab.
3. Click **Advanced settings**.
4. In the *H.264 advanced motion detection settings* dialog box, lower the **Vectors weight** to 1 or 0, and click **OK**.

   This should allow the Archiver's motion detection algorithm to respond to different *Sensitivity* settings.
5. Test the motion detection with different sensitivity settings until satisfactory results.
6. Click **Apply**.

Motion detection is not working in Security Center

[KBA00965] If motion detection is not working for some cameras in Security Center, you can troubleshoot the issue.

To troubleshoot motion detection in Security Center:

1. Make sure the unit is supported by Security Center, and that it is running the certified firmware.

   For a list of video units supported by Security Center, see the Supported Devices List.
2. Make sure that there are no known issues or limitations related to motion detection for you camera in the *Security Center Release Notes*.
3. Make sure that the motion detection settings are configured properly for the camera.
4. Make sure that you are receiving motion events in Security Desk, as follows:
   a) From the Security Desk home page, click **Options** > **Events**.
   b) Make sure that the Motion on and Motion off events are selected, and click **Save**.
   c) Open the Monitoring task.
   d) At the bottom of the Monitoring task, click **Monitoring** (🔭), and then click **Add** (➕).
   e) In the **Select entities** section, select the camera you want to monitor, and click **Add**.

      The entities you selected are added to the **Monitoring** list.
   f) Create some motion near the camera, and make sure that the motion events show up in the event list of the Monitoring task.
5. If you do not receive any motion events, then lower the **Motion on threshold** value in the camera's *Motion detection* tab and try creating motion near the camera again.
6. Do one of the following:

   - If you still do not receive any motion events, then it might be an issue with your camera. Contact Genetec™ Technical Assistance.
   - If you receive the motion events, then verify that motion detection is working by configuring the camera to record on motion as follows:

     1. From the Config Tool home page, open the **Video** task.
     2. Select the camera to configure, and click the *Recording* tab.
     3. Under the **Recording modes** section, in the **Mode** column, select **On motion/Manual**.
     4. Click **Apply**.

Related Topics

KBA: Axis cameras do not have a Motion detection tab on page 483

KBA: Axis cameras do not have a Motion detection tab

[KBA01211] If your Axis camera is missing the Motion detection tab in Config Tool, then you must uninstall the *Axis Video Motion Detection* application from the unit's web page.

What you should know

The Motion detection tab is hidden when Security Center detects that the *Axis Video Motion Detection* application is installed on the unit.

To show the motion detection tab for Axis cameras:

1 Open the unit's web page.

2 Click **Setup** > **Applications**.

3 Under **Installed Applications**, select **Axis Video Motion Detection**, and then click **Remove**.

4 Reset the camera to its factory settings (usually performed from the *System Options* menu).

The Motion detection tab is now visible in Security Center.

Related Topics
Motion detection is not working in Security Center on page 482

Configuring Security Center to open live video quickly

You can minimize the time it takes for a camera to open and display live video in the Security Desk *Monitoring Task* by adjusting several settings in Config Tool and Security Desk.

What you should know

- The time it takes to display live video from a camera in Security Desk varies depending on the model and manufacturer of the camera.
- A camera streaming MJPEG video usually displays live video quicker than a camera streaming H.264 video.
- A camera with video image quality of 70% usually displays live video quicker than a camera that has video image quality of 100%, or video image quality below 60%.
- Not all cameras support keyframe requests, configuring a low **Key frame interval** setting on the **Video** tab of Config Tool might produce better results.

To configure a camera to display live video faster:

1. From the Config Tool home page, open the *Video* task.
2. Select the camera to configure, and then click the **Video** tab.
3. In the **Stream usage** section, turn on **Live** and **Recording** for the selected stream.
4. In the **Network settings** section, select **Multicast** as the **Connection type**.
5. Click **Apply**.
6. Click the **Recording** tab, and select **Continuous** from the **Recording modes** drop down list.
7. Click **Apply**.
8. From the Security Desk home page, click **Options** > **Video**.
9. Scroll down to the **Video cache** section and turn off **Live video caching**.
10. Under **Advanced settings**, set the **Jitter buffer delay** to **0** ms.
11. Restart Security Desk.

Part V

Access control

This part includes the following chapters:

27

Access control at a glance

This section includes the following topics:

About Synergis™

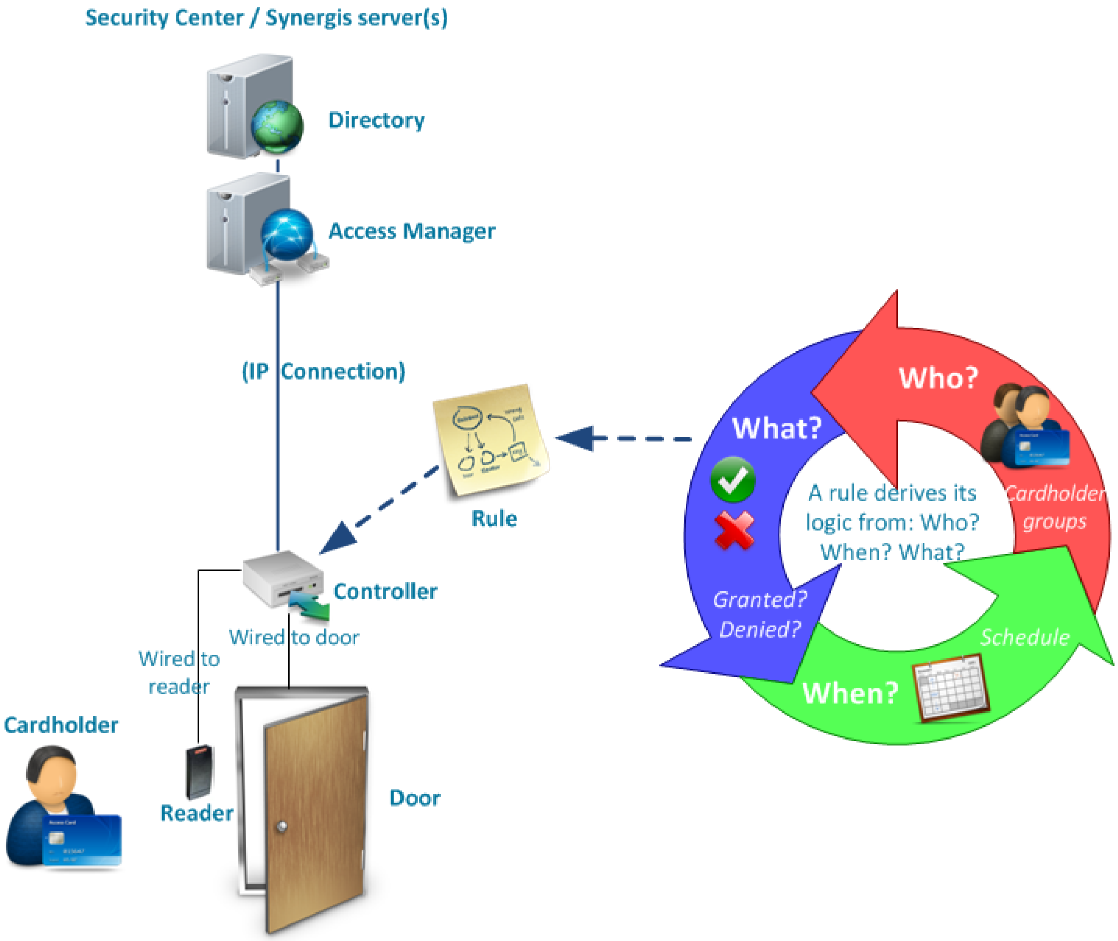
Synergis™ is the IP access control system of the Security Center designed to offer end-to-end IP connectivity, from access control reader to client workstation. Synergis™ seamlessly integrates a variety of access control capabilities including, but not limited to, badge design, visitor management, elevator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

Synergis™ was designed with an open and distributed architecture. You can build your system with new IP readers or use what you already have. Integrate your access control system with other third-party systems, like intrusion or building management, and distribute Synergis™ server components on many different network machines to optimize bandwidth and workload.

Synergis™ *Enterprise* supports an unrestricted number of doors, controllers and client workstations. You can grow your system one door at a time or scale your system across multiple buildings using the *Federation* feature.

How Synergis™ works

Synergis™ architecture is based on the server role known as the *Access Manager*, which controls the physical door controllers.



The following provides a general description of how Synergis™ architecture works:

- System configurations are saved by the Directory role.
- The Directory pushes configurations to the Access Manager.

- Access Manager communicates directly with the physical door controllers, called access control units, over TCP/IP.
- Access Manager pushes schedules, cardholder information, and access rules to the door controllers.
- When a cardholder presents their credential to a reader, the controller refers to the access rule to determine whether the user should be granted or denied access.
- Once controllers have synchronized with the Access Manager, they can operate autonomously, even if they lose the network connection to the Access Manager.

With additional configuration, a cardholder can belong to a cardholder group, a door can be part of an area, and there can be multiple schedules and rules pushed to a unit.

Benefits of Synergis™

Unlike other products or solutions, Synergis™ does not use “Clearance codes” or “Access levels” to grant or deny access. Instead, the basic logic used by Synergis™ to grant or deny access is defined by the *access rule*.

The biggest difference between an *access rule* approach and an *access level* approach is that access rules are applied to to the access points of the physical locations we want to protect, whereas access levels are applied to people. Access rules specify *who* can pass through a door and *when* they can do so. An access level defines *where* and *when* a person can gain access.

An access rule contains the three W’s:

- Who? (Who can pass through — *cardholders* or *cardholder groups*)
- What? (Whether access is granted or denied)
- When? (The *schedule* when the access rule is applied)

Notice that Synergis™ does not grant access to a card or credential. Rather, access is granted or denied based on the cardholders themselves. This subtle, but fundamental shift in the applied logic has a significant benefit in managing lost and stolen cards. The access rules that have been pushed to the *door controllers* do not have to be modified. If you associate a new credential with a cardholder, the old rule is still valid.

Entities related to access control

The Synergis™ access control system supports many of the entities that are available in Security Center.

Icon	Entity	Description
	Access Manager (role)	Role that manages the door controllers in the system.
	Access control unit	Door controller that a reader is attached to.
	Door	Physical barrier controlled by an access control unit.
	Elevator	A single elevator cabin.
	Access rule	Logic used to determine whether or not to grant access.
	Secured area	Physical location whose access is controlled by *access rules* and other access control behavior, such as antipassback, interlock, first-person rule, two-person rule, and so on.
	Cardholder	Individual who possesses a credential.
	Cardholder group	Group of cardholders sharing common characteristics.
	Credential	Claim of identity, such as card, PIN, biometric scan, and so on.
	Badge template	Custom-designed printing template for user credentials.
	Schedule	Date and time range.
	Partition	Group of entities on the system visible only to a group of users.
	User	Individual who uses Security Centerapplications.
	User group	Group of users sharing common characteristics.

28

Access control deployment

This section includes the following topics:

Preparing to deploy your access control system

To make sure that your access control deployment goes smoothly, you need to perform a series of pre-configuration steps.

Before deploying your access control system:

1 Have a network diagram showing all public and private networks used within your organization, and their *IP address* ranges.

For public networks, you also need the name and public IP address of their proxy servers. Ask your IT department for this information.

2 Install the following Security Center software components:

a) Security Center Server software on your main server.

The *main server* is the computer hosting the *Directory* role.

b) (Optional) Security Center Server software on expansion servers.

An *expansion server* is any other server on the system that does not host the Directory role. You can add expansion servers at any time.

c) Security Center Client software on at least one workstation.

For more information about installing Security Center, see the *Security Center Installation and Upgrade Guide*.

d) Security Center Client software on at least one workstation.

3 Have a list of *partitions* (if any).

Partitions are used to organize your system into more manageable subsystems. This is especially important in a multi-tenant environment. If, for example, you are installing one large system in a shopping center or, office tower, you might want to give local administration privileges to the tenants. By using partitions, you can group the tenants so that they can only see and manage the contents of their store or office, but not the others.

4 Have a list of all known users with their names and responsibilities.

To save time, identify users who have the same roles and responsibilities, and organize them into user groups.

NOTE: For large installations, users and user groups can be imported from a Windows *Active Directory*.

5 Install all *access control units* (door controllers and/or edge *readers*) on your company's IP network, and wire them to your doors, all the while collecting the following information:

- Manufacturer, model, and IP address of each unit.
- Manufacturer and model of the *interface modules* connected to each unit.
- Login credentials (username and password) for each unit.
- Which *access points* is each unit/interface module connected to.
- Are the doors *card-in/card-out* or *card-in/REX-out*?
- Which inputs are connected to the door sensors, REX, and manual stations?
- Which outputs are connected to the door locks, buzzers, our push buttons?

TIP: A site map or floor plan showing door, elevator, controller and reader locations would be very helpful.

6 Have a list of *secured areas* with their perimeter *doors* where access is controlled.

7 Have a list of all known *cardholders* (and *cardholder groups* where applicable).

Cardholders are people who have physical access to the monitored site.

NOTE: For large installations, cardholders can be imported from a text file or from a Windows *Active Directory*.

8 Have a list of available *credentials* with their facility codes and card numbers.

9 Have a list (and details) of all required schedules (office hours, holidays, and so on).

10 Have a list (and details) of all required *access rules* (*who* is allowed *where* and *when*).

11 If you are integrating Omnicast™, have a list indicating which *cameras* will be associated with which access points (door side and elevator floors).

NOTE: A camera can be associated with more than one door, and vice versa.

Deploying your access control system

To integrate a variety of access control capabilities and provide end-to-end IP connectivity, you can deploy your access control system once the pre-configuration steps are completed.

Before you begin

Perform the pre-configuration steps.

What you should know

A Security Center system can be deployed with access control only (Synergis™ alone), or access control with video integration (Synergis™ with *Omnicast*™). It does not matter whether the video or the access control system is set up first.

NOTE: Unless otherwise specified, you can perform the following steps in any order.

To deploy your access control system:

1. Use the **Admin** account on Config Tool to connect to your system.
2. Create a partition for each independent group of entities.

   By first defining the partitions, you will not have to move entities around after you have created them.

3. To organize the entities in your system (areas, doors, and so on), configure the area view.
4. Configure the Access Manager roles.
5. Define custom fields for your system entities.
6. Discover and enroll access control units.

   The Access Manager role needs to detect the door controllers over the IP network.

7. Configure the newly enrolled access control units and the interface modules that are attached to them.
8. Create doors and configure the wiring of the readers, sensors, locks, and so on to the access control units.
9. Create elevators and configure the wiring of the cabin reader and floor buttons to the access control units.
10. Create schedules, such as open and closed hours, holidays, and so on.
11. Create access rules and link the rules to doors and schedules.
12. Transform the areas in the area view into secured areas with access rules, perimeter doors, and advanced access control behaviors.
13. Create cardholder groups and create cardholders, and then link them to the access rules.
14. Create badge templates.
15. Create credentials.
16. Create user groups and create users.
17. Create alarms.
18. Create threat levels.

After you finish

Test your configuration.

Deploying your access control system with video

Once your Omnicast™ and Synergis™ systems are available, you can integrate the two systems.

Before you begin

Do the following:

- Set up your access control system.
- Set up your Omnicast™ system.

To deploy your access control system with video:

1. If the Omnicast™ *Archiver* and the Synergis™ *Access Manager* are found on the same Security Center system, do the following:
   a) Link your doors to the Omnicast™ cameras.
   b) Link your elevators to the Omnicast™ cameras.
2. If the Omnicast™ Archiver and the Synergis™ Access Manager are found on independent systems, do the following:
   a) Federate the Omnicast™ cameras with your access control system.
   b) Link your doors to the Omnicast™ cameras.
   c) Link your elevators to the Omnicast™ cameras.

About Access Managers

Access Manager is the role that manages and monitors access control units on the system.

The Access Manager keeps the units updated with the access control settings configured in Security Center, in real-time or on a schedule, so that they can make independent access control decisions whether they are connected to the Access Manager or not.

The Access Manager also logs the access control *events* in the database for access control investigation and maintenance reports. All events generated by the units (access granted, access denied, door open, etc.) are forwarded by the Access Manager, through the Directory, to the concerned parties on the system.

Multiple instances of this role can be created on the system.

Configuring Access Manager roles

To monitor the units, keep them in sync with the access control settings in Security Center, and allow them to make access control decisions independently, you can configure an Access Manager to control the units.

What you should know

When Synergis™ is enabled by your license, an Access Manager role is created by default and hosted on the main server.

To configure an Access Manager role:

1. From the Config Tool home page, open the *Access control* task, and click the **Roles and units** view.
2. Select the Access Manager role to configure, and click the **Resources** tab.
3. If necessary, configure the database required to run this Access Manager.
4. Click the **Properties** tab.
5. In the **Keep events** option, select how long you want access control events that are logged by the Access Manager to remain in the database for reporting and maintenance purposes (this includes events related to doors, elevators, areas, and other access control entities).
   - **Indefinitely:** Keep the events until you manually delete them.
   - **For:** Select the number of days for the retention period.

   CAUTION: If you are using the *SQL Server 2014 Express* database engine (included with the Security Center installation files), the database size is limited to 10 GB. A door event uses (on average) 200 bytes in the database. If you configure the Access Manager to retain door events indefinitely, the database eventually reaches the 10 GB limit and the engine stops.
6. Select the **Enable peer to peer** option to enable communication between the Synergis™ units managed by this Access Manager.

   BEST PRACTICE: Only enable peer to peer communication if you plan to create I/O zones that involve multiple Synergis™ units, or apply antipassback to areas controlled by multiple Synergis™ units. Leave this option off for better system security and performance.
7. Select **Enable global antipassback** if you need to apply antipassback to areas controlled by multiple Synergis™ units.

   To enable this option, you must first enable peer to peer.

   BEST PRACTICE: If all your antipassback areas are controlled by a single unit, do no enable global antipassback. Enabling global antipassback increases the communication between Synergis™ units.
8. If necessary, add the manufacturer extensions for the access control unit types that you want this Access Manager to manage.
9. Add the access control units that you want this Access Manager to manage.

After you finish

If you need more than one Access Manager role on your system, you can create additional Access Manager roles and host them on separate servers.

Related Topics

About Access Managers on page 495
Databases on page 117

Adding access control unit manufacturer extensions

For the *Access Manager* to communicate with access control units, you must add the manufacturer-specific extensions.

What you should know

Starting from Security Center 5.3, the manufacturer extensions are added by default when the Access Manager is created. Therefore, you only need to add the extensions manually if the Access Manager was created prior to version 5.3. However, the Genetec™ Synergis™ extension required by Synergis™ units is created with the default discovery port, 2000. If you configured your Synergis™ units with a different port number, you must also change it on the Access Manager.

To add a manufacturer extension to the Access Manager:

1. Open the *Access control* task, and click the **Roles and units** view.
2. Select the Access Manager, and click the **Extensions** tab.
3. At the bottom of the extensions list, click **Add an item** (➕).
4. In the *Add extensions* dialog box, select the extension types you need and click **Add.**

   NOTE: If you only selected **HID VertX**, the procedure ends here.
5. Select the Genetec™ Synergis™ extension you just added.
6. To add a discovery port, click **Add an item** (➕), at the bottom of the *Discovery ports* section.
7. In the *Discovery port* dialog box, enter the port number configured for your Synergis™ units and click **Create**.

   The port number must match the discovery port configured on your Synergis™ units. The default value is 2000. Do not change the default value unless your IT department uses this port for a different purpose.
8. Click **Apply.**

Related Topics

Access Manager configuration tabs on page 853

29

Access control units

This section includes the following topics:

About access control units

An access control unit is a type of entity that represents an intelligent access control device, such as a Synergis™ appliance or an HID network controller, that communicates directly with the Access Manager over an IP network. An access control unit operates autonomously when it is disconnected from the Access Manager.

Supported types of access control units

Security Center supports the following types of access control units:

- **Synergis™ appliances:** A Synergis™ appliance is an IP-ready security appliance manufactured by Genetec Inc. that is dedicated to access control functions. All Synergis™ appliances come preinstalled with Synergis™ Softwire and can be enrolled as access control units in Security Center.

  There are two generations of Synergis™ appliances:

  - Synergis™ Cloud Link (second generation)
  - Synergis™ Master Controller (first generation)

  All Synergis™ appliances support a variety of third-party interface modules over IP and RS-485. For a complete list of supported interface modules and limitations, see the *Synergis™ Softwire Release Notes* and the *Synergis™ Softwire Integration Guides*, available on the Technical Information Site.
- **HID network controllers:** The HID network controllers include the VertX EVO (V1000, V2000), Edge EVO controllers, and the legacy VertX and Edge controllers. HID controllers are intelligent IP devices that can acquire their network address automatically when your network has a DHCP server (the default). They can also be configured with static addresses (recommended).

To simplify our language, Synergis™ appliances are also called *Synergis™ units*, and HID network controllers are called *HID units*.

About interface modules

An access control unit typically controls sub-panels, such as HID VertX-series sub-panels, and Mercury MR-series sub-panels, which in turn connect to door sensors and readers. In the case of Synergis™ appliances, the unit is also capable of managing other intelligent devices, such as intelligent locks and other controllers.

In Security Center, all devices directly connected to the access control unit are referred to as interface modules, thus the following definition:

An interface module is a third-party security device that communicates with an access control unit over IP or RS-485, and provides additional input, output, and reader connections to the unit.

Related Topics

HID features and models supported by Security Center on page 962
About unit synchronization on page 500
How access control units operate on page 501
Applying antipassback to areas on page 527

About unit synchronization

Unit synchronization is the process of downloading the latest Security Center settings to an access control unit. These settings, such as access rules, cardholders, credentials, unlock schedules, and so on, are required so that the unit can make accurate and autonomous decisions in the absence of the Access Manager.

A unit is synchronized for the first time when you enroll it to your system. The Access Manager through which the unit is enrolled automatically takes care of this process. Only the settings necessary for the unit to make autonomous decisions are downloaded. When synchronizing a unit, the Access Manager knows how much memory the unit has, and fills it with as much information as it can handle.

The Access Manager roles automatically synchronizes the units assigned to it when a change is made in Security Center. For HID units, you can configure the synchronization to occur periodically, or only on request.

You can request a manual synchronization at any time if you suspect that a unit is not perfectly in synch with the system by going to the unit's **Synchronization** tab in Config Tool, and clicking **Synchronize now**.

While the unit is synchronizing, the synchronization icon (⇅) appears over the unit and the entities it controls, such as doors, elevators, and zones.

IMPORTANT: All synchronization errors are displayed in yellow. Pay attention to these errors to avoid any disruption in the operation. For example, HID VertX units are limited to 65,000 credentials. Exceeding this limit causes the synchronization to fail and the unit to reset.

Related Topics

About access control units on page 499
How access control units operate on page 501
Access control unit - HID - Synchronization tab on page 784
Access control unit - Synergis™ – Synchronization tab on page 791

How access control units operate

All access control units make autonomous decisions by default, relying on the access control settings downloaded from Security Center during unit synchronization. The unit only falls back on the Access Manager when it is presented with an unknown credential.

Online operation

The access control unit is operating online when it is connected to its Access Manager. The unit makes decisions on its own, based on the access control settings (access rules, cardholders, credentials, unlock schedules, and so on) downloaded from Security Center when it was last synchronized.

When the access control settings are changed in the system, the Access Manager automatically updates the units that are affected by the change, every 15 seconds. For HID units, you also have the option to configure the synchronization to be carried out daily, weekly, or on demand. When an unknown credential is presented, the unit immediately queries its Access Manager in order to carry out the correct decision, and thus, updates its memory at the same time.

As long as the unit remains connected to its Access Manager, it reports every decision it makes (*Access granted* and *Access denied*) and all activities (*Door opened*, *Door closed*, *Entry detected*, and son on) in real time to the Access Manager. The Access Manager can override a decision to deny access if it contradicts the current settings in Security Center.

Server mode

The server mode is a special online operation mode restricted to Synergis™ units, in which the unit allows the Access Manager (the server) to make all access control decisions. The unit must stay connected to the Access Manager at all times to operate in this mode..

NOTE: Do not enable this mode unless instructed by a representative of Genetec Inc.. When the unit operates in server mode, certain access control features are no longer supported.

Offline operation

The access control unit is said to operate offline when the connection to its Access Manager is lost. When operating offline, the unit appears in red in Config Tool and Security Desk.

Although offline, the unit continues to make access control decisions based on the information previously downloaded through the Access Manager during synchronization. The difference is that the Access Manager is no longer able to override any deny decisions, nor to update the unit when settings are changed in Security Center. All activities are logged locally on the unit, and are uploaded to Security Desk when the connection with the Access Manager is re-established.

Related Topics

About access control units on page 499
About unit synchronization on page 500

Preparing to add HID access control units

Before you can add an HID unit in Security Center, you must know its IP address and login credentials. To find this information, you can use the *Unit enrollment* tool.

What you should know

HID VertX (V1000, V2000), and Edge devices are IP devices that can acquire their network address automatically when your network has a *DHCP server*. If no DHCP server is present on your network, you must assign a static IP configuration to the unit (recommended).

To change the unit's initial IP configuration if necessary, you can use the *HID Discovery GUI*. For more information about the *HID Discovery GUI*, see your HID documentation.

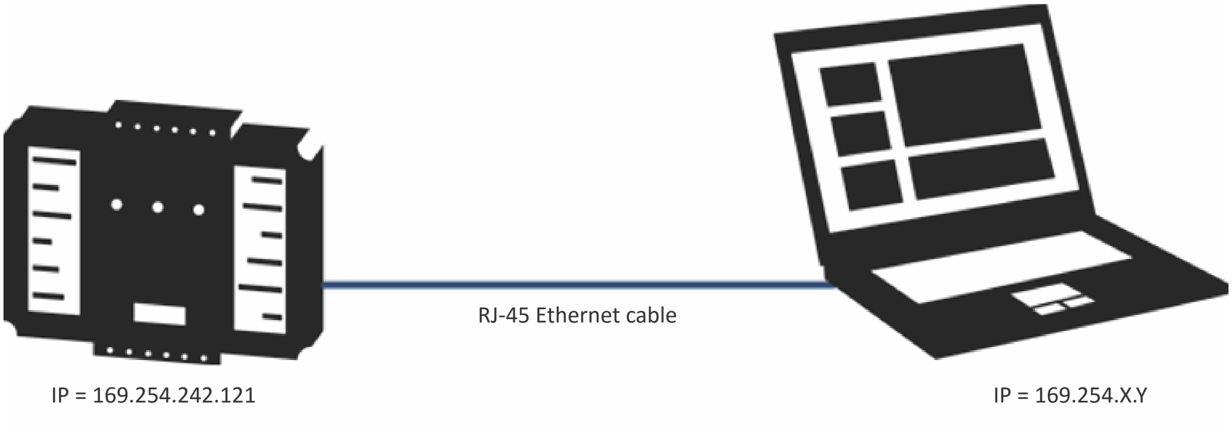
For more information about initial HID hardware setup, see the HID device documentation in the *Documentation|Controllers* folder of your Security Center installation package, or download the documentation from http://www.HIDglobal.com.

To prepare to add an HID unit in Security Center:

1 Discover the access control units on your network.

2 If the HID unit you want is not found, disconnect your workstation’s network cable and plug it directly into the HID unit. For PoE units, such as Edge or Edge EVO, connect your laptop and unit to a standalone switch.

The address 169.254.242.121 is the factory-assigned default address for every HID device. Even if the unit has been configured with an IP configuration, it still listens on this address for possible troubleshooting needs.



3 Type *http://169.254.242.121* in your web browser.

4 To log on, enter the default username (root) and password (pass).

NOTE: The web interface for EVO units can only be accessed with the *admin* account. By default, the password is blank. Change it after changing the IP settings. To enrol the unit into Security Center, you must use root/pass.

5 In the **Basic Setup** page, assign the device’s IP configuration.

CAUTION: If no DNS server is present on your network, you must use the unit’s own *IP address* for the **Primary DNS Server** value, and the **Basic Central Station**’s IP address should be set to the IP address of your Security Center server running the *Access Manager* role.

6 (Optional) Click **Change Login Password**, and then change the password.

Changing the password applies to the *admin* user not the *root* user.

7 Click **Submit**.

The new IP configuration is applied to the unit and it restarts. You can now add the unit in Security Center.

Adding access control units

To control access in your system, and monitor access control-related events in Security Center, you must add access control units to an Access Manager.

Before you begin

Add the access control unit manufacturer extensions.

The HID units you plan to add must be online, and you must know their IP addresses and login credentials (username and password).

What you should know

This section only covers adding HID units. For information about adding Synergis™ units, see the *Synergis™ Appliance Configuration Guide*.

To add an HID unit:

1. Open the *Access control* task, and click the **Roles and units** view.
2. Click **Add an entity** (➕), and select **Access control unit**.
3. From the **Network endpoint** drop-down list in the **Unit information** tab, select the Access Manager that will manage the unit.
4. Click **Unit type** and select **HID VertX**.

   If the unit type is greyed out, it means that the manufacturer extension is not added in the Access Manager.
5. Enter the IP address of the HID unit.

   NOTE: If there is a NAT router between the unit and its Access Manager, you must click on **More** and specify the NAT router's IP address that is visible from the unit.
6. Enter the **Username** and **Password**.

   NOTE: The default username/password is `root/pass`.
7. Click **Next**.
8. Select a **Partition** where the access control unit should be added.

   Partitions determine which Security Center users have access to this entity. Only accepted users of the partition can view or modify the access control unit.

   - If no partitions were created, select the default **Public partition**.
   - If there are partitions in your system, select the partition that will include the doors, schedules, rules, and cardholders linked to this specific door controller.
9. Click **Next**.
10. Review the *Creation summary*, and click **Create** > **Close.**

    The Access Manager attempts to connect to the unit and enrolls it in your system. Once the process has been successfully completed, a confirmation message appears.
11. Click **close**.

    The newly added access control unit appears under the Access Manager it was assigned to in the **Roles and units** view.

    NOTE: It might take a few minutes before the unit can be used, as it undergoes automatic synchronization. This process involves the Access Manager sending schedules, access rules, and cardholder information to the unit. The unit saves the information locally so that it can operate even if the Access Manager is unavailable.
12. To confirm that the unit successfully synchronized with Access Manager, do the following:

    a) From the **Roles and units** view, select the access control unit that was just added.

b) Click the **Synchronization** tab, and check the date and time of the **Last update.**

Configuring access control unit settings

For optimal performance, configure your access control unit settings after they have been added in Security Center.

What you should know

Security Center provides default settings; however, it is recommended that you carefully go through the configuration of each entity in order to get the best results.

HID and Synergis™ units have different capabilities, therefore different configuration requirements. For information about configuration requirements for Synergis™ units, see the *Synergis™ Appliance Configuration Guide*.

TIP: To save time configuring your access control units, you can configure one, and then copy the settings they have in common to the rest of the units.

To configure an access control unit's settings:

1. Open the **Access control** task, and click the **Roles and units** view.
2. Select the access control unit (HID or Synergis™) to configure, and click the **Properties** tab.
3. In the **Properties** tab, do one of the following:
   - Configure the properties of the HID unit.
   - Configure the properties of the Synergis™ unit.
4. Configure the wiring of entities controlled by this unit:
   - Configure the wiring of doors.
   - Configure the wiring of elevator floors.
   - Configure the wiring of hardware zones.
5. Click the **Peripherals** tab of the access control unit.

   This is where you configure the properties of the peripherals attached to the unit, such as the reader type and the input contact type. Validate your wiring configuration and give meaningful names to the devices if necessary.
   - Configure the peripherals attached to the HID unit.
   - Configure the peripherals attached to the Synergis™ unit.
6. (HID units only) Select the **Synchronization** tab, and choose how often you want to synchronize the unit:
   - **Automatically:** This is the recommended setting.

     Any configuration change is sent to the access control unit 15 seconds after the change is saved by the Config Tool, Web Client or Security Desk. Only configurations that affect that particular unit are sent.
   - **Daily:** The unit is synchronized daily, at the specified times.
   - **Every:** The unit is synchronized weekly, at the specified day and time.
   - **Manual:** The unit is only synchronized when you click **Synchronize now**.

     Make sure you synchronize the unit before the configuration expires.
7. Click **Apply**.

Automatic enrollment of access control units

Automatic enrollment is when new IP units on a network are automatically discovered by and added to Security Center. The role that is responsible for the units *broadcasts* a discovery request on a specific port, and the units listening on that port respond with a message that contains the connection information about themselves. The role then uses the information to configure the connection to the unit and enable communication.

The *Access Manager* role is able to automatically discover the Synergis™ appliances as access control units when the following conditions are met:

- The Synergis™ appliance has never been connected to any Access Manager before.
- The Synergis™ appliance and the Access Manager use the same discovery port.
- The Synergis™ appliance and the Access Manager are on the same network segment.
- The Synergis™ appliance is using the default logon username and password (`admin`/`softwire`).

HID units do not support automatic discovery.

When automatic discovery is not supported or does not work, use the *Unit enrollment tool* to find the units on your network and add them manually.

Enabling external access control devices

You can enable and disable external access control devices, such as USB readers, signature pads, card scanners, and so on, from the *Options* dialog box.

What you should know

These settings are saved locally for your Windows user profile. For information about the access control devices available, see your manufacturer documentation.

To enable or disable external access control devices:

1. From the home page, click **Options** > **External devices**.
2. Next to each external device, set the option **ON** or **OFF**.
3. Click **Save**.
4. Restart your Config Tool.

Related Topics

Using signature pads on page 550

30

Areas, doors, and elevators

This section includes the following topics:

About doors

A door is a type of entity that represents a physical barrier. Often, this is an actual door but it could also be a gate, a turnstile, or any other controllable barrier. Each door has two sides, named *In* and *Out* by default. Each side is an access point (entrance or exit) to a secured area.

There are three basic door configurations:

- Card in/Card Out - 2 *readers* are required
- Card In/REX Out - 1 reader is required
- Readerless doors - No readers are required

Readerless doors

If a reader is not required for a door configuration, the I/Os found on the interface modules (such as HID VertX V200 and V300) can be used to control the REX, door sensor, and lock. You do not need to link any access rules to a readerless door. However, you can still assign unlock schedules to readerless doors.

Some examples of where readerless doors might be used could include the following:

- Fire exits - Locked from the outside, with a push-bar to open the door from the inside using a REX.
- Stadiums/Theatres/Arenas - Everyone must enter through the ticket booth but once the event is finished, many exits become available to decrease congestion at the main entrance.

Door wiring

It is a best practice to have an electrician verify the functionality between all door sensors and actuators.

Door buzzers

You can assign an access control unit output to sound a buzzer from the door *Hardware* tab. The *Buzzer* does not refer to the reader’s beeper, but an external buzzer that is wired to an output relay on the access control unit. The buzzer output is triggered by the *Sound buzzer* and *Silence buzzeractions*.

Entry sensors

You can configure an entry sensor on each side of a door to increase the accuracy of people counting and the application of advanced access restriction rules on areas, such as antipassback and first-person-in rule. The system can only generate the *Entry detected* event when an entry sensor is triggered. In the absence of an entry sensor, the door sensor is used, and entry is assumed when the door sensor is triggered. If both types of sensors are absent, entry is assumed when an access is granted.

Two-person rule

You can protect a highly secured area with the *two-person rule*. The two-person rule is the access restriction placed on a door that requires two cardholders (including visitors) to present their credentials within a certain delay of each other in order to gain access.

NOTE: A visitor that requires an escort cannot be counted as one of the two people in the two-person rule.

TIP: A door can be configured in Security Center to protect a physical area (a room) without necessarily configuring a secured area if no other types of access restrictions need to be enforced.

Related Topics
About secured areas on page 523

Creating doors

Once the physical wiring between the access control unit and the door is complete, you can create and configure the door in Config Tool.

Before you begin

Wire your doors to access control units.

To create a door:

1. From the Config Tool home page, open the *Area view* task.
2. Select the area where you want to add the door.
3. Click **Add an entity** (➕) > **Door**.
4. In the **Creating a door** wizard, enter the door name and description.
5. From the **Location** drop-down list, select the area in which the door will be created, and click **Next**.
6. In the **Door information** page, assign names to the door sides.

   Example: In/Out, Secure/Non-secure, Entrance/Exit, East/West.
7. To associate the door with the access control unit it is wired to:
   a) From the **Access control unit** drop-down list, select a unit.
   b) From the **Interface module** drop-down list, select an interface module.
   c) From the **Type of door** drop-down list, select a door type.
8. Click **Next**.
9. Review the *Creation summary*, and click **Create** > **Close.**

   The new door appears in the area view’s *entity tree*.
10. Select the door and click the **Properties** tab.
11. Configure the general access control behavior of the door.
12. Click **Apply**.
13. Describe the wiring between the access control unit and the door to Security Center.
14. Select who has access to the door.

After you finish

Link the door to the areas it secures.

Related Topics
About doors on page 510

Mapping physical door wiring to door entities

For your door entity to be functional, you must match the hardware wiring you made to the door (reader connections, door locks, door sensors, REX's, buzzers, and so on) in Security Center, so the Access Manager knows how to control the door.

What you should know

The way you wire your door and assign the hardware interfaces affects how the door can be secured and monitored. For example, if the door has an entry sensor, you can monitor *Door forced open* events, and *Entry detected* events. If a door side is configured with a REX, access rule cannot be applied to that door side.

IMPORTANT: The door's hardware configuration must correspond to the I/O configurations you set for the access control unit controlling the door.

To map the physical wiring of a door to a door entity:

1. From the Config Tool home page, open the *Area view* task.
2. Select the door entity to configure, and click the **Hardware** tab.
3. From the **Preferred unit** drop-down list, select the access control unit that is connected to the door.
4. In the Door side (A) section, select the **Reader**, **REX**, and **Entry sensor** from the drop-down lists, based on the door wiring.
5. To change the door reader settings, click **Reader settings** (✎).

   The *Reader settings* dialog box lets you to set the following:

   - **Pin entry timeout:** For an HID unit, this sets the entry timeout for the first PIN digit after the card has been read, as well as the entry timeout for all subsequent PIN digits. For a Synergis™ unit, this only sets the entry timeout for the first PIN digit after the card has been read. The entry timeout for all subsequent PIN digits is fixed at 5 seconds.
   - **Use card and PIN:** Set to **ON** to change the reader mode to Card and PIN and select the schedule when this mode applies.

   NOTE: Make sure your settings match the capabilities of your reader. The system cannot validate the capabilities of your hardware. You can configure this type of reader in the unit's **Peripherals** tab.

6. Repeat the steps for door side (B).
7. In the *Additional connections* section, assign the inputs and outputs for the buzzer, door lock, and so on.
8. Click **Apply**.
9. Link cameras that display each side of the door to the door entity.

Example

If a physical door has the following installed, then the door entity must have a Card-In/REX out configuration in Config Tool:

- A reader wired on *door side* A
- A REX wired on door side B
- A strike relay on the door lock
- A door sensor
- An auxiliary relay wired to a buzzer

Related Topics

Access control unit - HID - Peripherals tab on page 785

Access control unit - Synergis™ - Peripherals tab on page 792

Linking cameras to doors

You can link cameras to door entities, so that when an access control event is triggered at the door (*door forced*, *access denied*), it causes the camera’s video feed to be displayed in a Security Desk monitoring tile and to be recorded.

Before you begin

To monitor doors with cameras, you must have one of the following Security Center configurations:

- An Archiver role with available cameras.
- An Omnicast™ Federation™ role to connect to an external Omnicast™ system.
- A Security Center Federation™ role to connect to an external Security Center system with cameras.

What you should know

If there are multiple cameras associated with a door, by default the cameras linked to side (A) of that door are displayed in a Security Desk tile. Multiple cameras associated with a single door (composite entities) can be cycled or unpacked in Security Desk.

To link cameras to a door:

1. From the Config Tool home page, open the *Area view* task.
2. Select the door entity to configure, and click the **Hardware** tab.
3. In the *Door side (In)* section, click **Associate a camera** (➕).
4. From the **Camera** drop-down list, select a camera.

   If the camera has a PTZ motor, you can also include the PTZ preset number to ensure that the camera points towards the door.

5. To add another camera to the door side, click **Associate a camera** (➕) again.
6. Repeat the steps for *Door side (Out)*.
7. Click **Apply**.

Selecting who has access to doors

A door that is wired to an access control unit is locked by default. You can set schedules for when *free access* (unlocked) through the door is permitted, and when *controlled access* (credentials must be presented to unlock the door) is in effect, by applying *access rules*.

Before you begin

- Describe the wiring between the access control unit and the door to Security Center.
- Create the access rules.

What you should know

If the door is configured as an access point to a secured area, all access rules assigned to the area are applied to the door. If additional access restrictions are enforced on the area, they are applied to the door as well.

To select who has access to a door:

1. From the Config Tool home page, open the *Area view* task.
2. Select the door entity, and click the **Unlock schedules** tab.
3. Under the *Unlock schedules* section, click **Add an item** (+).
4. Select the schedules that you want apply free access periods to, and click **Select**.

   Example: A typical use of an unlock schedule might be the following: The main door of the office should be unlocked from 9:00 AM-12:00 PM, locked from 12:00 PM - 1:00 PM, and unlocked again from 1:00 PM - 6:00 PM.
5. Under the *Exceptions to unlock schedules* section, click **Add an item** (+).
6. Select the schedules that you want to apply controlled access periods and access rules to, and click **Select**.
7. Click **Apply**, and then click the **Access rules** tab.

   BEST PRACTICE: If all the perimeter doors around the area share the same access rules, associate these access rules to the area instead of the doors.
8. In the **Door access applies to** option, select whether the access rules for the controlled access periods apply to **Both sides** of **Individual sides** of the door.

   NOTE: If the door is only configured with one reader, you can only configure access rules for the side where the reader is configured.
9. Under the *Access rules* section, click **Add an item** (+), select access rules and/or cardholders, and then click **OK**.

   If you assign cardholders or cardholder groups directly to the door, the cardholders are granted access all the time.
10. If the access rules are specific to each door side, then set access rules for the other door side.
11. Click **Apply**.

Related Topics

HID I/O linking considerations on page 960

About elevators

An elevator is a type of entity that provides access control properties to elevators. For an elevator, each floor is considered an access point.

When a cardholder uses a credential, the floor buttons to access those floors for which that cardholder is authorized, are enabled. This is achieved by controlling an output relay to enable the floor button.

Floor tracking is achieved by monitoring inputs, which records the floor buttons that are pressed. This permits tracking reports for elevator usage in the Security Desk.

Hardware required for elevator control and floor tracking

To control access to an elevator, you require the following:

- An *access control unit*.

  NOTE: Only Synergis™ units are supported for new installations.
- A reader in the elevator cab.
- Outputs that close relay contacts to enable the floor buttons.
- Inputs that record the floor buttons that have been selected (only necessary when floor tracking is required).
- *Interface modules* supplying or connecting the above hardware to the access control unit.

Reader modes

The following reader settings can be applied to the elevator cabin reader:

- Card only
- Card or PIN
- Card and PIN
- Card and PIN on a schedule

Elevator-wide settings

The following elevator-wide settings can be configured:

- **Grant time:** This value indicates for how long the elevator floor buttons stay enabled after the access has been granted.
- **Output relay state for free access:** There are two possible choices: (1) *Normal*, means floor access is enabled when the access control unit output relay is de-energized; (2) *Active*, means floor access is enabled when the access control unit output relay is energized.

Limitations

- An elevator (both the cabin reader and the I/Os) must be controlled by a single access control unit.
- *Antipassback*, *interlock*, and *people counting* do not work with elevators.
- Minimum *security clearance* cannot be enforced on elevators.

Related Topics

Differences between HID and Synergis™ units on elevator control on page 516

Differences between HID and Synergis™ units on elevator control

Both HID and Synergis™ units can be used for elevator control. However, due to HID's many limitations regarding elevator control, we only recommend Synergis™ units for new installations.

NOTE: If you need to replace a defective HID VertX V1000 unit that controls an elevator, we strongly recommend switching to Synergis™ units, especially if you have unlock schedules on your floors.

Supported features	HID units	Synergis™ units
Controller models / number of inputs / number of outputs	• HID VertX V2000 / 4 /6 • HID iClass Edge / 2 / 2 • HID VertX V1000 with • V100 / 4 / 4 • V200 / 2 / 18 • V300 / 12 / 4	Synergis™ unit requires *interface modules* for I/O: • HID VertX • V100 / 4 / 4 • V200 / 2 / 18 • V300 / 12 / 4 • Mercury • MR50 / 2 / 2 • MR52 / 8 / 6 • MR16IN / 16 / 2 • MR16OUT / 0 / 16 • STid readers Interface modules from different manufacturers can be mixed on the same unit.
Number of elevators per unit	One.	Up to 32. One Synergis™ unit can support up to 32 interface modules. So, one Synergis™ unit could support 32 elevators with 6 floors each (using 32 MR52), or 6 elevators with 60 floors each. This number will be less if you use floor tracking, since you need to replace output modules with input modules. With V100 and V300 modules, you get a little less, since they have less outputs per module.
Mixed use	An HID unit used to control an elevator cannot be used to control anything else.	A Synergis™ unit can be used to control elevators, doors, and zones, all at the same time.

Supported features	HID units	Synergis™ units
Reader types	- Wiegand - Clock & Data - Wiegand (Dorado) - Clock & Data (Dorado)	- Wiegand - Clock & Data - Wiegand (Dorado) - Clock & Data (Dorado) - STid smart card readers
Exception to access rules	Not supported.	Can be configured for the cabin reader and each individual floor.
Floor tracking	Only supported when the unit is online (connected to the Access Manager).	Supported even when the unit is offline (disconnected from the Access Manager).
Single floor selection per access grant	Not supported.	As soon as the cardholder selects a floor, and the Synergis™ unit receives the signal from the floor tracking input, all floor outputs return to controlled state.
Non-overlapping elevator grant time	Not supported. All floors released by the first card read stay released when a second card is read before the grant time expires.	Supported. A subsequent card read ends the current grant time on all floors released by the previous card read, regardless whether the previous cardholder selected a floor or not.
Different access schedules for different floors. Scenario: Bob is granted access to floor 1 from 9 am to 10 am through access rule 1, and to floor 2 from 10 am to 11 am through access rule 2.	Not supported. Schedules from different access rules applied to different floors are merged when the rules are granted to the same cardholder. In our sample scenario, Bob has access to both floor 1 and 2 from 9 am to 11 am.	Supported. Schedules from different access rules applied to different floors are kept separate. In our sample scenario, Bob can only access floor 1 from 9 am to 10 am, and floor 2 from 10 am to 11 am.

Creating elevators

To control access and monitor access control events related to elevators, you must create elevator entities in Security Center.

Before you begin

Make sure you have all the hardware required to control the elevator, installed the reader in the elevator cab, and wired the reader to the interface module connected to the access control unit.

To create an elevator:

1. From the Config Tool home page, open the *Area view* task.
2. Click **Add an entity** (➕) > **Elevator**.
3. In the elevator creation wizard, enter the elevator name and description.
4. From the **Location** drop-down list, select the area in which the elevator will be created, and click **Next**.

   NOTE: Unlike doors, elevators are not treated as *access points* to areas. Nevertheless, each elevator floor is an access point on its own.

5. Enter the number of elevator floors, and click **Create**.

   The default floor entities are created.
6. To change a floor name, select the floor, and enter a new name.
7. Make adjustments if necessary, and click **Next**.
8. Review the *Creation summary*, and click **Create** > **Close.**

   The new elevator appears in the area view with its floors. It initially appears in red until it is fully configured.
9. Select the output relay settings for the elevator floor.

   The output relay settings affect how you will wire the unit.
10. Describe the physical wiring between the access control unit and the elevator to Security Center.
11. Select who has access to the elevator floors.

Selecting output relay behavior for elevator floors

Before you can finish wiring your elevator, you must configure the unit output relay settings.

Before you begin

Create the elevator entity in Security Center.

What you should know

The output relay settings affect how you will wire the units. You must use the appropriate NO or NC relay contacts on the units, based on the settings you select in Security Center.

To select the output relay behavior for an elevator floor:

1. From the Config Tool home page, open the *Area view* task.
2. Select the elevator to configure, and click the **Advanced** tab.
3. In the **Grant time** option, select how long the elevator floor buttons stay enabled for after an access has been granted.
4. In the **Free access when the output relay is** option, select what the relay state must be for free access to be granted:
   - **Normal:** Floor access is enabled when the access control unit output relay is de-energized. This means that a power loss results in free access to the floor.
   - **Active:** Floor access is enabled when the access control unit output relay is energized. This mean that a power loss results in floor access being denied.
5. Click **Apply**.

After you finish

Finish wiring the elevator floors according to the relay settings you specified and map your wiring to the elevator entity.

Mapping physical elevator floor wiring to elevator entities

For your elevator entity to be functional, you must match the hardware wiring you made to the elevator in Security Center, so the Access Manager knows how to control the elevator.

To map the physical wiring of an elevator floor to an elevator entity:

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

2 Select the elevator entity to configure, and click the **Floors** tab.

3 From **Preferred unit** drop-down list, select an access control unit that is connected to the elevator cab reader.

4 From the **Elevator cabin reader** drop-down list, assign the reader input.

5 To change the elevator cab's reader settings, click **Reader settings** (✎).

The *Reader settings* dialog box lets you to set the following:

- **Pin entry timeout:** For an HID unit, this sets the entry timeout for the first PIN digit after the card has been read, as well as the entry timeout for all subsequent PIN digits. For a Synergis™ unit, this only sets the entry timeout for the first PIN digit after the card has been read. The entry timeout for all subsequent PIN digits is fixed at 5 seconds.
- **Use card and PIN:** Set to **ON** to change the reader mode to Card and PIN and select the schedule when this mode applies.

NOTE: Make sure your settings match the capabilities of your reader. The system cannot validate the capabilities of your hardware. You can configure this type of reader in the unit's **Peripherals** tab.

6 Under the **Floors** section, use the following buttons to add elevator floors or change their configuration:

- To add an elevator floor, click ➕.
- To delete the selected elevator floor, click ✖.
- To move the selected elevator floor up, click ▲.
- To move the selected elevator floor down, click ▼.
- To modify the selected elevator floor, click ✎.

The *Floor properties* dialog box lets you do the following:

- Change the floor name.
- Assign an output relay to the push button corresponding to that floor.

  Use the appropriate NO or NC relay contacts on the unit, according to output relay settings configured in the **Advanced** tab.

  NOTE: The output relay state can be inverted according to your regulatory requirements.
- (Optional) Assign an input for floor tracking.

NOTE: On an access control unit dedicated to elevator control, all inputs can be used for floor tracking except for the door monitor inputs.

7 Link cameras to the elevator cabin and to each elevator floor.

8 Click **Apply**.

Related Topics

Access control unit - HID - Peripherals tab on page 785

Access control unit - Synergis™ - Peripherals tab on page 792

Linking cameras to elevators

You can link cameras to elevator entities, so that when an access control event is triggered at the elevator (floor accessed, or access denied), it causes the camera's video feed to be displayed in a Security Desk monitoring tile. The video recording automatically starts for the floor accessed event.

Before you begin

To monitor elevators with cameras, you must have one of the following Security Center configurations:

- An Archiver role with available cameras.
- An Omnicast™ Federation™ role to connect to an external Omnicast™ system.
- A Security Center Federation™ role to connect to an external Security Center system with cameras.

To link cameras to an elevator:

1 From the Config Tool home page, open the *Area view* task.
2 Select the elevator entity to configure, and click the **Floors** tab.
3 In the *Cabin* section, click **Associate a camera** (✚).
4 From the **Camera** drop-down list, select a camera.

   If the camera has a PTZ motor, you can also include the PTZ preset number to ensure that the camera points towards the elevator.

5 To add another camera to the elevator, click **Associate a camera** (✚) again.
6 To link a camera to each elevator floor:
   a) In the **Floors** section, select a floor and click **Edit the item** (✎).
   b) In the **Floor properties** dialog box, click **Associate a camera** (✚).
   c) From the **Camera** drop-down list, select a camera.
   d) Click **OK**.
   e) Repeat the steps for all elevator floors.
7 Click **Apply**.

Selecting who has access to elevators

You can set schedules for when access to an elevator is controlled, and who can access the elevator with their credentials when access is controlled by applying *access rules*.

Before you begin

Create the access rules.

What you should know

Just like a door, elevator control requires access rules to determine *who* will be granted access, *where* and *when*. You can also assign unlock schedules to permit *free access* (no credentials required) during certain periods.

To select who has access to an elevator floor:

1. From the Config Tool home page, open the *Area view* task.
2. Select the elevator entity, and click the **Access** tab.
3. Under the *Access rules* section, click **Add an item** (✚).
4. Select the access rules to apply to the elevator, and click **Select**.

   The access rules determine which cardholders can access the elevator and when.
5. For each access rule, click the **Floor** drop-down list, and select which floor the access rule applies to.
6. Under the *Exceptions* section, click **Add an item** (✚).
7. Select the schedules that you want apply exceptions to, and click **Select**.
8. From the **Floor** column drop-down list, select which floors the exception applies to.
9. From the **Mode** column drop-down list, select whether the elevator has free access or controlled access during the exception schedule.
   - **Free access:** Cardholders do not require a credential to access the elevator, and no access rules apply.
   - **Controlled access:** Cardholders require a credential to access the elevator, and access rules apply.
10. Click **Apply**.

Related Topics
HID I/O linking considerations on page 960

Best practices for configuring exceptions to controlled access

Elevators are in controlled access mode by default. Therefore, the best practice is to start with an unlock schedule that tells when the elevator should be in free access mode (unlocked). Consequently, any non-selected time in the schedule sets the elevator in controlled access mode.

When schedules overlap, the controlled access schedules have priority over the unlock (free access) schedules. A controlled exception schedule is only useful if there is at least one unlock exception schedule.

About secured areas

A secured area is an area entity that represents a physical location where access is controlled. A secured area consists of perimeter doors (doors used to enter and exit the area) and access restrictions (rules governing the access to the area).

In the presence of a threat, access to secured areas can either be restricted (to keep the danger out) or relaxed (to allow people to get away from danger) by activating *threat levels*.

You can configure the following access restrictions on a secured area:

- Access rules
- Antipassback
- Interlock
- First-person-in rule
- Visitor escort rule

Access rights

The basic access restrictions to an area are defined by granting access to specific cardholders (who can access this area and when). When nothing is configured, no one is allowed to enter or exit the area. Access rights can be granted through access rules (recommended approach) if it is constrained by a schedule, or directly to cardholders, if there is no schedule constraint. Access rights can be granted on the entire area, or individually to each access point of the area.

Antipassback

Antipassback is an access restriction placed on a secured area that prevents a cardholder from entering an area that they have not yet exited from, and vice versa. When access is denied due to an antipassback violation, the violation must be "*forgiven*" in Security Desk for the cardholder to unlock the door. The antipassback event might be forgiven automatically after a period of time if it is configured with a timeout value.

NOTE: HID units support antipassback *or* interlock, but not both simultaneously.

Interlock

An interlock (also known as sally port or airlock) is an access restriction placed on a secured area that permits only one door to be open at any given time. This is typically used in a passageway with at least two doors. The cardholder unlocks the first door, enters the passageway, but cannot unlock the second door until the first door is closed.

For interlock logic to work, the door sensors must be able to detect when the door is opened.

NOTE: HID units support antipassback *or* interlock, but not both simultaneously.

First-person-in rule

The first-person-in rule is the additional access restriction placed on a secured area that prevents anyone from entering the area until a supervisor is on site. The restriction can be enforced when there is free access (on door unlock schedules) and when there is controlled access (on access rules).

- When enforced on door unlock schedules, the doors remain locked until a supervisor enters the area. Cardholders who have access can still enter the area. Once an unlock schedule is enabled, it remains in effect till the end of the current time interval defined in the schedule.

- When enforced on access rules, no one can enter the area even though they have valid credentials, until a supervisor enters the area. A schedule defines when the first-person-in rule applies. You can configure cardholders to be exempted from this constraint. An exempted cardholder can access the area without any supervisor being on site, but cannot clear the constraint for other cardholders.

  NOTE: The first-person-in rule schedule must define discrete time intervals to allow the constraint to be reset. The *Always* schedule cannot be used.
- To clear the first-person-in rule constraint, the supervisor must arrive within the time frame defined by the unlock schedule or the first-person-in rule schedule, up to a few minutes earlier, defined by the **On-site time offset** value. Once the constraint is cleared, normal access (free or controlled access) resumes till the end of the current time interval defined in the schedule.

  If the unlock schedule or the first-person-in rule schedule comprises several time intervals, then the supervisor must re-enter the area at the beginning of each time interval to clear the constraint.

NOTE: The *first-person-in rule* only works on areas controlled by a single Synergis™ unit. HID units do not support this feature. The *first-person-in rule* works best when the doors are equipped with entry sensors or door sensors. A Synergis™ unit is capable of differentiating between *No entry*, *Entry assumed*, and *Entry detected*. When no sensor is configured for a door, entry is assumed when access is granted.

Visitor escort rule

The visitor escort rule is the additional access restriction placed on a secured area that requires visitors to be escorted by a cardholder during their stay. Visitors who have an escort are not granted access through access points until both they and their assigned escort (cardholder) present their credentials within a certain delay. The escort must present their credential after the visitors before access is granted to both. If multiple visitors are accompanied by the same escort, the escort only needs to present their credential once all visitors have presented their credentials.

NOTE: HID units do not support the visitor escort rule.

Configuring secured areas

To set up an access control system with access rules and access control behavior, you must configure your areas as secured areas.

Before you begin

Create the areas that will represent your secured areas.

To configure a secured area:

1. From the Config Tool home page, open the *Area view* task.
2. Select the area entity ( ) you want to configure and click the **Identity** tab.
3. Click **Access control** to turn the option **ON**, and then click **Apply**.

   Two new tabs, **Properties** and **Advanced**, appear and the associated icon is updated to show that this is now a secured area ( ).
4. Click the **Properties** tab, and set the following:
   - **Access rules:** Define which cardholders are allowed to access (enter or exit) the area, and when by assigning access rules to the area. You can also assign cardholders or cardholder groups directly to the area, in which case, the cardholders are granted access all the time.
   - **Doors:** Link the doors that are used to enter and exit the area (perimeter doors) as well as the ones that are captive. Captive doors are necessary for the proper tracking of *people counting* and *antipassback*.

   NOTE: Access rules assigned to the area apply to all perimeter doors of the area. If each perimeter door must be governed by its own set of rules, configure the access rules on each door.
5. Click the **Advanced** tab, and set the following:
   - **Antipassback:** Access restriction placed on a secured area that prevents the same cardholder from entering an area they have not yet exited, and vice versa.
   - **Interlock:** Logic that only allows one perimeter door to be open at a time.
   - **First-person-in rule:** Unlock schedule is not triggered or regular access is disabled until a supervisor is present in the area.
   - **Visitor escort rule:** Visitors must be accompanied by their designated escort (cardholder) in order to enter the area.
6. Click **Apply**.

Related Topics

About secured areas on page 523

Adding doors to areas

To make sure an area is secure, add the doors to the area in Config Tool.

Before you begin

Create the areas that you want to link doors to.

What you should know

Doors that are members of an area can be configured as *Captive* or *Perimeter* doors. Perimeter doors are used to enter and exit an area, and help to control access. Captive doors are doors that are used within the area. Set the *door sides* correctly to ensure that *People counting* and *antipassback* are properly tracked. A door's *Entrance* and *Exit* sides are relative to the area being configured.

NOTE: Access rules configured for an area only apply to perimeter doors. All rules that deny access take precedence over the rules that grant access.

To add a door to an area:

1. From the Config Tool home page, open the *Area view* task.
2. Select an area and then click the **Properties** tab.
3. Under the *Doors* section, click **Add an item** (➕) and select the doors you want to link to your area.
4. For all doors in the **Doors** section, do the following:
   - If the door is used to enter or exit the area, set the slider to **Perimeter**.
   - If the door is located inside the area, set the slider to **Captive**.

     NOTE: If a smaller area is nested inside a larger area, you do not need to add the perimeter doors of the smaller area as captive doors of the larger area. The system automatically takes care of the logic of nested areas when calculating people counts and applying antipassback rules.
   - To swap the door sides, click **Swap door side** while the door is selected.
5. Click **Apply**.

After you finish

To control access to your secured area, apply access rules to the area.

Applying antipassback to areas

Once your area is created and it contains at least one perimeter door, you can apply antipassback to prevent cardholders from entering areas they have not yet exited, and vice versa.

Before you begin

Create and configure a secured area to apply the antipassback restriction to.

What you should know

An area enabled with antipassback must be controlled by a single unit. If the area is not controlled by a single unit, the following criteria must be met in order to apply antipassback.

- All units controlling the doors within the area are Synergis™ units.
- All units controlling the area are managed by the same Access Manager role.
- Global antipassback is enabled on the Access Manager role.

Limitations: For areas controlled by HID units, the antipassback logic is only applied to perimeter doors, not to captive doors.

To configure antipassback for an area:

1 From the Config Tool home page, open the *Area view* task.
2 Select the secured area, and click the **Advanced** tab.
3 Set **Antipassback** to **ON**.
4 If the doors are controlled by an HID unit, set **Interlock** to **OFF**.
5 Set the following:
   - **Schedule:** Select *Always* if you want antipassback to be applied at all times.
   - **Type:** Type of antipassback to apply.
     - **Soft:** Soft antipassback only logs the passback events in the database. It does not restrict the door from being unlocked due to a passback event.
     - **Hard:** Hard antipassback logs an entry in the database and prevents the door from being unlocked due to a passback event.
   - **Presence timeout:** Set how many minutes a cardholder’s presence in the area is remembered for the purpose of passback detection (not used for counting people). Past that period, a cardholder who never left the area can re-enter without triggering a passback event. The default value of zero (0) minutes means that a cardholder's presence never times out.

     NOTE: When global antipassback is enabled, the presence of a cardholder in an area is forgotten after seven days if no entry or exit from this area is reported for that cardholder during that period. This means that cardholders can re-enter an area that they never left, or leave an area they never entered, without triggering a passback event if no movement was registered for these cardholders on that area for seven days. This applies even if the **Presence timeout** is set to infinite (=0).
   - **Strict:** Turn this option on to generate passback events for both types of access violations: when cardholders try to re-enter an area that they never left, and when cardholders try to exit an area that they never entered. Otherwise, the default is set to **OFF** and antipassback logic is only verified on area entrances, and passback events are only generated when cardholders try to re-enter an area that they never left.

     BEST PRACTICE: If you choose to enable *strict* and *hard* antipassback on an area that is not controlled with turnstiles or similar devices that only allow one person through at a time, grant the *Forgive antipassback violation* privilege to the operators responsible for monitoring this area.

     NOTE: With strict antipassback turned off, you can have Card-In/REX-out perimeter doors, but the **Presence timeout** parameter must be configured (> 0). With strict antipassback turned on, all perimeter doors must be configured as Card-In/Card-Out, **Presence timeout** must be set to infinite (= 0), and no REX can be configured.

6 Click **Apply**.

Related Topics
About secured areas on page 523
About access control units on page 499

Enabling global antipassback on Access Manager roles

If the areas on which you want to apply the antipassback restrictions are controlled by multiple Synergis™ units, you must enable global antipassback on the Access Manager roles.

What you should know

When *strict* and *hard* antipassback is applied to an area without global antipassback, a cardholder who entered the area through one door cannot leave the area through another door if both doors are not controlled by the same unit. Also, the same cardholder who entered the area through one door, can re-enter the area through a different door if the two doors are not controlled by the same unit. With global antipassback enabled, these two violations can be prevented.

IMPORTANT: Global antipassback only works on areas that are entirely controlled by Synergis™ units. All units controlling the same area must be managed by the same Access Manager.

TIP: If you need to switch your units between Access Manager roles to meet the global antipassback requirements, use the Move unit tool.

To enable global antipassback on an Access Manager role:

1 From the Config Tool home page, open the *Access control* task, and click the **Roles and units** view.
2 Select the Access Manager role to configure, and click the **Properties** tab.
3 On the *Properties* page, select the following options: **Enable peer to peer** and **Enable global antipassback**.
4 Click **Apply**.

Interlocking doors within areas

Once your area is created and it contains at least two perimeter doors, you can apply an interlock logic to it so that only one door can be open at a time.

Before you begin

Do the following:

- Create and configure a secured area to apply the interlocking logic to.
- Link at least two perimeter doors to your area.

What you should know

For interlock logic to work, the door sensors must be able to detect when the door is opened.

To interlock the perimeter doors of an area:

1. From the Config Tool home page, open the *Area view* task.
2. Select the secured area, and click the **Advanced** tab.
3. Set **Interlock** to **ON**.

   When set to ON, only one perimeter door of the area can be open at any given time. To open a door, all others must be closed.
4. If the door is controlled by an HID unit, set **Antipassback** to **OFF**.
5. Set the following:
   - **Override:** Select the input that is wired to the *override* key switch or flip switch. When the switch in on, the interlock feature is disabled.
   - **Lockdown:** Select the input that is wired to the *lockdown* key switch or flip switch. When the switch is on, all perimeter doors remain locked until the switch is back to its normal position.
   - **Priority:** When both the *override* and *lockdown* inputs are configured, select which one has priority when both inputs are active.
6. Click **Apply**.

Related Topics

About secured areas on page 523

Enforcing a supervisory presence on secured areas

You can keep a secured area locked until a supervisor shows up, by enforcing the *first-person-in* rule on the area.

Before you begin

Create and configure a secured area to enforce the first-person-in rule to.

What you should know

The *first-person-in rule* only works on areas controlled by a single Synergis™ unit. HID units do not support this feature.

To ensure a supervisor is on site before granting access to an area:

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

2 Select the secured area, and click the **Advanced** tab.

3 In the *First-person-in rule* section, do the following:

- To ignore the door unlock schedules when no supervisor is present, set the **Enforce on doors unlock schedules** option to **ON.**
- To ignore the access rules when no supervisor is present, set the **Enforce on access rules** option to **ON**, and then select the schedule to dictate when the first-person-in rule applies.

4 Click the **On-site time offset** to grant more freedom to the time the supervisor must show up to clear the first-person-in rule constraint.

If the time offset is set to zero, the supervisor cannot show up earlier than the start of the access schedule, or else their arrival would be ignored.

5 Under the **Supervisors** list, click **Add an item** (✚), and then select the cardholder groups and cardholders to designate them as supervisors of the area.

You must configure at least one supervisor. Only one supervisor needs to be present in the area to satisfy the first-person-in rule constraint.

6 (Optional) Under the **Exemption list**, click **Add an item** (✚), and then select the cardholder groups and cardholders to whom the first-person-in rule does not apply.

Access is granted to those cardholders solely based on the access rules. A supervisor does not need to be present to grant them access to the area.

7 Click **Apply**.

Related Topics

About secured areas on page 523

Requiring visitors to be escorted to access secured areas

You can increase the security of certain areas by requiring visitors to be accompanied by a designated escort. The escort must present their credential after the visitor within a certain delay before access is granted to both.

Before you begin

Do the following:

- Create and configure a secured area to enforce the visitor escort rule to.
- Link at least one perimeter door to your area.

To require a visitor to be escorted to access an area:

1. From the Config Tool home page, open the *Area view* task.
2. Select the secured area, and click the **Advanced** tab.
3. In the **Visitor escort rule** section, do one of the following:
   - Set the **Enforce visitor escort rule** option to **ON**.
   - Click **Revert to inherited value** (⬆) if the parent area has visitor escort rule enforced.
4. Click **Apply**.
5. Select the **Properties** tab.
6. (Optional) For all perimeter doors configured for this area:
   a) Select door and click **Jump to** (➜).
   b) Select the door’s **Properties** tab.
   c) Set the **Maximum delay between card presentations** in seconds.

      Access would be denied if the escort does not present their credential within the specified delay after the visitor.

   d) Click **Apply**.

After you finish

When you check-in visitors who need supervised access to this area, assign a host (cardholder or cardholder group who has access to this area) to the visitor, and select **Escort required**.

Related Topics
About secured areas on page 523

About access rules

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

An access rule contains the three W's:

- Who? (Who can pass through - *cardholders* or *cardholder groups*)
- What? (Whether access is granted or denied)
- When? (The *schedule* when the access rule is applied)

This logic is different from other access control solutions, where an access level defines *where* and *when* someone can gain access.

Access rules that have been pushed to the *door controllers* do not have to be modified. If you associate a new credential with a cardholder, the old rule is still valid.

Related Topics
About Synergis™ on page 487

Creating access rules

To control access anywhere on your site, you must create access rules that will apply to the areas, doors, and elevators.

Before you begin

Create the schedules that will apply to this access rule.

What you should know

As a best practice, use a descriptive name when creating new access rules so you can easily determine what each rule does (for example, "*Lab Technicians Only*", "All Employees Regular Hours").

To create an access rule:

1. From the Config Tool home page, open the *Access control* task, and click the **Access rules** view.
2. Click **Access rule** (✚).
3. Assign a name and description to the access rule.
4. In the **Partition** drop-down list, select the partition in which the access rule will be created, and click **Next**.
5. Select a schedule of when you want your rule to be active. The default is **Always**.
6. Click **Next.**
7. Review the *Creation summary*, and click **Create** > **Close.**
8. Select the access rule, and click the **Properties** tab.
9. Select a schedule, and select whether to **grant access** or **deny access** during that schedule.

   BEST PRACTICE: Usually schedules are used to grant access. Access is denied when schedules are inactive. Use explicit **deny** schedules only for exceptions.

10. Under the *Cardholders affected by this rule* section, click **Add an item** (✚), select the cardholders or cardholder groups the access rule applies to, and then click **Add**.

    BEST PRACTICE:

    Create cardholder groups instead of individual cardholders, as this becomes much more manageable in large systems as more people come and go.

11. Click **Apply**.

After you finish

Assign the access rule to secured areas, doors, and elevators so the access rule is operational.

31

Cardholders

This section includes the following topics:

About cardholders

A cardholder is a type of entity that represents a person who can enter and exit secured areas by virtue of their credentials (typically access cards) and whose activities can be tracked. They are the *Who* in an access rule.

Cardholder groups

The *cardholder group* entity is used to configure the common *access rights* and properties of a group of cardholders.

If you have a large access control system, cardholders and access rules are much easier to manage when cardholders are members of cardholder groups.

Creating cardholder groups

To configure the access rights and properties that are common to a group of cardholders, you can create cardholder groups.

What you should know

If you have a large access control system, cardholders and access rules are much easier to manage when cardholders are members of cardholder groups.

To create a cardholder group:

1. Open the **Access control** task, and click the **Cardholder groups** view.
2. Click **Cardholder group** (➕).

   A new cardholder group appears in the entity tree.
3. Type a name for the group, and press **ENTER**.
4. Select the cardholder group, click the **Properties** tab.
5. At the bottom of the page, click ➕ to add individual cardholders or cardholder groups to your new group.
6. Click **Apply**.

Creating cardholders

To add new employees who must enter and exit secured areas using access cards, and to track their activities, you can create cardholders using the *Cardholder management* task.

Before you begin

- To add custom information to cardholders, create custom fields.
- If you require different groups of cardholders with different access rights, create cardholder groups.

What you should know

Instead of creating cardholders manually, you can import them from a CSV file, or from your company's Active Directory.

To create a cardholder:

1. Open the **Cardholder management** task, and click **Create new cardholder** (✚).
2. At the top of the dialog box, enter the cardholder's first name, last name, and e-mail address.
3. To assign a picture to the cardholder, click the silhouette and select one of the following options:
   - **Load from file:** Select a picture from disk. All standard image formats are supported.
   - **Load from webcam:** Take a snapshot with your webcam. This option appears only if you have a webcam attached to your workstation.
   - **Load from camera:** Take a snapshot from a camera managed by Security Center. When you click **Load from camera**, a separate capture dialog box opens. Select the video source, and click **Take snapshot** (▣).
   - **Load from clipboard:** Load the picture copied to the clipboard. This option appears only if you used the Windows copy command to save a picture onto your clipboard.
4. To edit the picture, click it to open the *Image editor* and use the editing options at the top of the editor's dialog box.
5. In the *Status* section, set the following:
   - **Status:** Set the their status to *Active* or *Inactive*. For their credential to work, and for them have access to any area, their status must be *Active*.
   - **Activation:** If their status is currently set to *Inactive*, set a date and time to activate their profile.
   - **Expiration:** Set an expiration for their profile:
     - **Never:** Never expires.
     - **Specific date:** Expires on a specific date and time.
     - **Set expiration on first use:** Expires after a specified number of days after the first use.
     - **When not used:** Expires when it has not been used for a specified number of days.
6. Assign a credential to the cardholder so they can access secured areas.

   NOTE: You can assign a credential now or after all credentials have been enrolled in the system.
7. Assign the cardholder to a *cardholder group*.

   NOTE: A cardholder can belong to more than one cardholder group.

   a) To assign the first cardholder group, click the **Cardholder group** drop-down list and select a cardholder group.

   b) To assign additional cardholder groups, click **Advanced** (⊕), then click **Add and item** (✚). In the dialog box that appears, select the cardholder groups, and click **OK**.

8 Enter the cardholder’s e-mail address.

9 (Optional) If custom fields are defined for cardholders, such as department, phone numbers, and so on, enter the additional cardholder information.

10 (Optional) In the *Advanced* section, configure the following cardholder properties:

NOTE: Some of these properties can be inherited from the parent cardholder groups. When a specific value is configured for the cardholder, click **Revert to inherited value** (⬆) to inherit the property from the parent cardholder groups. If multiple parent groups exist, the most privileged value is inherited.

a) If the cardholder has been assigned a credential, grant access privileges to the cardholder:

- **Use extended grant time:** Grants them more time to pass through doors where the *Extended grant time* parameter is configured for a door. Use this option for those with reduced mobility.
- **Bypass antipassback rules:** Exempts them from all antipassback restrictions.

b) In the **Security clearance** field, enter the cardholder’s security clearance level. The security clearance level determines their access to areas when a threat level is set in Security Center. Level 0 is the highest clearance level, with the most privileges.

c) In the **Entity name** field, type a name for the cardholder entity, if you do not want to use the cardholder’s name.

By default, the **Entity name** uses the **First name** and **Last name** fields.

d) In the **Description** field, type a description for the cardholder.

e) Assign the cardholder to a *partition*.

Partitions determine which Security Center users have access to this entity. Only accepted users of the partition can view or modify the cardholder.

11 Click **Save**.

After you finish

Assign access rules to the cardholder.

Related Topics

Cropping pictures on page 540
Applying transparent backgrounds to pictures on page 541
Creating doors on page 511
Configuring secured areas on page 525

Assigning access rules to cardholders

To grant or deny a cardholder access to *areas*, *doors*, and *elevators*, you must assign *access rules* to them.

Before you begin

Create access rules.

What you should know

You can assign access rules while you are creating new cardholders, or after they are created. In this procedure, it is assumed you have already created a cardholder.

BEST PRACTICE: Assign access rules to cardholder groups, rather than to individual cardholders. Assign access rules to individual cardholders only as a temporary measure. When used too often, the access control system can quickly become unmanageable.

To assign access rules to a cardholder:

1 In the **Cardholder management** task, select a cardholder, and then click **Modify** (✎).

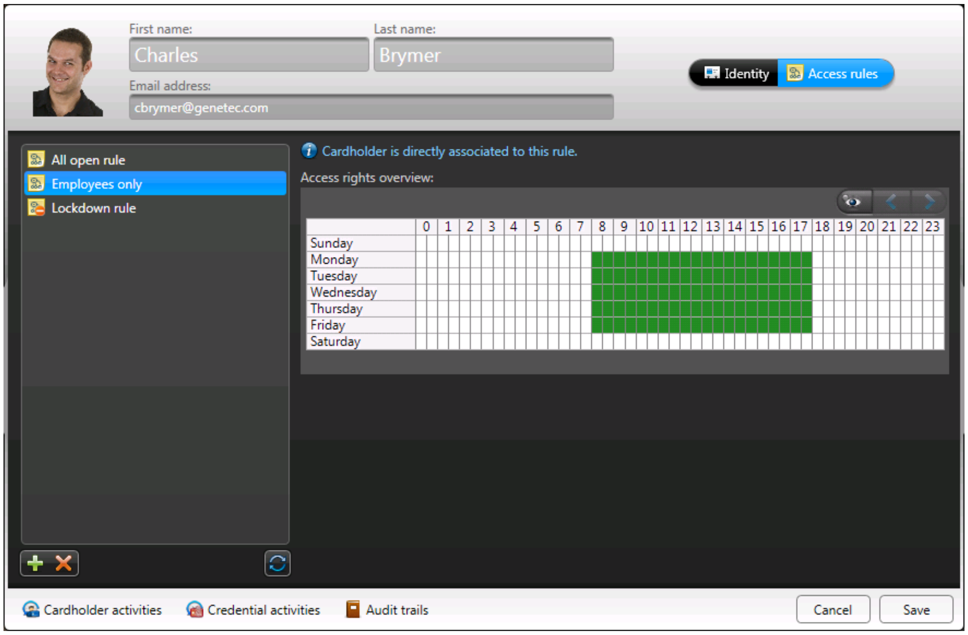
2 Click the **Access rules** (▨) tab > **Add** (+).

A dialog box that lists all access rules in the system opens.

3 Select the rule you want to add, and click **Add**.

4 Select the access rule from the list.

The schedule that applies to the access rule is shown in a grid on the right. Green areas indicate periods when access is granted by the rule. Red areas indicate periods when access is denied by the rule. White areas are times not specified by the schedule; therefore, access is denied.



First name: Charles

Last name: Brymer

Email address: cbrymer@genetec.com

- All open rule
- Employees only
- Lockdown rule

Cardholder is directly associated to this rule.

Access rights overview:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday																								
Monday									🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩						
Tuesday									🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩						
Wednesday									🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩						
Thursday									🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩						
Friday									🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩						
Saturday																								

5 To view the access rule schedule in minutes, click 👁.

Use the arrow buttons to scroll left or right.

6 To assign another access rule to the cardholder, click ✚.

7 To remove an access rule directly assigned to the cardholder, click ✖.

You cannot remove the *All open rule*, or the *Lockdown rule*.

8 Click **Save**.

After you finish

Assign a credential to the cardholder.

Cropping pictures

To cut out an area of a cardholder or visitor's picture and focus on the part of the image that you would like to keep, you can crop the picture using the *Image editor*.

To crop a picture:

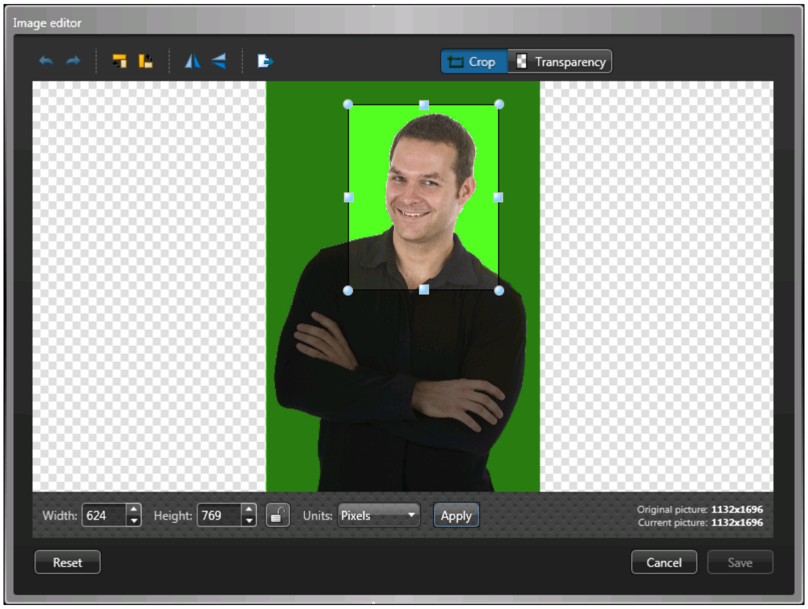
1 Click the picture.

2 In the *Image editor*, click the **Crop** () tab.

3 On the image, click and drag the icon to crop the picture.

4 To adjust the crop area, do one of the following:

- Use the blue icons on the image to adjust the crop area.
- At the bottom of the *Image editor* dialog box, use the **Width** and **Height** values to resize the crop area. The width and height values can be in pixels, inches, or millimeters.



Width: 624 Height: 769 Units: Pixels

Original picture: 1132x1696
Current picture: 1132x1696

5 To revert the picture to its original state, click **Reset**.

6 Click **Apply**.

Applying transparent backgrounds to pictures

If a cardholder or visitor's picture was taken in front of a chroma key screen, you can make the picture background transparent. This is helpful if you create a badge template that has an image in the background.

What you should know

You can also set the transparency and color for backgrounds of cardholder pictures in the Import tool, so you can use the same settings while importing multiple cardholder pictures.

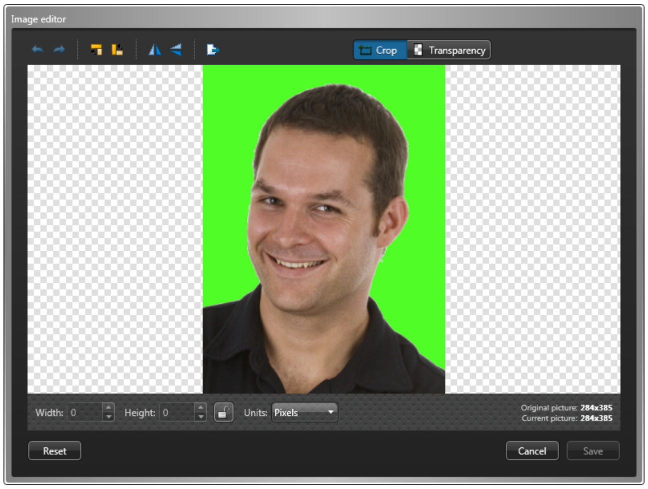
To apply a transparent background to a picture:

1 Click the picture.

2 In the *Image editor*, click the ***Transparency*** tab.

The cursor changes to the eyedropper tool when you point to the image.

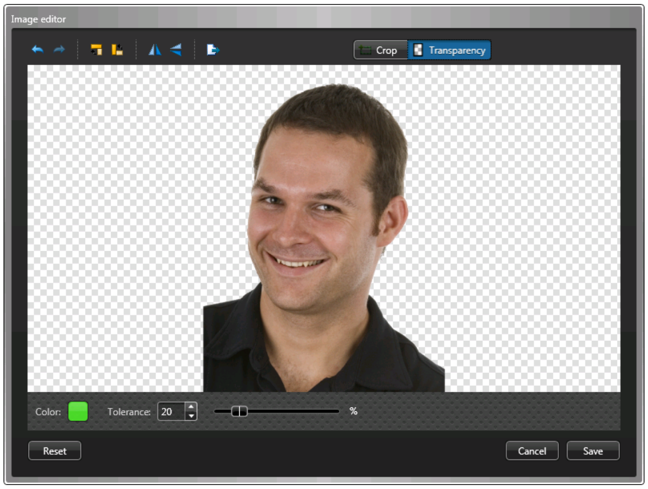
3 Click the background where the chroma color is (usually green or blue).



Width: 0 Height: 0 Units: Pixels

Original picture: 284x385
Current picture: 284x385

4 Using the **Tolerance** slider, adjust the transparency percentage.



Color: 🟩 Tolerance: 20

5 To revert the picture to its original state, click **Reset**.

6 Click **Save**.

Defining the maximum file size of pictures

To save disk space, you can set the maximum file size for pictures that are stored in the Directory database.

What you should know

The maximum file size applies to cardholder pictures, and when you are importing cardholders using the *Import tool*. When loading image files, Security Center automatically reduces the image size so that their file size is under the limit you set.

The default value is 20 KB. You can set the limit anywhere between 20 and 5000 KB.

To define the maximum file size of pictures:

1 Open the *Access control* task, and click the **General settings** view.

2 In the **Maximum picture file size** option, set the maximum number of kilobytes.

3 Click **Apply**.

Assigning credentials

To grant cardholders or visitors access to secured areas, you must assign them credentials.

What you should know

Cardholders and visitors can be assigned multiple *credentials*. You can assign credentials while you are creating a new cardholder or visitor, or after they are created. In this procedure, it is assumed you have already created them.

To assign credentials:

1 Do one of the following:

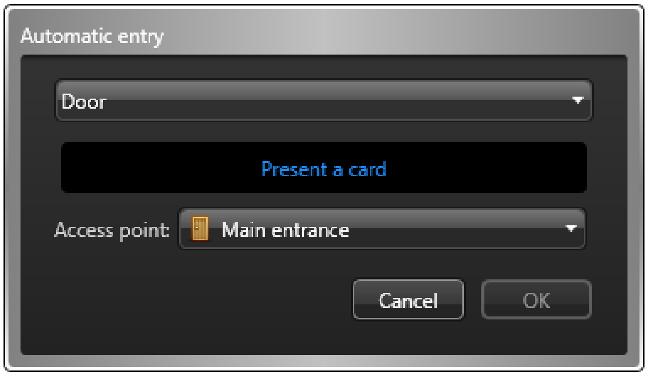
- For cardholders, open the **Cardholder management** task, select a cardholder, and then click **Modify** (✏).
- For visitors, open the **Visitor management** task, select a visitor, and then click **Modify** (✏).

2 In the *Credential* section, click **Add a credential** (➕).

3 Select one of the following options:

- **Automatic entry:** Present the card at a reader.
- **Manual entry:** Manually enter the card data. Use this method when you do not have a card reader near you.
- **Existing credential:** Select a pre-enrolled, unassigned credential.
- **PIN:** Create a PIN credential.
- **Request card:** Request a credential card for the cardholder or visitor. Use this method if you do not have a printer on site.
- **Paper credential (print):** Print a badge (name tag or photo ID card) without assigning a credential. The paper credential cannot be used to open doors. It is only used to visually identify the cardholder or visitor.

4 If you select **Automatic entry**, then select a reader (USB reader or a door), and present the card at the reader.

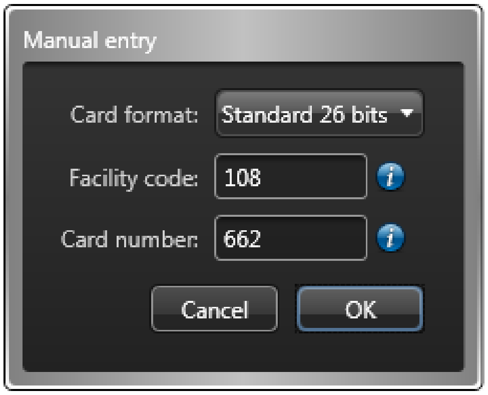


Door

Access point: Main entrance

The dialog box closes automatically after an eligible card is presented. If the card has not been enrolled, it is enrolled automatically. If it was already assigned to someone, it is rejected.

5 If you select **Manual entry**, then select a card format, enter the required data fields, and click **OK**.



Manual entry

Card format: Standard 26 bits

Facility code: 108

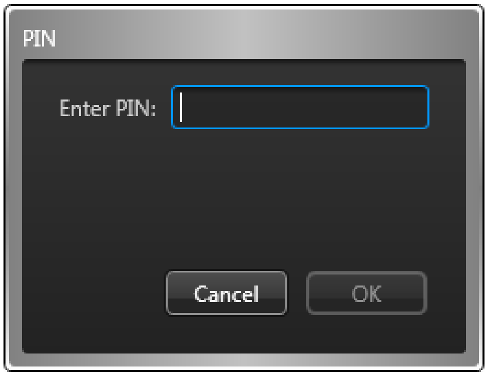
Card number: 662

If the card has not been enrolled, it is enrolled automatically. If it was already assigned to someone, it is rejected.

CAUTION: Be careful when you enter the card data, because the system cannot validate whether the data you entered correspond to a physical card or not.

6 If you select **Existing credential**, a dialog box listing all existing but unassigned credentials in the system appears. Select an unassigned credential from the list, and click **OK**.

7 If you select **PIN**, then do the following:



PIN

Enter PIN:

a) Enter the PIN as a numerical value.

NOTE: Be careful not to exceed the number of digits accepted by your readers. A typical PIN length is five digits. But certain models accept up to 15 digits.

b) Click **OK**.

8 After the credential is assigned, it appears in the *Credential* section.

The credential name and status are displayed. *Active* indicates the credential is assigned.

NOTE: If the credential is a PIN, the keypad icon is displayed. If the credential is a card, a default *badge template* is assigned, and a print preview of the badge is displayed instead of the credential icon.

9 (Optional) If the credential is a card, select a different badge template as follows.

a) In the *Credential* section, click the badge image.

b) Select a badge template, and then click **OK**.

A print preview of the badge appears, with data corresponding to the current cardholder or visitor and their credential.

10 Click **Save**.

You must save all your changes before you can print the badge.

11 To print the badge, click **Print badge** next to the badge preview.

Related Topics

Designing badge templates on page 573

Requesting credential cards

When you are not in possession of the credential cards, you can request the credential cards to be assigned to the cardholders and visitors you are managing by someone else.

What you should know

You can request a card while you are creating a new cardholder or visitor, or after they are created. In this procedure, it is assumed you have already created a cardholder or visitor.

NOTE: You can only manage visitors in Security Desk.

To request a credential card:

1. Do one of the following:
   - For cardholders, open the **Cardholder management** task, select a cardholder, and then click **Modify** (✏).
   - For visitors, open the **Visitor management** task, select a visitor, and then click **Modify** (✏).
2. In the *Credential* section, click **Add a credential** (➕).
3. From the drop-down menu, click **Request card**.
4. In the **Request card** dialog box, select the reason why you are requesting a card.

   NOTE: Card request reasons only appear if your administrator has created possible reasons in Config Tool.
5. From the **Badge template** drop-down list, select a badge template.

   You only need to select a badge template if you want a badge to be printed.

   A print preview of the badge appears.
6. In the **Activate** option, select when to activate the credential.
   - **Never:** The credential will never be activated.
   - **After enrollment:** After another user responded to the card request.
   - **On:** Select a specific date to activate the credential.
7. If you want to receive an email when the credential has been printed, select the **Email me when the card is ready** option.

   NOTE: For this option to work, your user must have a valid email address.
8. Click **OK**.

   The credential is shown as **Requested** in the *Credential* section of the cardholder or visitor details window.
9. Click **Save**.

The **Card requests** (💳1) icon appears in the notification tray.

Related Topics

Designing badge templates on page 573
Adding reasons for credential card requests on page 564
Responding to credential card requests on page 565

Printing paper credentials

When you do not have credentials assigned to cardholders or visitors, you can print paper credentials (badges without credential data) as name tags or photo IDs for visual identification.

Before you begin

Add a badge template.

What you should know

To print a badge, you need a badge template. A badge template is generally associated to a card credential so that it can be used to unlock doors, but you can also print a badge without any credential data (called a paper credential) that can be used as a name tag or a photo ID for visual identification.

You can print a badge while you are creating a new cardholder or visitor, or after they are created. It is assumed the cardholder or visitor is already created.

NOTE: You can only manage visitors in Security Desk.

To print a badge:

1. Do one of the following:
   - For cardholders, open the **Cardholder management** task, select a cardholder, and then click **Modify** (✏).
   - For visitors, open the **Visitor management** task, select a visitor, and then click **Modify** (✏).
2. In the *Credential* section, click **Add a credential** (➕).
3. In the menu that appears, click **Paper credential (print)**.

   The **Badge printing** dialog box appears.
4. From the drop-down list, select a badge template.

   A print preview of the badge is shown. Cardholder or visitor information might be shown on the badge, depending on how the badge template is designed. No credential data is shown on the badge.
5. To print the paper credential, click **Print badge**.

Related Topics
Designing badge templates on page 573

Modifications to cardholders imported from an Active Directory

If you have cardholders that are imported from an Active Directory, there are a few cardholder properties that you can modify in Security Center.

You can make the following modifications:

- Assign pictures to imported cardholders.
- Assign temporary cards to imported cardholders.
- Modify the status of imported cardholders.

Temporary cards for imported cardholders

If an imported cardholder forgets or loses their card, you can assign them a temporary card in the *Cardholder management* task. When you assign them a temporary card, their credential becomes greyed out in Config Tool until the card is returned. For more information about assigning or returning temporary cards, see the *Security Desk User Guide*.

Assigning pictures to imported cardholders

You can assign pictures to imported cardholders from Security Center, and then synchronize the pictures with the Active Directory.

Before you begin

The cardholder *Picture* field must be mapped to the AD attribute *thumbnailPhoto*.

To assign a picture to an imported cardholder:

1. From the **Cardholder management** task, assign a picture to the cardholder.
2. Open the **System** task, and click the **Roles** view.
3. Select the Active Directory role, and then click the **Links** tab.
4. Select the **Upload pictures to Active Directory** option, and set the **Maximum uploaded picture file size** (default=20 KB).
5. Click **Apply**.
6. Click the **Properties** tab, and then click **Synchronize now**.

   NOTE: If Security Center synchronizes with the AD based on a scheduled task, then the next time the synchronization occurs, the new cardholder picture is synchronized with the AD.

Modifying the status of imported cardholders

You can modify the status and expiration date of an imported cardholder in Security Center. The cardholder becomes desynchronized from the AD.

To modify the status of an imported cardholder:

1. Open the **Access control** task.
2. Select an imported cardholder (👤), and click the **Properties** tab.
3. In the **Status** section, move the slider from **Keep synchronized** to **Override**.
4. Set the cardholder’s status and expiration date:

- **Status:** Set the their status to *Active* or *Inactive*. For their credential to work, and for them have access to any area, their status must be *Active*.
- **Activation:** Displays the current date.
- **Expiration:** Set an expiration for their profile:
  - **Never:** Never expires.
  - **Specific date:** Expires on a specific date and time.
  - **Set expiration on first use:** Expires after a specified number of days after the first use.
  - **When not used:** Expires when it has not been used for a specified number of days.

5 Click **Apply**.

The cardholder is no longer synchronized with the AD. It will only become synchronized again once you set the cardholder’s status to **Keep synchronized**.

Selecting which cardholder fields to synchronize with Active Directory

Before synchronizing with the AD, you need to select which cardholder attributes you want to import from the AD by mapping them to Security Center fields in the *Links* tab of the Active Directory role. The mapping can be different for each Active Directory role in your system.

What you should know

The cardholder picture field can be mapped to any AD binary attribute if you just want to import them from the AD. But if you want to upload the cardholder pictures from Security Center to the AD, then you must map it to the AD attribute *thumbnailPhoto*.

To map AD attributes to cardholder fields:

1. From the **Links** tab of the Active Directory role, click **Add an item** (✚).
2. Select a Security Center cardholder field and an AD attribute, and then click **OK**.

   IMPORTANT: The data type of the Security Center field must match that of the AD attribute: text with text, decimal with decimal, date with date, and so on. The Security Center image data type must be mapped to the AD binary data type, and the mapped AD attribute must contain a valid JPEG image.

   The new mapping appears in the **Links** tab.
3. Repeat the previous steps as needed.
4. If you are importing cardholder credential fields, do the following in the **Links** tab:
   - From the **Card format** drop-down list, select the default card format to use for the imported cardholder credentials when the card format property is either not mapped to an AD attribute, or when the mapped attribute is empty.
   - From the **Badge template** drop-down list, select a default badge template to use for the imported cardholder credentials.
5. Click **Apply**.

The mapped cardholder fields are displayed in the **Links** tab. When you synchronize with the AD, most of them are read-only.

Related Topics

Integration with Windows Active Directory on page 318

Using signature pads

If you have a signature pad attached to your computer, you can use it to capture cardholder and visitor signatures, and save them directly to a signature custom field that was created beforehand.

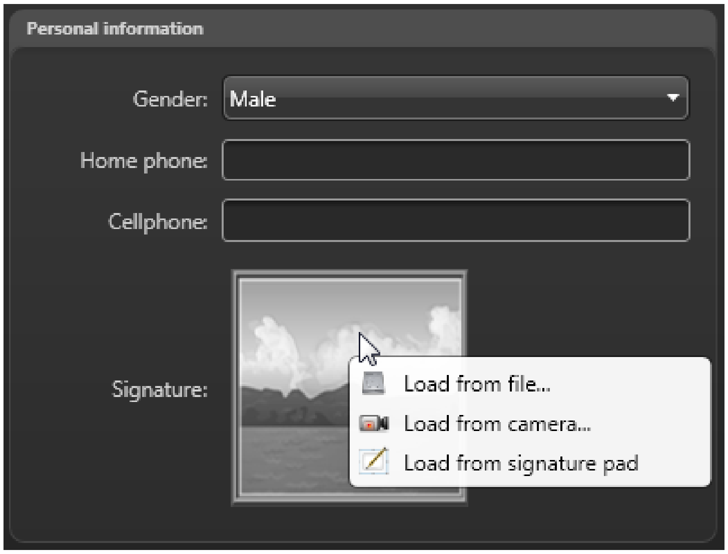
Before you begin

- Make sure cardholder and visitor signature custom fields have been created with the *Image data* type.
- Attach a Topaz signature pad to your computer, and enable it in Security Desk.

To use a signature pad:

1 Open the *Cardholder management* task or *Visitor management* task to create or modify the cardholder or visitor.

2 In the property dialog box, click the custom field reserved for the signature and select **Load from signature pad**.



3 Hand the signature pad to the cardholder or visitor and ask them to sign.

The captured signature appears in the signature field.

4 Click **Save**.

Receiving notifications when cardholders are expiring

You can configure Security Center to send you or another user an email before cardholders or their credentials expire.

Before you begin

If you want the user to be notified by email, make sure they have a valid email address.

What you should know

Users can be notified for every cardholder or credential that is expiring soon, or only for specific entities.

If a cardholder expires, their credential is no longer valid either.

To receive a notification when a cardholder or their credential is expiring:

1 Open the **Access control** task, and click the **General settings** view.

2 Switch the **Trigger event 'Entity is expiring soon'** option to **ON**, and select how many days prior to the expiration to trigger the event.

3 Click **Apply**.

4 Open the **System** task, and click the **General settings** view.

5 Click the **Actions** page, and click **Add an item** (➕).

6 In the **Entity type** page, do one of the following:

- To send a notification when any cardholder or credential is expiring, select **System**, and click **Next**.
- To send a notification when a cardholder is expiring, select **Cardholder**, and click **Next**.
- To send a notification when a credential is expiring, select **Credential**, and click **Next**.

7 If you selected **Cardholder** or **Credential**, select a specific entity in the **Source** page, and click **Next**.

8 In the **Event** page, select *Entity is expiring soon*, and click **Next**.

9 In the **Action** page, select one of the following actions:

- To send a pop up message to a user's Security Desk window, select **Send a message**.
- To send an email to a user, select **Send an email**.

10 Select the **Recipient**, type a message, and click **Next**.

11 Verify that the information is correct, and then click **Create** > **Close**.

The user is sent a message or an email, the number of days you specified before the entity expires.

32

Credentials

This section includes the following topics:

About credentials

A credential is a type of entity that represents a proximity card, a biometrics template, or a PIN required to gain access to a secured area. A credential can only be assigned to one cardholder at a time.

The credential entity represents a proximity card, a biometrics template, or a PIN. Credentials are used by Security Center to identify who is requesting access through a secured *access point*. Credentials are really *claims of identity*. A credential distinguishes one cardholder from another. For access control to be operational, every cardholder must possess at least one credential. These are typically (but not exclusively) access control cards.

The required credential depends on the type of reader installed at the door.

Supported card formats

Security Center supports a few standard card formats.

For card formats, a card number is always required. Depending on the card format, the facility code might not be necessary. The following table describes the standard card formats supported by Security Center, and the valid ranges for the facility code (also known as *Company ID Code*) and card number (also known as *Card ID Number*).

Card format	Facility code range	Card number range
Standard 26 bits	0 to 255	0 to 65 535
HID H10306 34 Bits	0 to 65 535	0 to 65 535
HID H10302 37 Bits	Not required[1]	0 to 34 359 738 367
HID H10304 37 Bits	0 to 65 535	0 to 524 287
HID Corporate 1000 (35 bits)	0 to 4095	0 to 1 048 575
HID Corporate 1000 (48 bits)	0 to 4 194 303	0 to 8 388 607

[1] If HID H10302 37 Bits is the only card format referenced in your CSV file, it is preferable to bind the card number to the Security Center Card data field instead of the Card number field since the facility code is not required. Because a single value is stored in the Credential card data field, no separator character is needed.

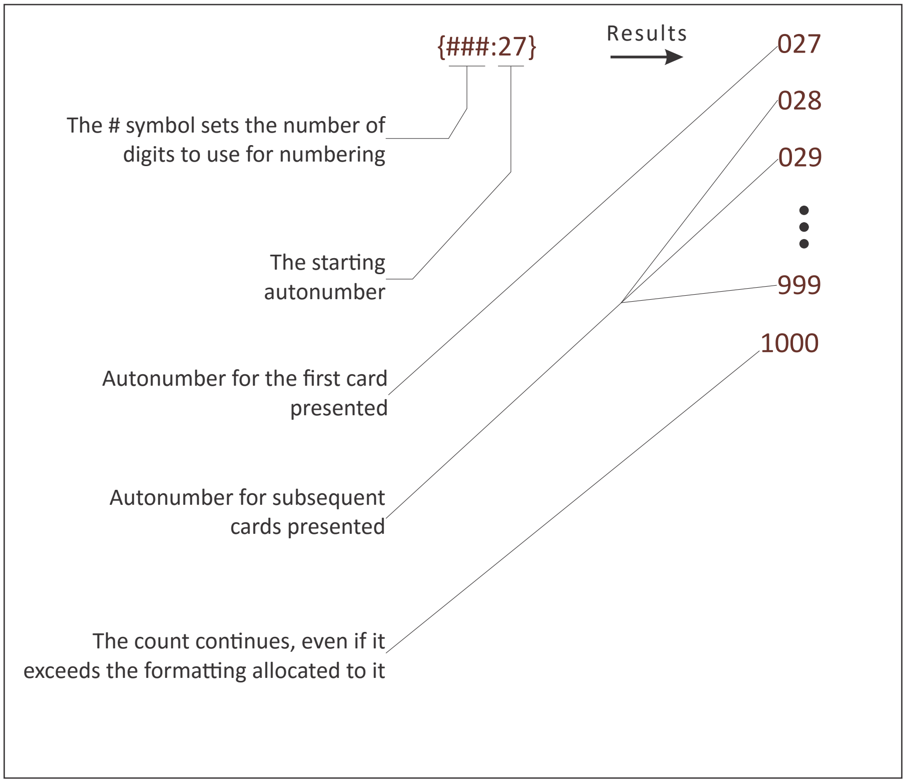
Custom card formats can also be defined using the *Custom format editor* tool.

The credential prefix and the counter

The **Credential prefix** sets the name of enrolled credentials. The Credential management task ensures that all enrolled credentials have a unique name by automatically adding a number to the name set in **Credential prefix**. You can also control the counter by adding an autonumber format (between curly brackets) to the credential prefix.

The credential autonumber format defines the counter style. The autonumber format can be placed anywhere in the credential prefix. Only one autonumber format can be used in the credential prefix at a time.

The autonumber format is explained below.


{###:27}
Results
027
028
029
999
1000
The # symbol sets the number of digits to use for numbering
The starting autonumber
Autonumber for the first card presented
Autonumber for subsequent cards presented
The count continues, even if it exceeds the formatting allocated to it

The following are examples for the autonumber format.

Credential prefix	Credential sequence generated	Comments
Credential_	Credential_0 Crediential_1 Credential_2	When the autonumber format is omitted, the autonumber is appended at the end of the prefix and starts at 0.
Credential #{##:1}	Credential #01 Credential #02 Credential #03	A basic autonumber for the credential prefix.
1{####:46} 11203162-2	10046 11203162-2 10047 11203162-2 10048 11203162-2	Enrolled credentials can be autonumbered in Security Center so their names correspond to the serial number printed on the back of a series of cards.

Card naming recommendation

When enrolling card credentials, it is a best practice to use the card number printed on the card as the name of the credential in Security Center. If a lost card is found, then you can easily find it in the system.

If you plan to print the credential name on a badge as a barcode, ensure that only the characters supported by the barcode type are used.

PIN recommendation

When using PIN as a credential, you can use it either with ar card (Card and PIN) or on its own (Card or PIN). Your reader capabilities and configuration determine how the PIN is required.

If you plan to use your readers in a Card or PIN mode, ensure that the PINs are unique for all cardholders and that there are no duplicates in the system. Duplicate PINs may lead to confusion as there is no way to determine which cardholder it belongs to when a user type it in at the door.

Credential enrollment methods

If you need many card credentials in your access control system, you can enroll multiple credentials at a time.

The following two enrollment methods are available in the *Credential management* task:

- **Automatic entry:** This is the recommended method when the cards you want to enroll are at your disposal, and when the card data is not found within any known range of values. It is also appropriate to use this enrollment method when the cards come in many types of formats.
- **Manual entry:** This is the recommended method when all the cards you want to enroll are the same format, and one of the data fields (typically the *Card number*) contains a range of consecutive values. You do not require the actual cards, or a card reader to use this method, and it can be an effective way of pre-enrolling large quantities of cards.

You can also enroll credentials using the *Import tool*.

Enrolling multiple credentials automatically

If you need many card credentials in your access control system, you can enroll multiple card credentials automatically by presenting them to a reader.

Before you begin

You must have access to a card reader. The cards you present must be from a predefined format in your system.

Make sure that this is the correct enrollment method you require.

What you should know

All credentials you enroll must be new to your Security Center system. Any previously enrolled credential is discarded, because the same credential cannot be enrolled twice in Security Center.

To enroll multiple credentials automatically:

1 In the **Credential management** task, click **Batch enrollment**.

2 In the *Automatic entry* tab, select a card reader that is nearby.
Ensure the selected reader supports the card formats you have.

3 In the **Credential prefix** section, type the pattern for the enrolled credential names.

4 In the *Credential status* section, set the status, activation date, and expiration date for the credentials.
   - **Status:** All possible values are accepted.
   - **Activation:** Can be *Never*, or a specific date.
   - **Expiration:** Set an expiration for the credential:
     - **Never:** The credential never expires.
     - **Specific date:** The credential expires on a specific date and time.
     - **Set expiration on first use:** The credential expires after a specified number of days after the first use.
     - **When not used:** The credential expires when it has not been used for a specified number of days.

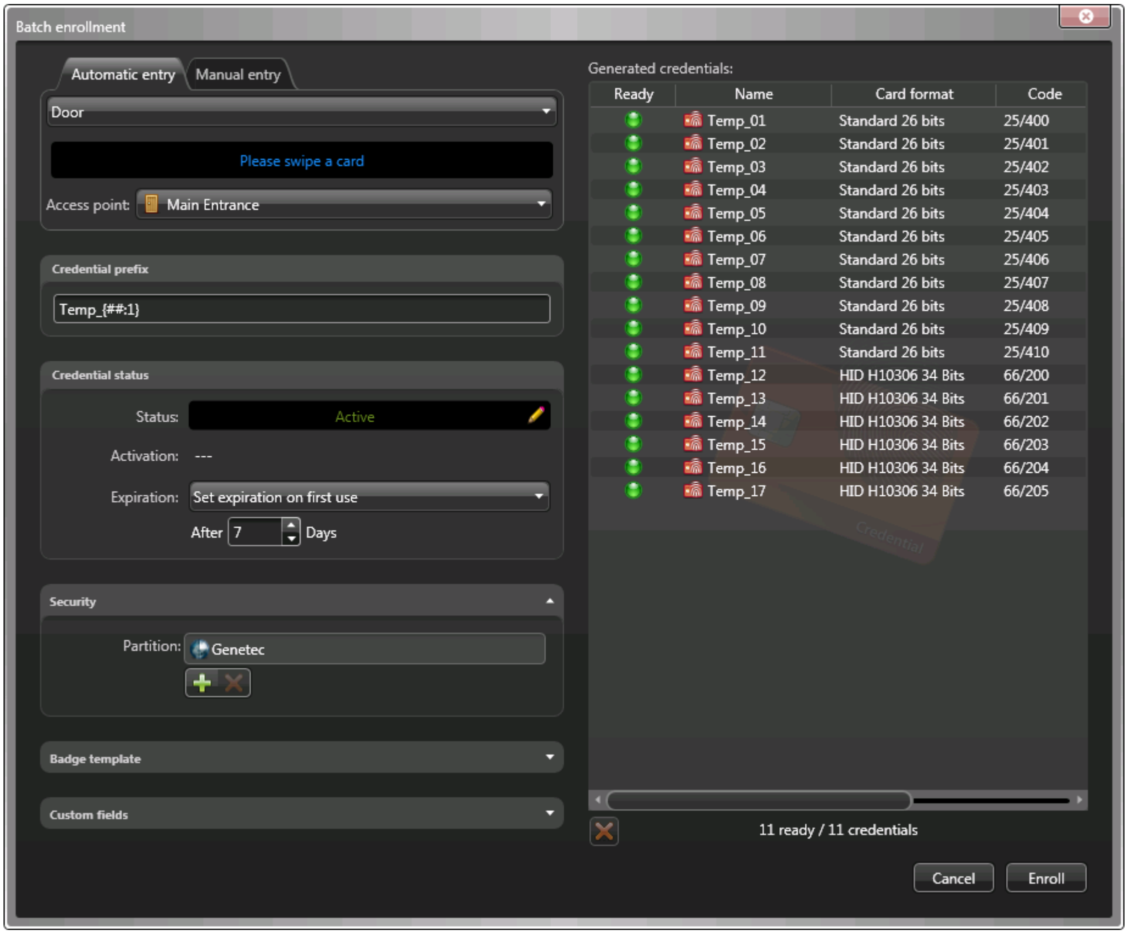
5 In the *Security* section, select the partition the enrolled credentials belong to.
This field determines which users can view and modify the credentials.
   - To add a partition, click **Add** (➕).
   - To remove a partition, select the partition, and then click **Remove** (✖).

6 From the **Badge template** drop-down list, select the default badge template used to represent the credential.

7 In the *Custom fields* section, set the default values for the custom fields.
Custom fields are only available if they have been created for credentials.

8 Present the cards on the selected reader.

All presented cards are listed in the *Generated credentials* section.



Door

Please swipe a card

Access point: Main Entrance

Credential prefix

Temp_{##:1}

Credential status

Status: Active

Activation: ---

Expiration: Set expiration on first use

After 7 Days

Security

Partition: Genetec

Badge template

Custom fields

Generated credentials:

Ready	Name	Card format	Code
●	Temp_01	Standard 26 bits	25/400
●	Temp_02	Standard 26 bits	25/401
●	Temp_03	Standard 26 bits	25/402
●	Temp_04	Standard 26 bits	25/403
●	Temp_05	Standard 26 bits	25/404
●	Temp_06	Standard 26 bits	25/405
●	Temp_07	Standard 26 bits	25/406
●	Temp_08	Standard 26 bits	25/407
●	Temp_09	Standard 26 bits	25/408
●	Temp_10	Standard 26 bits	25/409
●	Temp_11	Standard 26 bits	25/410
●	Temp_12	HID H10306 34 Bits	66/200
●	Temp_13	HID H10306 34 Bits	66/201
●	Temp_14	HID H10306 34 Bits	66/202
●	Temp_15	HID H10306 34 Bits	66/203
●	Temp_16	HID H10306 34 Bits	66/204
●	Temp_17	HID H10306 34 Bits	66/205

11 ready / 11 credentials

If some of the credentials are already enrolled, they are discarded, and marked as rejected in the list with a red button. If you present the same card twice, it is highlighted momentarily in the list.

9 To remove a discarded card from the list, select it and click ✖.

10 Click **Enroll**.

After you finish

Assign the credentials to your cardholders.

Related Topics

Credential enrollment methods on page 556
How credential card formats work with Active Directory in Security Center on page 566
About credentials on page 553

Enrolling multiple credentials manually

If you need many card credentials in your access control system, you can enroll multiple credentials simultaneously by entering the card format and data manually.

Before you begin

You must know the exact range of values represented in the card data. Because those cards are not presented by a reader, the application cannot validate them.

Make sure that this is the correct enrollment method you require.

What you should know

All credentials you enroll must be new to your Security Center system. Any previously enrolled credential is discarded, because the same credential cannot be enrolled twice in Security Center. Only a maximum of 5000 credentials can be created at once.

To enroll multiple credentials manually:

1 In the **Credential management** task, click **Batch enrollment**.

2 Click the *Manual entry* tab.

3 From the **Card format** drop-down list, set the card format used by the credentials you want to enroll.

This option determines the data fields you must enter, and the range of values that they can have.

4 In the **Facility code** and **Card number** fields, enter the starting and ending values for the card numbers.

The **Card number** field is used as a sequence generator.

NOTE: If the specified **Card number** range contains more than 5000 values, the end value is automatically adjusted to be the start value plus 5000.

5 In the **Credential prefix** section, type the pattern for the enrolled credential names.

6 In the *Credential status* section, set the status, activation date, and expiration date for the credentials.

- **Status:** All possible values are accepted.
- **Activation:** Can be *Never*, or a specific date.
- **Expiration:** Set an expiration for the credential:
  - **Never:** The credential never expires.
  - **Specific date:** The credential expires on a specific date and time.
  - **Set expiration on first use:** The credential expires after a specified number of days after the first use.
  - **When not used:** The credential expires when it has not been used for a specified number of days.

7 In the *Security* section, select the partition the enrolled credentials belong to.

This field determines which users can view and modify the credentials.

- To add a partition, click **Add** (➕).
- To remove a partition, select the partition, and then click **Remove** (✖).

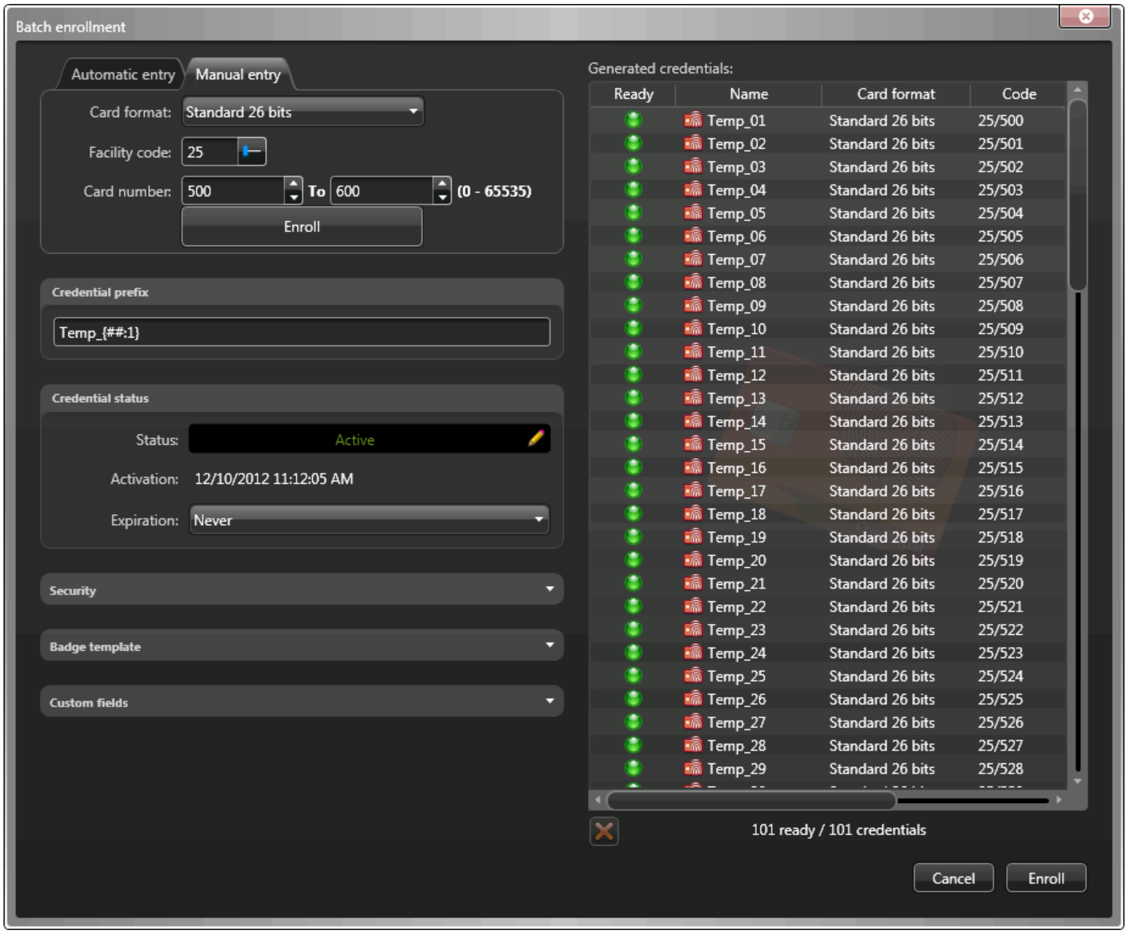
8 From the **Badge template** drop-down list, select the default badge template used to represent the credential.

9 In the *Custom fields* section, set the default values for the custom fields.

Custom fields are only available if they have been created for credentials.

10 Click **Enroll**.

The credentials you are going to create are listed in the *Generated credentials* section.



Card format: Standard 26 bits

Facility code: 25

Card number: 500 To 600 (0 - 65535)

Credential prefix: Temp_{##:1}

Credential status

Status: Active

Activation: 12/10/2012 11:12:05 AM

Expiration: Never

Generated credentials:

Ready	Name	Card format	Code
●	Temp_01	Standard 26 bits	25/500
●	Temp_02	Standard 26 bits	25/501
●	Temp_03	Standard 26 bits	25/502
●	Temp_04	Standard 26 bits	25/503
●	Temp_05	Standard 26 bits	25/504
●	Temp_06	Standard 26 bits	25/505
●	Temp_07	Standard 26 bits	25/506
●	Temp_08	Standard 26 bits	25/507
●	Temp_09	Standard 26 bits	25/508
●	Temp_10	Standard 26 bits	25/509
●	Temp_11	Standard 26 bits	25/510
●	Temp_12	Standard 26 bits	25/511
●	Temp_13	Standard 26 bits	25/512
●	Temp_14	Standard 26 bits	25/513
●	Temp_15	Standard 26 bits	25/514
●	Temp_16	Standard 26 bits	25/515
●	Temp_17	Standard 26 bits	25/516
●	Temp_18	Standard 26 bits	25/517
●	Temp_19	Standard 26 bits	25/518
●	Temp_20	Standard 26 bits	25/519
●	Temp_21	Standard 26 bits	25/520
●	Temp_22	Standard 26 bits	25/521
●	Temp_23	Standard 26 bits	25/522
●	Temp_24	Standard 26 bits	25/523
●	Temp_25	Standard 26 bits	25/524
●	Temp_26	Standard 26 bits	25/525
●	Temp_27	Standard 26 bits	25/526
●	Temp_28	Standard 26 bits	25/527
●	Temp_29	Standard 26 bits	25/528

101 ready / 101 credentials

If some of the credentials are already enrolled, they are discarded, and marked as rejected in the list with a red button.

11 To remove a discarded credential from the list, select it, and then click ✖.

12 Click **Enroll**.

After you finish

Assign the credentials to your cardholders.

Related Topics

Credential enrollment methods on page 556

How credential card formats work with Active Directory in Security Center on page 566

About credentials on page 553

Creating credentials

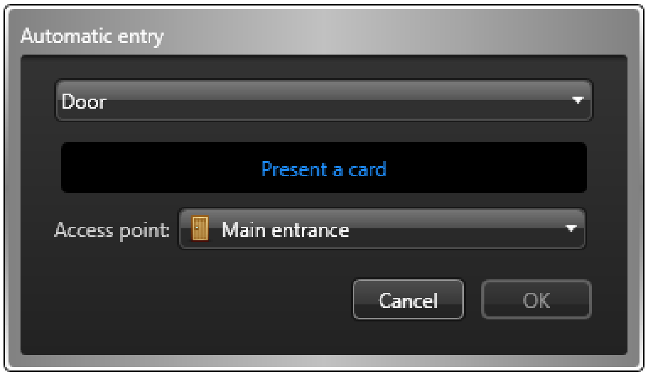
You can create a new credential, configure its properties, and assign it to a cardholder or visitor, using the *Credential management* task.

What you should know

Instead of creating cardholders manually, you can import them from a CSV file, or from your company's Active Directory.

To create a credential:

1. In the **Credential management** task, click **Create new credential** (+).
2. Select one of the following options:
   - **Automatic entry:** Present the card at a reader.
   - **Manual entry:** Manually enter the card data. Use this method when you do not have a card reader near you.
   - **Existing credential:** Select a pre-enrolled, unassigned credential.
   - **PIN:** Create a PIN credential.
3. If you select **Automatic entry**, then select a reader (USB reader or a door), and present the card at the reader.



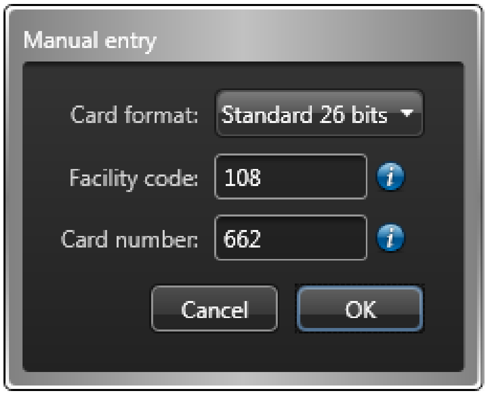
Automatic entry

Door

Present a card

Access point: Main entrance

   The dialog box closes automatically after an eligible card is presented. If the card has not been enrolled, it is enrolled automatically. If it was already assigned to someone, it is rejected.
4. If you select **Manual entry**, then select a card format, enter the required data fields, and click **OK**.



Manual entry

Card format: Standard 26 bits

Facility code: 108

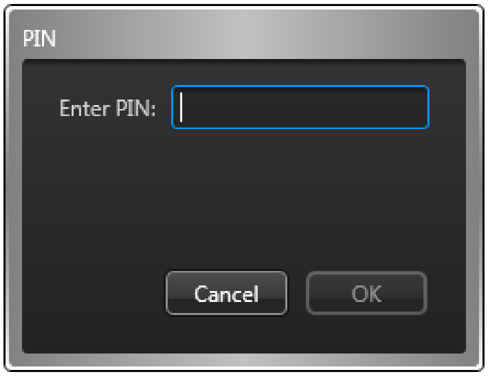
Card number: 662

   If the card has not been enrolled, it is enrolled automatically. If it was already assigned to someone, it is rejected.

CAUTION: Be careful when you enter the card data, because the system cannot validate whether the data you entered correspond to a physical card or not.

5 If you select **Existing credential**, a dialog box listing all existing but unassigned credentials in the system appears. Select an unassigned credential from the list, and click **OK**.

6 If you select **PIN**, then do the following:



a) Click inside the first box to start entering the PIN.

Only numerical values are accepted. You can enter up to five digits.

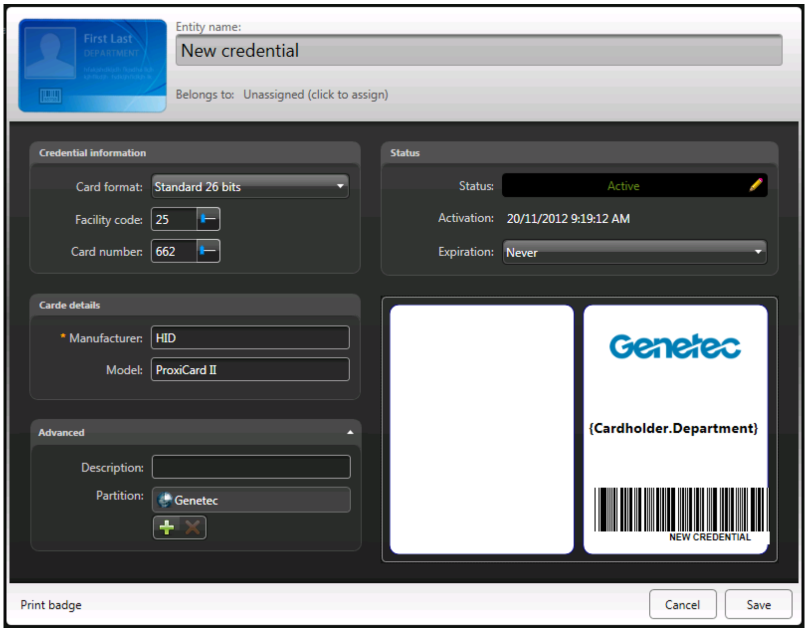
NOTE: The numeric value corresponding to the PIN cannot exceed 65535.

IMPORTANT: If your system is configured to use card or PIN, ensure that there are no PIN duplicates. Duplicates create confusion when a user types a PIN and the system cannot associate this PIN to the right cardholder.

b) Re-enter the PIN, and click **OK**.

The credential details dialog box opens.

7 In the **Entity name** field, enter a name for the credential entity.



Entity name: New credential

Belongs to: Unassigned (click to assign)

Card format: Standard 26 bits

Facility code: 25

Card number: 662

* Manufacturer: HID

Model: ProxiCard II

Description:

Partition: Genetec

Status: Active

Activation: 20/11/2012 9:19:12 AM

Expiration: Never

8 Click the **Belongs to** field, select a cardholder or visitor to assign the credential to, and then click **OK**.

Without assigning a credential, you cannot monitor the activities, or generate activity reports for that cardholder or visitor.

9 In the *Status* section, set the status and activation period for the credential.

If the credential is inactive, the cardholder or visitor does not have access to any area.

- **Status:** Set the credential status to **Active**.

- **Activation:** Displays the current date.
- **Expiration:** Set an expiration for the credential:
  - **Never:** The credential never expires.
  - **Specific date:** The credential expires on a specific date and time.
  - **Set expiration on first use:** The credential expires after a specified number of days after the first use.
  - **When not used:** The credential expires when it has not been used for a specified number of days.

10 If custom fields are defined for credentials, such as the manufacturer, the card model, and so on, enter the credential's custom information under the *Credential information* section.

11 (Optional) Click the *Advanced* section, and configure the following credential properties:

a) In the **Description** field, type a description for the credential.

b) Assign the credential to a *partition*.

Partitions determine which Security Center users have access to this entity. Only accepted users of the partition can view or modify the credential.

12 (Optional) If the credential is a card credential (not a PIN), select a badge template.

a) In the lower-right corner of the credential details dialog box, click the badge image.

b) Select a badge template, and then click **OK**.

Badge templates are created in Config Tool.

A print preview of the badge appears, with data corresponding to the credential.

NOTE: The badge template remains associated to the credential even if you unassign the credential from a cardholder or visitor.

13 To print the badge, in the lower-left corner of the credential details dialog box, click **Print badge**.

14 When you are finished editing the credential, click **Save**.

The new credential is added to the list in the **Credential management** task.

After you finish

To modify a credential, select the credential in the list, and then click **Modify** (✎).

Related Topics

Importing cardholders and credentials on page 595
Assigning credentials on page 543
Designing badge templates on page 573
Responding to credential card requests on page 565

Adding reasons for credential card requests

To allow users to specify why they are requesting a credential card, you can add a set of reasons that they can choose from.

What you should know

A common reason a user might request a credential card is: “no printer on site”.

To add a credential card request reason:

1 Open the **Access control** task, and click the **General settings** view.

2 Under the *Card request reasons* section, click **Add an item** (➕).

3 In the **Add a new card request reason** dialog box, type a reason, and click **Add** > **Apply**.

4 To modify a card request reason, select it in the list, and click **Edit the item** (✏).

5 To delete a card request reason, select it in the list, and click **Remove the item** (✖).

The new reason can now be selected when users request credential cards.

Responding to credential card requests

After a credential card request has been made, you can respond by assigning a credential to the applicant the request was made for, or by denying the request.

What you should know

The number of pending card requests is shown in the **Card requests** () icon in the notification tray, and at the top of the *Credential management* task.

Credential requests are sent when a user creates a new cardholder, but cannot assign a credential or print a card for the cardholder (for example, because no printer is available). After you assign and print a credential card, it can be shipped to another site, if required.

To respond to a credential card request:

1 Do one of the following:

- In the notification tray, click **Card requests** ().
- At the top of the **Credential management** task, click **Card requests**.

2 In the *Card requests* dialog box, select the request you want to respond to.

3 To modify the request, click **Modify** (), edit the request, and then click **OK**.

4 To deny the request, click **Deny request** ().

5 To assign a card credential, click **Associate card** ().
In the *Associate cards* dialog box that opens, do one of the following:

- To assign a credential automatically, click **Automatic entry**, then select a reader (USB reader or a door), and present the card at the reader.

  If an eligible card is presented, it is immediately assigned. If the card has not been enrolled, it is enrolled automatically. If it was already assigned to someone, it is rejected.

- To assign a credential manually, click **Manual entry**, then select a card format, enter the required data fields, and click **Enroll**.

  If an eligible card is entered, it is immediately assigned. If the card has not been enrolled, it is enrolled automatically. If it was already assigned to someone, it is rejected.

  CAUTION: Be careful when you enter the card data, because the system cannot validate whether the data you entered correspond to a physical card or not.

- To assign an existing credential, click **Existing credential**, then double-click a credential from the list of eligible credentials.

6 To print the badge on the card, click **Print cards** () and follow the instructions.

7 Click **Close** to complete this request.

After the card request is completed or denied, an email is sent to the requester only if they selected the **Email me when the card is ready** option when they requested the card.

Related Topics

Requesting credential cards on page 545
Creating credentials on page 561

How credential card formats work with Active Directory in Security Center

If you decide to map the credential *Card format* property to an Active Directory attribute, that attribute must contain either a numeric value (for standard card formats) or the exact card format name (text).

The following table describes the standard card formats supported by Security Center, their numeric values, and the valid ranges for the facility code (also known as *Company ID Code*) and card number (also known as *Card ID Number*).

Number	Format name (Text)	Facility code range	Card number range
0	Standard 26 bits	0 to 255	0 to 65 535
1	HID H10306 34 Bits	0 to 65 535	0 to 65 535
2	HID H10302 37 Bits	Not required[1]	0 to 34 359 738 367
3	HID H10304 37 Bits	0 to 65 535	0 to 524 287
4	HID Corporate 1000 (35 bits)	0 to 4095	0 to 1 048 575
5	HID Corporate 1000 (48 bits)	0 to 4 194 303	0 to 8 388 607

[1] If HID H10302 37 Bits is the only card format referenced in your CSV file, it is preferable to bind the card number to the Security Center Card data field instead of the Card number field since the facility code is not required. Because a single value is stored in the Credential card data field, no separator character is needed.

IMPORTANT: For custom card formats, you must use the exact spelling used to create the custom card format.

Related Topics

Integration with Windows Active Directory on page 318
Custom card formats on page 567
Custom card format editor tool on page 568
Creating custom card formats on page 569

Custom card formats

In addition to the standard card formats that are supported in Security Center, you can define custom card formats with unique data fields.

You can define custom card formats in Config Tool from the *General settings* view in the Access control task..

Benefits of custom card formats

Creating custom card formats has the following benefits:

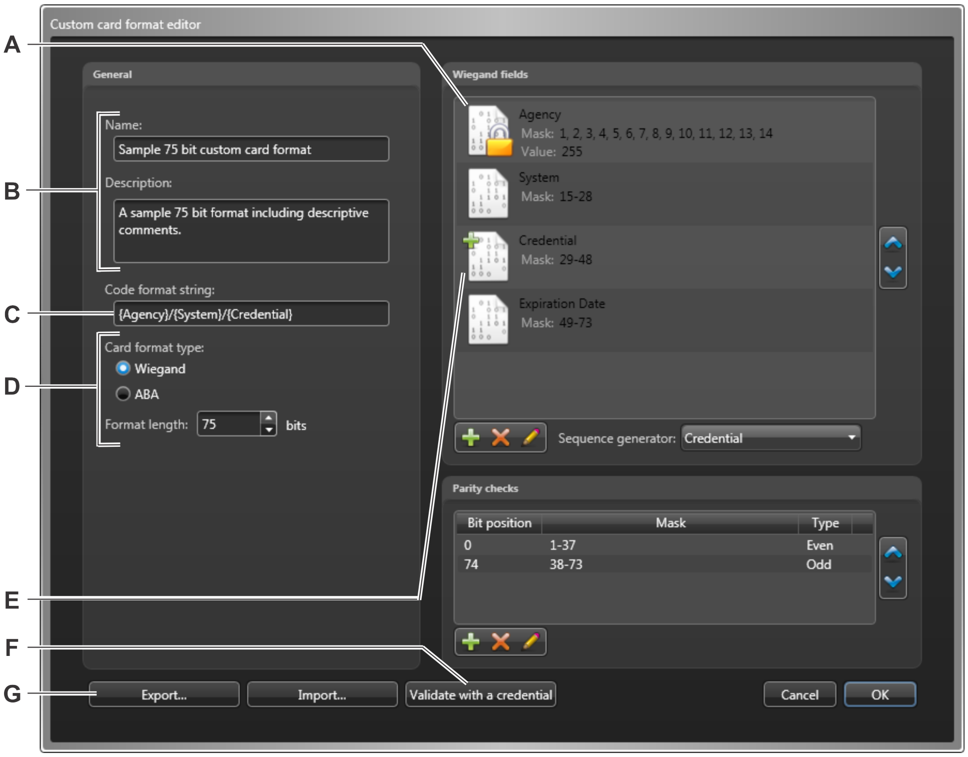
- You can manually enroll a new card using a standard workstation keyboard, whereas a card with an unknown format can only be enrolled using a card reader.
- You can view the card number in the Config Tool and the Security Desk, whereas data for unknown card formats cannot be displayed.
- You can import cards using custom formats with the *Import tool*.
- You can enroll cards automatically, with a card reader, or manually in bulk, without a card reader, using the Credential management task.

Related Topics
Importing security groups from an Active Directory on page 323
About federated entities on page 190

Custom card format editor tool

The *custom card format editor* is a Synergis™-specific tool that allows you to define your own card formats. It is available from the *General settings* view in the Access control task.

Only administrative users can use this tool.



Name: Sample 75 bit custom card format

Description: A sample 75 bit format including descriptive comments.

Code format string: {Agency}/{System}/{Credential}

Card format type:
● Wiegand
○ ABA

Format length: 75 bits

Agency
Mask: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
Value: 255

System
Mask: 15-28

Credential
Mask: 29-48

Expiration Date
Mask: 49-73

Sequence generator: Credential

Bit position	Mask	Type
0	1-37	Even
74	38-73	Odd

A	Fixed value field (indicated by the padlock 🔒 icon).
B	Card format name and description listed in the *Access control* task, view.
C	Format used to display the *Credential code* in reports.
D	Select the card format type and length before defining the fields.
E	Field designated as the sequence generator (indicated by the plus ✚ icon).
F	Validate the format with pre-enrolled credentials.
G	Import/export card format from XML file.

Related Topics

How credential card formats work with Active Directory in Security Center on page 566
Creating custom card formats on page 569

Creating custom card formats

To define custom card formats that have unique data fields, you can create custom formats manually, or import them from XML files, using the *Custom card format editor* tool.

What you should know

If you delete a custom card format after it is being used in Security Center, all credentials using that format appear as *Unknown*, but the credentials are still granted access at the doors.

To create a new custom card format:

1 Open the **Access control** task, and click the **General settings** view.

2 Under **Custom card formats**, click **Add an item** (+).

3 In the **Custom card format editor**, enter the **Name** and **Description** of the custom card format.

4 Specify the **Card format type** and **Format length**.

- **Wiegand** (8 to 128 bits)
- **ABA** (2 to 32 characters)

5 Define the Wiegand fields or define the ABA fields that constitute the custom card format.

6 If you selected **Wiegand** format type, you might have to add parity check bits to the format.

7 (Wiegand type only) If you want to enroll a range of credentials in bulk, you can designate one field as the **sequence generator**.

The field designated as the sequence generator allows you to define a range of values for enrolling the credentials in bulk in the *Credential Management* task.

8 Enter the format string for printing the **credential code**.

The credential code is the printed form of the credential data. It is an optional column that is available in most access control related reports.The **Code format string** tells the system how to print the credential data. To include a field in the credential code, the field name must be specified in the code format string as it is spelled in the card format field definition, between curly brackets "{ }". The field names are case-sensitive. Any other characters in the format string that are not found between curly brackets are printed as is.For example, with the format string "{Facility}/{Card Number}", a credential with the respective field values 230 and 7455 will be printed as "230/7455".

9 To validate the new custom card format with a pre-enrolled credential, click **Validate with a credential**, select a pre-enrolled credential, and click **OK**.

10 (Optional) Click **Export** to save the custom card format to an XML file.

Exporting the custom card format to an XML file allows you to import that same card format definition to other Synergis™ systems.

11 Click **OK** > **Apply**.

Related Topics
Custom card formats on page 567

Defining ABA fields

If you are adding a custom ABA card format, you must define the ABA data fields that constitute the card format.

What you should know

ABA field length is measured in characters (4 bits each). The maximum ABA field length is 18 characters, or up to the card format length, whichever comes first. The maximum ABA card format length is 32 characters or 128 bits.

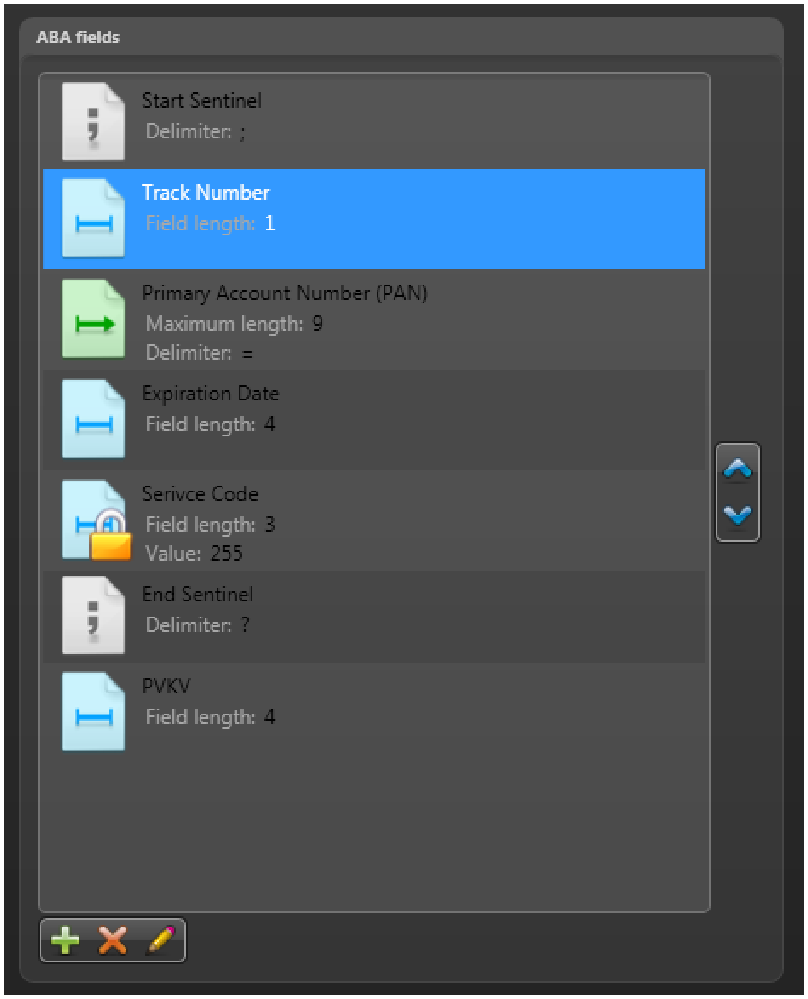
The order of the ABA fields in the format is important for two reasons:

- It defines the card format.
- It corresponds to the order the field values are read from the Credential card data when using the Import tool.

To define an ABA field:

1. In the *Custom card format editor*, click **Add an item** (➕) under the **ABA fields** section.
2. Select one of the following ABA field types:
   - **Delimiter:** Specifies a delimiter character, typically used at the beginning or the end of the card format.
   - **Sized:** A fixed-length field. The length is specified in characters (4 bits each). The field can contain a fixed value. The field length must be long enough to hold the fixed value.
   - **Delimited:** A variable length field. You must specify a maximum length (as 4-bit characters) and a delimiter character.
3. Click **OK**.

   The field is added in the **ABA fields** section.



ABA fields

Start Sentinel
Delimiter: ;

Track Number
Field length: 1

Primary Account Number (PAN)
Maximum length: 9
Delimiter: =

Expiration Date
Field length: 4

Serivce Code
Field length: 3
Value: 255

End Sentinel
Delimiter: ?

PVKV
Field length: 4

Defining Wiegand fields

If you are adding a custom Wiegand card format, you must define the Wiegand data fields that constitute the card format.

What you should know

A Wiegand field is composed of a series of bits. The maximum field length is 63 bits.

The order of the Wiegand fields for the card format is important. It corresponds to the order that field values are read from the Credential card data when using the *Import tool*.

To define a Wiegand field:

1 In the *Custom card format editor*, click **Add an item** (+) under the **Wiegand fields** section.

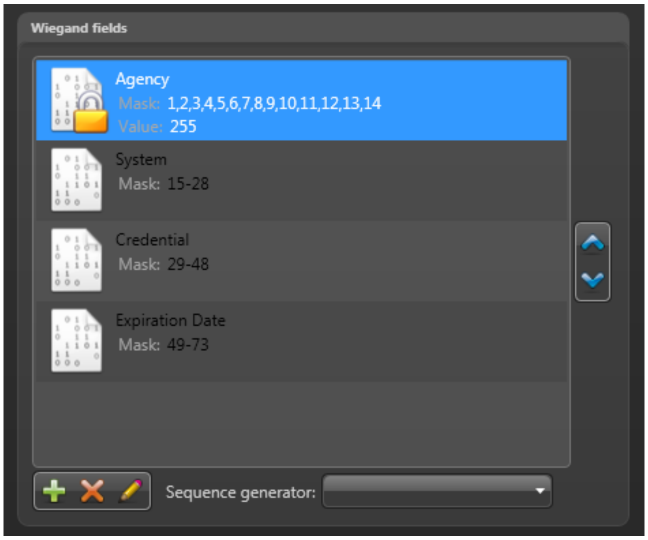
2 In the **Name** field, type a name for the Wiegand field.

3 In the **Mask** field, type the number of bits that are part of the Wiegand field.

The bits are named according to their position in the card format, starting from 0. You can enter the masks as a list of comma-separated bit positions, or as a range of bit position. For example, the mask “**1,2,3,4,5,6,7,8**” can also be written as “**1-8**” or “**1-4,5-8**”. The order of the bits within the field is important (“**1,2,3,4**” is not the same as “**4,3,2,1**”).

4 Click **OK**.

The field is added in the **Wiegand fields** section.



Wiegand fields

Agency
Mask: 1,2,3,4,5,6,7,8,9,10,11,12,13,14
Value: 255

System
Mask: 15-28

Credential
Mask: 29-48

Expiration Date
Mask: 49-73

Adding parity checks

If you are defining a custom Wiegand card format, you can add parity checks to strengthen the validation of your credentials.

What you should know

The order of the parity checks in the **Parity checks** list is important. It corresponds to the order in which the parity checks are evaluated. The mask of a subsequent parity check can include the parity bit of a previous parity check and their masks can overlap.

To add a parity check:

1. In the *Custom card format editor*, click **Add an item** (➕) under the **Parity checks** section.
2. In the **Parity checks** dialog box, select the **Type** of parity check (**Even** or **Odd**).
3. In the **Parity bit** field, type the position of the parity bit in the card format (starts at 0)
4. In the **Mask** field, type the bits that should be evaluated.

   The syntax must match the Wiegand data field mask values, but the order of the bits is not important.

5. Click **OK.**

   The parity check is added in the **Parity checks** list.

Designing badge templates

To use customized printing templates for credential cards, you can design new badge templates that are tailored to your needs.

What you should know

A badge template is represented by a *badge template* entity in Security Center, and can include fields from the configuration database so that the correct name, cardholder photo, and so on, will appear on each card.

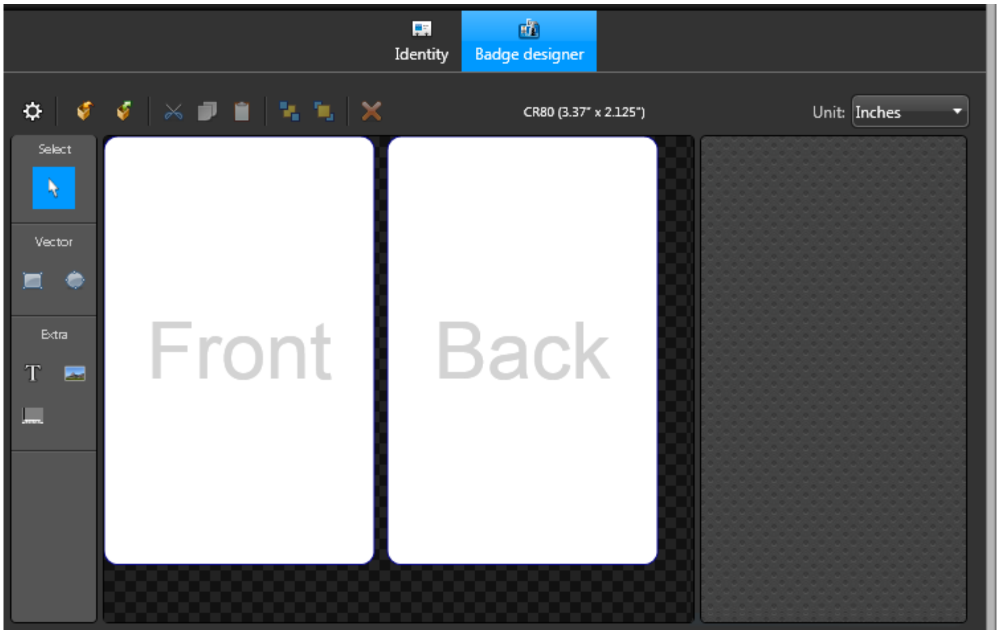
For example, you can add a company logo, a background image, employee photo, or a custom color to be printed on the access control cards.

To design a badge template:

1. Open the **Access control** task, and click the **Badge template** view.
2. Click **Badge template** (+).
3. Type a name for the new badge template that appears in the entity list, and press **ENTER**.
4. In the **Identity** tab, type a description for the badge template.
5. In the **Relationships** section, select the partition where you want the badge template to be placed.

   Partitions determine which Security Center users have access to this entity. Only users that are part of the partition can view or modify the badge template.

6. Click **Apply**.
7. Click the **Badge designer** tab.
8. To select the size of the access control cards you want to print, click **Properties** (⚙).
9. In the **Format** dialog box, select a card size and orientation.
   - To create custom card size, click +, enter the card name, width, and length, and then click **OK**.
10. Click **OK.**



    Once the card size/format is chosen, you can design the actual printing template.

11. In the **Tools** section, select a tool, and then click on the template to use it.

    There are six graphical tools you can use to edit the template:

- **Select tool:** Use to click and select an object on the template.
- **Rectangle tool:** Use to draw a square/rectangle on the template.
- **Ellipsis tool:** Use to draw circles/ovals on the template.
- **Text tool:** Use to insert text on to the template. You can enter a static text or add dynamic cardholder and credential text fields, such as *First name*, *Last name*, and so on.
- **Image tool:** Use to insert a picture on to the template. You can insert cardholder pictures, a background image for the card, and so on.
- **Barcode tool:** Use to insert barcodes on to the template.

12. If you added an image to the template, select the image to edit it using the options in the **Image** and **Color and border** widgets.

    In the **Image** widget, choose whether the **Source** of the image is a cardholder picture or an image from a file, and whether the image should be stretched or not.

    - **Cardholder's picture:** Dynamic cardholder picture that changes, depending on which cardholder credential you are printing. This image field links to the value *Cardholder* picture in the configuration database.

      TIP: If a cardholder's picture was taken in front of a chroma key screen, you can make the picture background transparent. This is helpful if you are creating a badge template that has an image in the background.

    - **File:** Static image selected from a file.

    In the **Color and border** widget, you can use the following tools:

    - **Fill:** Use to modify the fill color of an inserted object like a square or oval.
    - **Border:** Use to modify the border color of an inserted object.
    - **Opacity:** Use to modify the opacity of an inserted object.
    - **Border thickness:** Use to modify the thickness of the inserted object's border

13. If you added text to the template, select the text to edit it using the options in the **Text** widget.

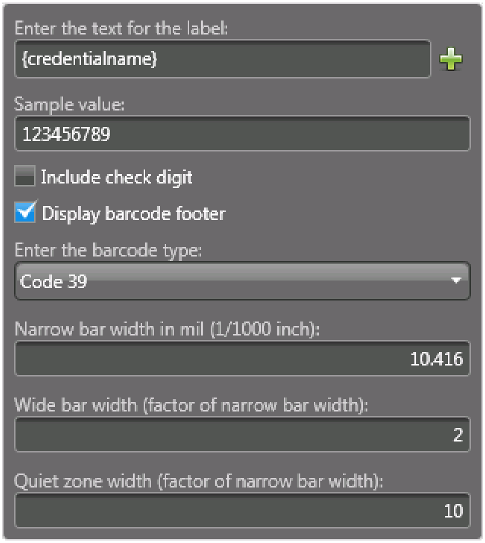
    Right-click the text field to select the **Z order**, the text **Border**, **Font**, **Color**, and **Alignment**.

    In the **Text** widget, you can use the following tools:

    - Click **Add field** (➕) to add a dynamic cardholder or credential field. You can mix static text with the dynamic fields.
    - Click **Fill** to set the text color.
    - Click **Align left**, **center**, or **right** to set the text alignment.
    - Click **Wrap text if too long** to turn on text wrapping.

      If text wrapping is turned on, the system will wrap the text if it is too long to fit inside the text box, without changing the font size. If text wrapping is turned off, the system will fit the text inside the text box by changing the font size.

14. If you added a barcode to the template, right-click the barcode, and then click **Properties** to edit it. The data on the barcode can be static or use dynamic credential properties.



Enter the text for the label:

{credentialname}

Sample value:

123456789

□ Include check digit

☑ Display barcode footer

Enter the barcode type:

Code 39

Narrow bar width in mil (1/1000 inch):

10.416

Wide bar width (factor of narrow bar width):

2

Quiet zone width (factor of narrow bar width):

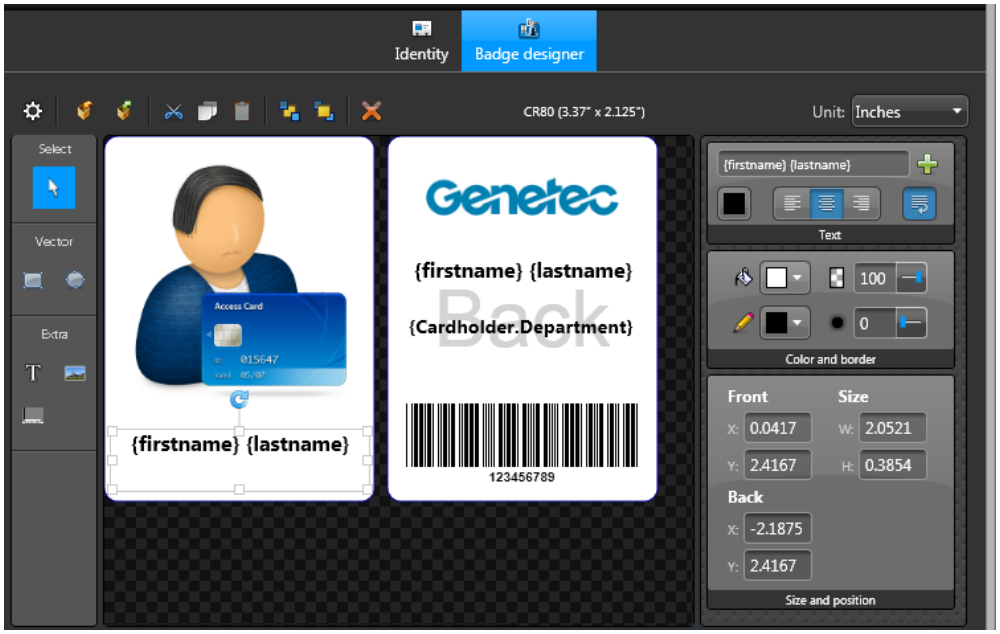
10

15 In the **Size and position** section, select where the text, image, or barcode is located on the badge, and its width and height.

16 Click **Apply**.

Example

Here is a sample badge template with objects already inserted:



Unit: Inches

{firstname} {lastname}

100

0

Front

X: 0.0417

Y: 2.4167

Size

W: 2.0521

H: 0.3854

Back

X: -2.1875

Y: 2.4167

- Two different images have been inserted. One is dynamic, and the other is static:
  - The dynamic cardholder picture appears on the front of the card.
  - The static image appears on the back of the card. It is the company logo that is displayed on every card.
- Three dynamic text fields have been inserted:
  - **{Firstname} {lastname}** appears on the front of the card. The text printed will be taken from the configuration database and we will see *first name, (space), last name*. The text is centered and text wrapping is turned on.

  - **{Firstname} {lastname}** appears on the back of the card. This is the same as the name field on the front except with a smaller font size, and text wrapping is turned off.
  - **{Cardholder.Department}** *Custom field* that was created for the cardholder entity.
- A barcode has been inserted, containing dynamic data. It displays the credential name, using the barcode type Code 39.

Viewing print previews of badge templates

After you design a new badge template, you can see what it is going to look like on a credential card.

To view a print preview of a badge template:

1 Open the **Access control** task, and click the **Credentials** view.

2 Select the credential that you want to preview badge template with, and then click the **Badge templates** tab.

33

Global cardholder management

This section includes the following topics:

Global cardholder management

Global cardholder management (GCM) is used to synchronize cardholders between independent Security Center installations.

GCM allows you to have a central repository of cardholder information for your entire organization, whether this information is managed from a central office or by individual regional offices. The different locations can have their independent installations share information with a centralized human resource management system.

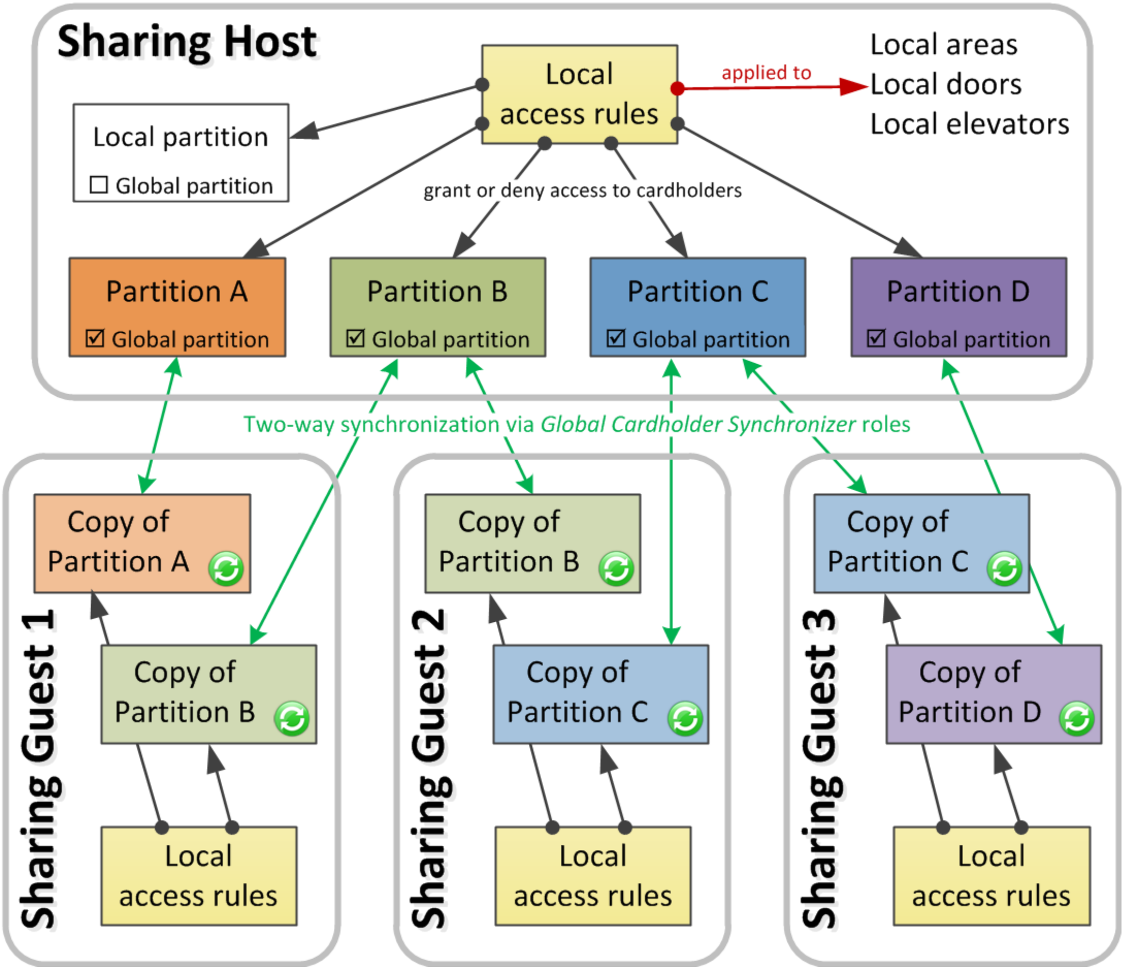
Each local office continues to manage the employees working at their local office, such as maintaining the employee profiles, photo ID’s, credentials, and so on. For employees that need to travel from site to site, that same information can be shared among all sites within the organization.

With global cardholder management, you can do the following:

- Create global cardholders from a central location (for example your head office) and synchronize them at remote Security Center systems that operate independently of the central system and of each other.
- Allow local system administrators to decide which areas global cardholders can or cannot access at their local facilities.
- Allow local system administrators to make changes to global cardholders and their related entities, and synchronize those changes with other sharing systems.
- Allow local system administrators to keep exclusive ownership of their local cardholders and related entities, while sharing global cardholders with other systems.

Architecture of Global cardholder management

In order to share cardholders across multiple independent Security Center systems, one of the system must act as the *sharing host*, while the others act as *sharing guests*.



Sharing host system

The sharing host is the Security Center system you choose to *initiate* the sharing process, by creating a *global partition* on that system. All *cardholders*, *cardholder groups*, *credentials*, and *badge templates* which are members of the global partition automatically become available for sharing. Other types of entities can be part of the global partition, but will not be visible to the sharing guests.

The sharing host owns the *master copy* of the global partition and the entities that are in it. All changes made by the sharing guests to the content of the global partition must first be validated by the sharing host before they are propagated to other sharing parties.

The global partition is like a central database, the sharing host is like the database server, while the sharing guests are like the database clients. There is no limit to the number of global partitions a host system can share.

Sharing guest systems

The sharing guest is a Security Center system that *participates* in the sharing process. Participation is achieved by creating a Global Cardholder Synchronizer (GCS) role on that system, and using it to connect the sharing guest to the sharing host.

As the sharing guest administrator, you can decide which partitions shared by the host are of interest to your system. The GCS role then creates a copy of the selected shared partitions and entities on your local system. Only *cardholders*, *cardholder groups*, *credentials*, and *badge templates* are eligible for sharing. The shared entities are visually identified with a green icon (●) superimposed over the regular entity icon.

You can assign local access rules and credentials to global cardholders to grant them access to your local areas, doors, and elevators. You can create, modify, and delete entities from the global partition. The actions you can perform depend on the rights of the *user* representing the GCS role on the sharing host. All changes made to global entities on the guest system must be validated on the host system. All modifications rejected on the host system are also rejected on your local system.

Differences between Federation™ and GCM

Global cardholder management (GCM) and *Federation* are both used for sharing information in Security Center, but cardholders and other information are shared differently.

The following table highlights the differences between GCM and Federation.

BEST PRACTICE: Use GCM and Federation™ together on the same system to complement each other.

Federation (applied to access control)	Global Cardholder Management (GCM)
Purpose: Central activity/event monitoring	Purpose: Sharing of a central configuration
Allows an organization to *monitor* from a central location (Federation™ host), the access control events and activities at independent remote locations (federated sites).	Allows an organization to *share* the common configuration of access control entities, hosted at a central location (sharing host), with independent remote locations (sharing guests).
The Federation™ host uses the Security Center Federation™ role to connect to the remote sites.	The remote sites use the Global Cardholder Synchronizer role to connect to the sharing host.
Entities created at remote sites are federated at the central system.	Entities created at the central system are shared at the remote sites.
The Federation™ host can observe, but cannot change anything on the remote sites.	The remote site can create, modify, and delete the entities that are shared by the host with all other remote sites (two-way synchronization).
A federated site has no visibility on what is going on at the federation host or other federated sites.	All sharing guests have the same read/write access to all shared (global) entities, while maintaining full ownership of the local entities.
Almost all entities that generate events can be federated (monitored).	Only cardholders, cardholder groups, credentials, and badge templates can be shared.
Custom fields are not federated.	All custom fields and data types are shared.
A federated cardholder can be granted access to the facility managed by the Federation™ host, but not the reverse.	A global cardholder can be granted access to all facilities participating in the sharing.

Related Topics

Global cardholder management rules and restrictions on page 583

Differences between Active Directory integration and GCM

Global cardholder management (GCM) and Active Directory integration are both used to centralize the management of cardholder information in Security Center, but their approach is different.

The following table highlights the differences between GCM and Active Directory integration.

BEST PRACTICE: Use Active Directory integration and GCM in tandem. The sharing host should be the only system that integrates with the Active Directory. This solution keeps the Active Directory protected on the corporate LAN, while the sharing host only pushes the employee information that need to be shared to the satellite systems.

Active Directory integration	Global Cardholder Management (GCM)
Purpose: Centralized employee (users and cardholders) security management	Purpose: Centralized employee (cardholders) security management
Allows an organization to *manage* the employee information from a central location, and share it with a single Security Center system (users and cardholders).	Allows an organization to *manage* the cardholder information from a central location, and share it with all Security Center systems within the organization.
The corporate directory service is the information source. Security Center gets the employee information from the corporate directory service.	One Security Center system acts as the information source (sharing host), and shares it with all other Security Center systems within the organization (sharing guests).
The Security Center system connects to the information source (directory service) through the Active Directory role.	The sharing guests connect to the information source (sharing host) through the Global Cardholder Synchronizer role.
Custom fields defined on the Active Directory can be linked to Security Center custom fields.	All custom fields and data types are shared.
The shared employee information can only be modified on the Active Directory. Only the cardholder picture can be loaded in Security Center and updated on the Active Directory.	The shared information can be modified by all sharing parties. The sharing host validates and propagates the changes to all sharing parties.
The source information can only be shared with one Security Center system. If multiple Security Center systems need to share the same information, they need to connect individually to the corporate directory service.	The central Security Center system can share the cardholder information with as many satellite Security Center systems as necessary.

About Global Cardholder Synchronizers

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

Only a single instance of this role is permitted on each system.

The Global Cardholder Synchronizer can synchronize the host and the guest using the following three ways:

- **On demand:** The guest system is synchronized only when it is requested by a user.
- **On schedule:** The guest system is synchronized on schedule using a scheduled task.

The guest-to-host synchronization is always performed immediately by the GCS role, because all changes to the shared partitions must be validated by the host system before they can be accepted by the guest system. The host system processes the change requests on a first come, first served basis. The Global Cardholder Synchronizer (GCS) role must stay connected to the sharing host to keep the local copies of the *global entities* synchronized with the host.

Global cardholder management rules and restrictions

The are some rules and restrictions that apply when using Global cardholder management.

Before you start globally managing your cardholders, read the following rules and restrictions.

Rules concerning local and global partitions

- A sharing guest cannot have more than one host. Only one instance of the GCS role is allowed per system.
- A global partition cannot be modified on a sharing guest, but its members can.What the sharing guest is actually allowed to modify is subject to the privileges of user assigned to the GCS role.
- No system is allowed to share what it does not own. Two-tier sharing is not permitted. An effect of this rule is that a local partition cannot be converted into a global partition if it contains global entities, unless it is performed on the host system.
- Adding a local entity to a global partition transfers the ownership of that entity from its local owner (sharing guest) to the partition owner (sharing host).
- Deleting a global entity on a sharing guest also deletes it on the sharing host, unless that entity also belongs to another global partition, in which case, only its membership is removed from the first partition.

Rules concerning local and global entities

- An entity is global by virtue of its membership to a global partition.This means that a cardholder does not automatically become global simply because its parent cardholder group is global.
- Local access rules can apply to local and global cardholders alike.Access rules are never shared. This ensures that local administrators always have full control over the security of their local facilities.
- Global cardholders/groups can become members of local cardholder groups.
- Local cardholders/groups cannot become members of global cardholder groups.An exception to this rule is when both entities belong to the same system. In this case, the local cardholder cannot be shared, although the cardholder group can.
- Both global and local credentials can be assigned to global cardholders.
- Global credentials cannot be assigned to local cardholders.
- Global credentials using custom card formats can be used and edited on the sharing guest. However, the credential data would only be visible if the corresponding custom card format (XML file) is also defined on the sharing guest using the *Custom card format editor* tool.

BEST PRACTICE: It is always recommended to apply access rules to cardholder groups rather than individual cardholders. For this reason, it is recommended to share the cardholders along with their parent cardholder groups. If this is not feasible for any reason, then we recommend that you create a local cardholder group for the global cardholders.

Rules concerning global custom fields and data types

- Custom fields and data types defined for global entities are automatically shared when the global entities are shared.
- Global custom field and data type definitions cannot be modified on the sharing guest.
- Global and local custom fields remain separate even when they use the same name. They are differentiated by their owner, which is the system that defines them.

- Global data types cannot be used to define local custom fields.
- Custom field values of global entities can be modified on sharing guests.
- Global custom fields also apply to local entities, but their values stay local.
- Local custom fields also apply to global entities, but their values stay local.
- When a guest system stops sharing a global partition, all local copies of the shared global entities, and the custom field values of the local entities are deleted.

BEST PRACTICE: If you are to implement GCM within your organization, we recommended that you define all custom fields and data types for global entities on the sharing host.

Rules concerning Federation™ and global entities

- If a *sharing host* also federates its *sharing guest*, only the local entities belonging to the sharing guest are federated. The entities that are shared will not be federated on the sharing host.
- The sharing host that also happens to be a *federation* host should not share the entities that it federates by adding them to a *global partition*, because it does not own the *federated entities*. An entity can only be shared by its rightful owner.For the federated entities to become shared, the federated system needs to be a sharing guest of the Federation™ host. This gives the Federation™ host the rights to share any of the federated entities.
- A sharing guest which happens to federate a third system cannot share its federated entities with the sharing host, because it is not the owner of the federated entities.
- If a sharing guest is federated by another system, both its local and global entities appear as federated entities on the Federation™ host.

Rules concerning Active Directory and global entities

- Cardholders and cardholder groups imported from an Active Directory can be added to a global partition on the sharing host.
- Cardholders and cardholder groups imported from an Active Directory that is local to the *sharing guest* cannot be added to a global partition because the Active Directory and the *sharing host* cannot both be owners of the shared cardholders.
- Global cardholders and cardholder groups imported from an Active Directory must only be modified through the directory service that owns them.

CAUTION: Although it is possible to modify global cardholders and cardholder groups imported from an Active Directory on the sharing guest, these changes are temporary. You lose the changes you made when the sharing host synchronizes with the Active Directory.

BEST PRACTICE: If all cardholder data entry must be centralized, the system that imports cardholders from your corporate Active Directory should act as the sharing host, and all modifications must be made using the directory service.

Related Topics

Importing security groups from an Active Directory on page 323
About federated entities on page 190
Custom card formats on page 567

Preparing to synchronize entities across sites

Before you can share and synchronize cardholders, cardholder groups, credentials, and badge templates with other sites, there are some steps you must take.

Before you begin

IMPORTANT: You should not attempt to deploy the Global Cardholder Management solution on your own if you intend to bring together systems that have data to share on both ends, meaning that both the sharing host and the sharing guest have existing data to share. If this is your situation, we strongly recommend that you book a technical consultation with a GTAP specialist.

To prepare synchronizing entities across sites:

1 Decide which Security Center system is going to be the sharing host.

The sharing host is typically the system running at your head office or the system that is synchronized with your corporate Active Directory.

2 If the sharing host is protected behind a firewall, open a port to allow the Global Cardholder Synchronizer role to connect to the sharing host.

3 Decide what types of updates the users on the guest systems are allowed to perform on the shared global partitions.

You can limit their range of actions by restricting the privileges of the user representing the GCS roles on the host system.

4 Make sure you follow the recommended best practice:

- Avoid assigning cardholders directly to access rules. Assign cardholder groups instead.
- Avoid assigning cardholders or cardholder groups directly to doors. Use access rules instead.

5 Back up the Directory database on all the systems you intend to synchronize and enable scheduled backups.

After you finish

Share entities across sites.

Related Topics

Common communication ports on page 941

Differences between Active Directory integration and GCM on page 581

Synchronizing entities across sites

To share information with other sites in your system, you can synchronize cardholders, cardholder groups, credentials, and badge templates.

Before you begin

Prepare the synchronization.

To synchronize entities across sites:

1 On the sharing host, create global partitions or change the status of local partitions to global.

2 Create a user with the proper level of administrative privileges over the shared entities to be used to connect the GCS roles to the sharing host.

You might have to create more than one user accounts if the sharing guests have different update requirements.

3 On each sharing guest system, create a GSC role and synchronize the sharing guest with the sharing host.

4 Assign local users and partition administrators to shared partitions (🌐).

5 Apply local access rules to shared cardholders (👤) and cardholder groups (👥).

NOTE: Custom card formats are not shared. If you have shared credentials that use custom card formats, the credentials will work on your local system, but you will not be able to view the card data fields unless the custom card format in use is also defined on your local system.

6 Create a scheduled task to periodically synchronize your local system to the host.

Related Topics

Custom card format editor tool on page 568

Setting up partitions for synchronizing

The entity synchronization is initiated on the *sharing host* by setting a partition as *a global* partition.

What you should know

You cannot share the *Public partition*.

To set up a partition for synchronizing:

1 Open the **Access control** task, and select the **Cardholders and credentials** view.

2 If the partitions are hidden, click **Show partitions** (🌐)

3 Select the partition you want to share.

4 Click the **Properties** tab, and switch the **Global partition** option to **ON**.

The partition is now visible to all GCS roles connected to this system. Only cardholders, cardholder groups, credentials, and badge templates are shared.

Synchronizing your system with the sharing host

You must create and configure the Global Cardholder Synchronizer (GCS) role to connect your local system to the sharing host.

To synchronize your system with the sharing host:

1 Open the **System** task, and click the **Roles** view.

2. Click **Add an entity** (✚) > **Global Cardholder Synchronizer**.
3. In the **Specific info** page, enter the following parameters, and then click **Next**.
   - **Server:** *Server* where this role will be hosted.
   - **Directory:** Sharing host’s *main server* name. If anything else than the default connection port (5500) is used, you must explicitly indicate the port number after the Directory name, separated by a colon. For example: `HostServer:5888`.
   - **Username and Password:** Credentials used to connect to the sharing host. The extent of what the sharing guest can do on the global partition will be limited by what this user can see and do on the sharing host.

     The user must have the *Global Cardholder Synchronizer* privilege on the sharing host in order to connect.
4. In the **Basic information** page, enter the name, description, and partition where the GCS role should be created.

   Partitions determine which Security Center users have access to this entity. Only users that are part of the partition can view or modify the GCS role.
5. Click **Next**, **Create**, and **Close**.

   A new Global Cardholder Synchronizer ( ) role is created. Wait a few seconds for the role to connect to the sharing host.
6. Click the **Properties** tab, and click **Refresh** (🔄) .

   The partitions shared by the host are listed under **Global partitions**.
7. Select the partitions you want your local system to share and click **Apply**.
8. Click **Synchronize** (⇅).

   The GCS role creates a local copy of all shared entities on your system. This might take a while depending on how many entities you are sharing.

After you finish

Configure the global entities you shared so they can be used on your local system.

Sharing entities with other sites

You share an entity by adding it to a global partition. This can be done from both the *sharing host* or the *sharing guest*. You can also create a new entity directly in a global partition.

What you should know

A *global entity* is an entity that is shared across multiple independent Security Center systems by virtue of its membership to a *global partition*. Only cardholders, cardholder groups, credentials, and badge templates are eligible for sharing.

To share an entity with another site:

1. Open the **Access control** task, and select the **Cardholders and credentials** view.
2. If the partitions are hidden, click **Show partitions** (🌐)
3. Select the global partition you want to share it from, and click the **Properties** tab.
4. Under the **Members** section, click **Add** (➕).
5. In the **Search** dialog box that appears, pick the entity you want to share, and click **Select**.

   On the sharing guest, only cardholders, cardholder groups, credentials, and badge templates can be added to a global partition.

On the sharing host, the effect of this action is immediately visible. On a sharing guest, the newly shared entity does not appear until after a synchronization is performed on their GSC role.

Related Topics
Global Cardholder Synchronizer configuration tabs on page 872

Stopping entity sharing with other sites

You stop sharing an entity by removing it from its global partition. This can be done from both the *sharing host* or the *sharing guest*.

What you should know

If you remove a shared entity from the sharing guest system, the entity is converted from a global entity to a local entity.

CAUTION: Removing a shared entity from a global partition deletes it from all other systems that might be sharing it, even from the sharing host.

To stop sharing an entity with another site:

1. Open the **Access control** task, and select the **Cardholders and credentials** view.
2. If the partitions are hidden, click **Show partitions** (🌐)
3. In the **Members** section, select the entity you want to stop sharing, and click **Remove** (❌).
4. To confirm the action, click **Remove**.

After you finish

Any entity removed from a partition ends up in the root partition. If the root partition is not where you want it to be, move it to another local partition.

Overriding synchronized cardholder statuses

If the GCS role is disconnected from the sharing host, and you need to change a cardholder status, you can override the entity synchronization.

What you should know

If the GCS role is disconnected from the sharing host, all global entities at the sharing guest become inactive (red), and you can no longer make any changes to them because they cannot be validated by the sharing host. However, if you urgently need to deactivate a cardholder (for example, if an employee has just been fired) you can temporarily *override* the synchronization.

To override the status of a synchronized cardholder:

1 Open the **Access control** task, and click the **Cardholders and Credentials** view.

2 Select the global cardholder you need to activate or deactivate.

3 Click the **Properties** tab, and switch the **Status** option to **Override**.

 The cardholder icon changes to . You can now change the cardholder’s status.

4 Make the necessary changes and click **Apply**.

After you finish

When the connection with the sharing host is re-established, turn the synchronization on again.

34

Import tool

This section includes the following topics:

About the Import tool

Import tool is a tool that allows you to import cardholders, cardholder groups, and credentials from a CSV (Comma Separated Values) file.

The CSV file must be plain text with delimiters (commas, spaces, periods, and so on) to separate the fields. The delimited fields in the text files would represent values like first name, last name, cardholder group, path and filename of employee photo, and so on.

The *Import tool* Security Center license option must be enabled in your system for this tool to be available. Only administrative users can use this tool.

You can use the import tool on a schedule, using the *Import from file* action.

How you can use the Import tool

You can use the Import tool to do the following:

- Import credentials alone (credential name, card format, facility code and card number, status, and the *partition* the credential belongs to).
- Import cardholders alone (cardholder name, description, picture, email, status, *custom fields*, and the group and partition the cardholder belongs to).
- Import cardholders and credentials together (in this case, the cardholder and the credential are specified on the same line and automatically linked together).
- Replace old credentials with new ones.

Limitations of the Import tool

If you are importing multiple cardholders who are members of different partitions, and there is either no cardholder group or only one cardholder group specified in the CSV file, the imported cardholders are added to all the partitions.

Related Topics
Replacing credentials on page 598
Scheduled tasks on page 183

CSV files and the Import tool

For you to be able to import CSV files using the Import tool, the CSV file needs to follow a certain format and include specific information for each type of entity. These files can be created from an Excel spreadsheet.

Minimum information required in CSV files

The information found in the CSV file must be coherent or it will not be accepted by the Import tool. When required information is missing, the *Next* button in the Bindings page is disabled. Each type of imported entity requires a minimum amount of information.

The following table describes what is required for each type of entity.

Entity type	Minimum information required
Credential	You have the choice of two credential keys: • Supply all fields required by a given card format. • Supply the *Credential card data*. If you choose a custom card format, all fields required by your card format must be bound to a column in the CSV file. Otherwise, the CSV file will be rejected. When credential are being imported, either one of these two keys must be present. If both keys are missing values, the line will be discarded. If both keys are present, only the card data is imported.
Cardholder	The default cardholder key is the combination of the cardholder's first and last name. One of these two fields must be bound to a CSV column if cardholders are to be imported. When cardholders are being imported, all CSV lines must have a value in at least one of these two fields. If not, the line would be discarded.
Cardholder group	Only the cardholder group name is required. Missing the cardholder group will not cause a line to be discarded.
Partition	Only the partition name is required. Missing the partition name will not cause a line to be discarded.

Format of the CSV file

Below is an example file called *EmployeeData.csv*, containing 3 new cardholders to import. It can be created from an Excel spreadsheet by doing "save as" and selecting the .csv format".

The sample file contains the following 4 lines of text:

```
#First name,Last name,Cardholder description,Cardholder email,Picture,
Cardholder group,Cardholder status,Credential name,Facility code,Card
 number,Credential status

Abdoulai,Koffi,Market Analyst,akoffi@genetec.com,C:\Data\Cardholder\Pictures\
Abdoulai Koffi.png,Marketing,Yes,82968378,102,8,active

Andrew,Smith,Sales Representative,asmith@genetec.com,C:\Data\Cardholder\Pictures\
Andrew Smith.png,Sales,Yes,82748590,101,12,active

Audrey,Williams,Technical Writer,awilliams@genetec.com,C:\Data\Cardholder\Pictures\
Audrey Williams.png,TechWriters,Yes,83748952,104,18,active
```

The first row is a comment line, listing the cardholder and credential fields that are included in the CSV file as a reference. The following three rows contain the fields that will be imported. You also can add additional custom fields if they have been created for cardholder or credentials in Security Center.

Custom field limitations

You can import cardholder and credential custom field values from CSV files with the following limitations:

- You cannot import custom fields using the *Entity* data type.
- Custom fields using the *Date* data type must be imported with the format ‘YYYY-MM-DD’.
- The Import tool performance decreases as the number of custom fields per imported record increases.
- When you have a large number of custom fields per record, the number of records you can import at once might also be limited. For example, if your records contain 100 custom fields each, including a 25 KB image data field, you can only import 1000 records at a time.

Related Topics
Database fields supported by the Import tool on page 599
About custom fields on page 69

Notes about imported entity names

Security Center supports multiple entities with the same name. If a cardholder already exists in Security Center with the same first and last name combination as one being imported, only the first matching cardholder found in the Security Center will be updated (for example, with a new description from the imported CSV file).

If there are two cardholder groups with the same name (for example, created in two different partitions) and an imported cardholder is assigned to one of these cardholder groups, the cardholder will be assigned to the first cardholder group found. The same logic also applies to partitions.

If the same cardholder is imported twice, each time with a different cardholder group, in the end, the cardholder will belong to both cardholder groups. Again, the same logic applies to partitions.

However, the association between cardholders and credentials might be treated differently, depending on whether the credential is part of the cardholder key or not.

Example

If the cardholder key is only composed of the cardholder's first and last names. The result of importing the following CSV file is the creation of a new cardholder: First name = Joe, Last name = Dalton, Email = JDalton@genetec.com, and with two card credentials (12/555 and 12/556).

First name	Last name	Facility code	Card number	Email
Joe	Dalton	12	555	jdalton@acme.com
Joe	Dalton	12	556	jdalton@acme.com

However, if the credential is also part of the cardholder key, the same CSV file will generate two separate cardholders with the same first name, last name and email address.

Importing cardholders and credentials

To accelerate the setup of your system, you can import cardholders and credentials from a CSV file instead of creating them manually in Security Center.

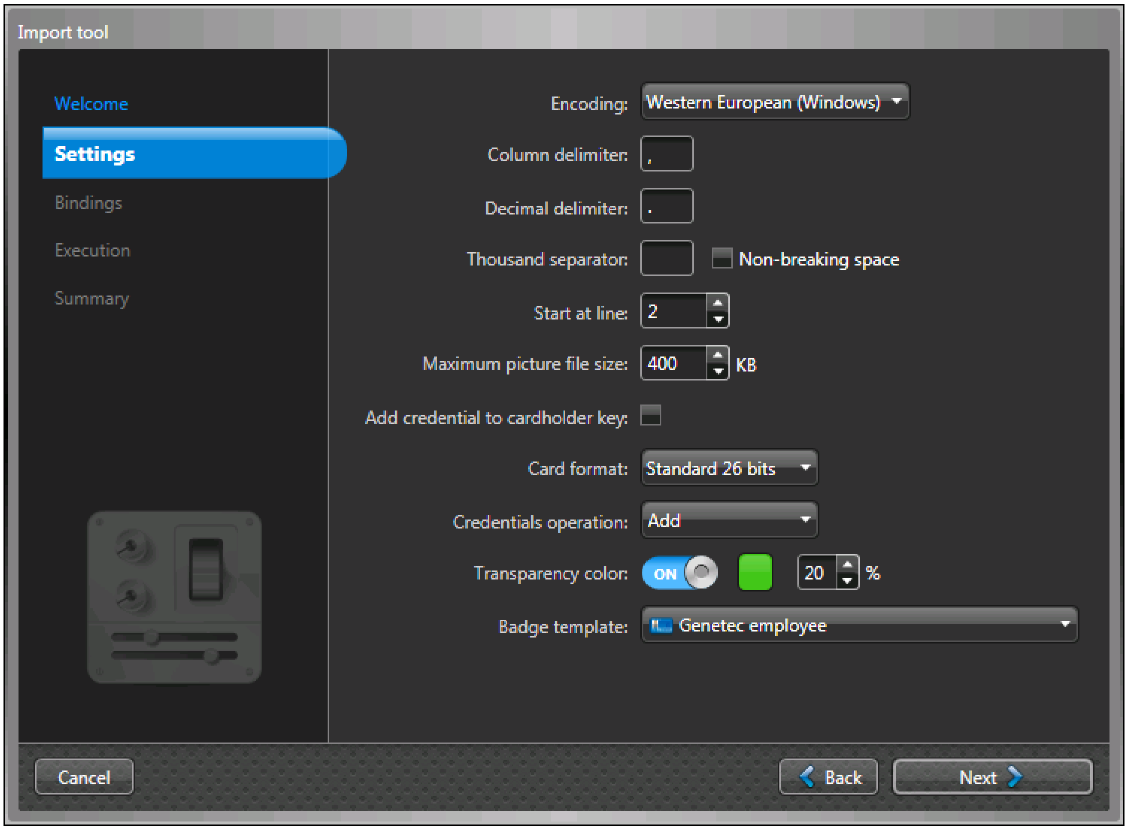
To import a cardholder or credential:

1 From the home page, click **Tools** > **Import tool**.

2 Enter the path to the CSV file you want to import, and click **Next**.

3 In the **Settings** page, set the **Encoding** type.

This is the character encoding used by the selected CSV file. The default selection is the default encoding used on your PC. If you open the CSV file on your PC and see all the characters displayed correctly, you do not need to change the default settings.



Encoding: Western European (Windows)
Column delimiter: ,
Decimal delimiter: .
Thousand separator: □ Non-breaking space
Start at line: 2
Maximum picture file size: 400 KB
Add credential to cardholder key: □
Card format: Standard 26 bits
Credentials operation: Add
Transparency color: ON 🟩 20 %
Badge template: Genetec employee

4 Set the CSV field delimiters (Column, Decimal, Thousand).

On first use, the tool takes the delimiter settings from Windows Regional Options (**Control Panel** > **Region and Language** > **Additional settings**). After the first use, the tool remembers the last delimiter settings you used. By default, Microsoft Excel also uses the field delimiters from Windows Regional Options when saving a CSV file. This can be overridden in Excel. It is recommended that you open the CSV file in WordPad to confirm the formatting delimiters obtained. When using a space as the **Thousands separator**, you can specify whether the space is non-breaking or not.

5 Set where the import is to start.

The first line in a CSV file is 1. You can choose to start the import at any line you want. For example, you can skip the first line and use it as column headings or a comment line. A comment line is a line with the hash character (#) in column 1.

6 (Optional) Set the maximum size for picture files.

Large picture files (like the ones produced by digital cameras) can very quickly use up the configuration database and impact performance. To minimize the impact of large picture files, the Import tool automatically reduces their sizes before loading them. It does this by reducing the resolution of the image until its file size falls below the **Maximum picture file size** limit. The default value is taken from your access control system settings. Changing its value in the Import tool also changes your system settings.

7 Add the credential as part of the cardholder key.

By default, the Import tool uses the combination of the first and last name to identify cardholders. If a cardholder already exists in the database, it is updated with the information read from the CSV file. If it does not, it is added. Using just the first and last names to differentiate cardholders might not be enough. One solution is to combine the credential information to the cardholder key. This is done by selecting the option **Add credential to cardholder key**. With this option, two lines from the CSV file refer to the same cardholder only if they contain the same cardholder first name, last name and credential data.

NOTE: This option is only applicable when both cardholders and credentials are imported from the same CSV file. When this solution is not applicable, other cardholder information can be used to strengthen the cardholder identification.

8 (Optional) Set the default **Card format**.

The default card format is only used when no credential card format is specified in the CSV file or when the field identified as **Card format** in the CSV file is blank.

9 Select one of the following **Credential operation** options:

- **Add:** This is the default option. All credentials read from the CSV file are added as entities to your system. If a credential already exists in your database, it will be updated.
- **Replace:** This option allows you to replace old credentials with new ones. In the **Bindings** page that comes next, you will find additional field options to specify the old (*previous*) and new credential values.

10 (Optional) Set the background transparency of the imported cardholder pictures.

If the cardholder pictures you are importing were taken in front of a chroma key screen, you can make the picture background transparent. This is helpful if you created a badge template that has an image in the background.

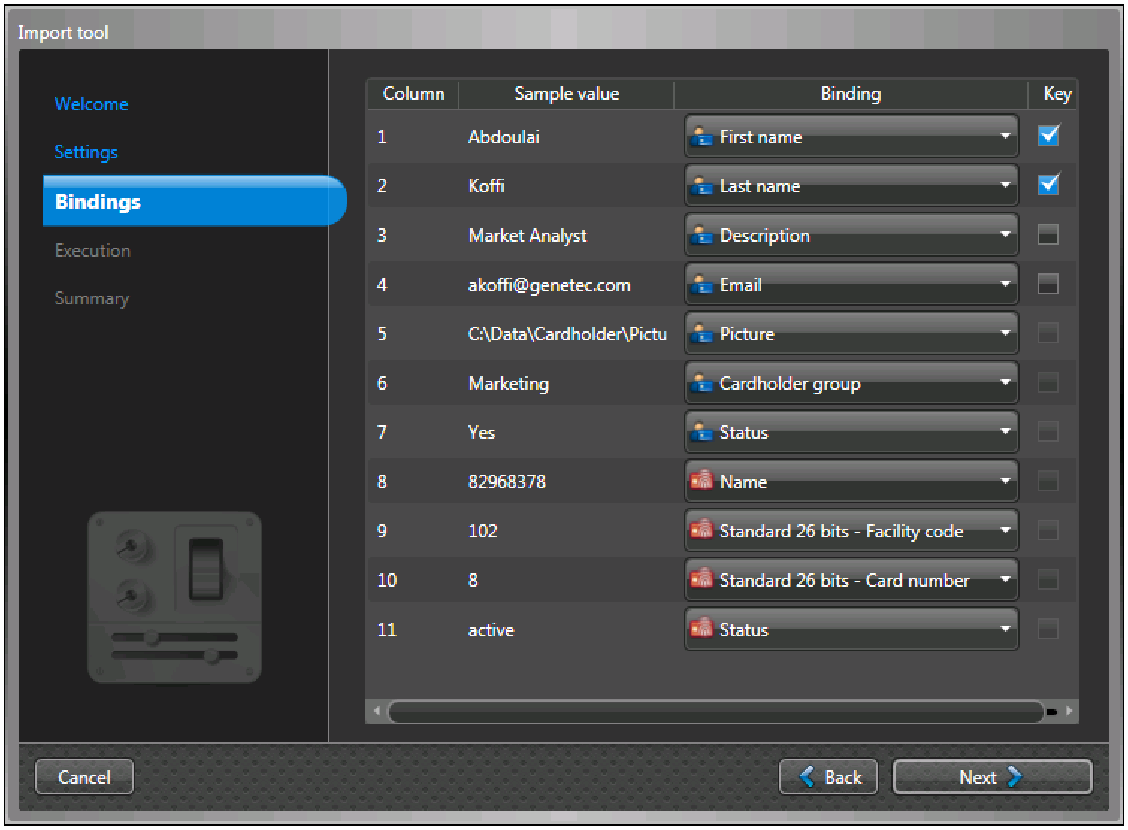
a) Set the **Transparency color** option to **ON**.
b) Select the color of the chroma key screen the cardholder pictures were taken in front of (usually green or blue).
c) Set transparency percentage.

11 (Optional) Set a default **Badge template** for the imported cardholders.

The badge templates available are ones you have already created in Config Tool.

12 Click **Next**.

The **Bindings** page appears, which displays sample data from the first row to be imported from your file. The first row to be imported is the **Start line**.



Column	Sample value	Binding	Key
1	Abdoulai	First name	☑
2	Koffi	Last name	☑
3	Market Analyst	Description	□
4	akoffi@genetec.com	Email	□
5	C:\Data\Cardholder\Pictu	Picture	□
6	Marketing	Cardholder group	□
7	Yes	Status	□
8	82968378	Name	□
9	102	Standard 26 bits - Facility code	□
10	8	Standard 26 bits - Card number	□
11	active	Status	□

13 Bind each sample value to the database field that it should be imported to.

If you need to skip a column in your CSV file, just leave the **Binding** column blank.

NOTE: The information read from the CSV file is used to create new entities in your system. For entities like cardholders and credentials, a minimum amount of information is required. If the information is incomplete, you will not be able to move to the next step.

14 (Optional) Add more fields to the cardholder key.

When you need more than the first and last name to differentiate cardholders, you can supplement the cardholder key with additional information.This is done by selecting the **Key** check box next to each field you want to add to the cardholder key. Not all fields can be part of the cardholder key. The check box is disabled if a field is not eligible.

TIP: The other method to strengthen the cardholder identification is to add the credential data to the cardholder key.

15 Click **Next**.

The Import tool imports the contents of your CSV file into the database. A summary window will appear confirming the number of entities imported and the number of errors encountered.

16 Click 📋 to copy and paste the contents of the report.

17 Click **Close**.

Related Topics

Database fields supported by the Import tool on page 599
CSV files and the Import tool on page 592
Defining the maximum file size of pictures on page 542
Replacing credentials on page 598
Designing badge templates on page 573

Replacing credentials

If you have multiple credentials that must be replaced, you can replace them all at the same time, using the *Import* tool.

Before you begin

Create a CSV file with both old and new credential values. Each line must contain both the old credential and the new credential to replace it with.

What you should know

The old and new credential must use the same card format. If the new credentials are to be assigned to the same cardholders, they must also be specified in the CSV file, and cannot be different than the current cardholder of the old credentials.

For example, replacing credentials is helpful if you want to give all the employees in your company new ID cards.

To replace a credential:

1 From the home page, click **Tools** > **Import tool**.

2 Enter the path to the CSV file you want to import, and click **Next**.

3 In the **Settings** page, select **Replace** as **Credentials operation**, and click **Next**.

4 In the **Bindings** page, bind the old credential values with the fields labelled as **(previous value)**, the new credential values with the fields not labelled as **(previous value)**.

5 Click **Next**.

The Import tool changes the status of the old credential to **Inactive**, while creating the new credential as **Active**. If the cardholders are also imported in the same file, the new credentials are associated to the cardholders.

The result of the operation are displayed in a summary window.

6 Click 📋 to copy and paste the contents of the report.

7 Click **Close**.

Related Topics

Importing cardholders and credentials on page 595

Database fields supported by the Import tool

Using the Import tool, you can import many database fields from a CSV file.

Field name	Field type	Description
Card format	Unsigned integer or string	Credential card format.You can use one of the following values: • 0 = Standard 26 bits • 1 = HID H10306 34 Bits • 2 = HID H10302 37 Bits • 3 = HID H10304 37 Bits • 4 = HID Corporate 1000 (35 Bits) To specify a custom card format, you must spell it in exactly the same way as you created it. If no card format is specified in a CSV line, the default format specified on the import settings page is used.
{Format} - Field name	Standard card format	You can specify a field in a specific card format, including custom card formats.
{Format} - Field name (previous value)	Standard card format	Field of an old credential to replace. These "(previous value)" choices appear only if you selected *Replace* as *Credential operation*
Cardholder <Field name>	As defined by the custom field	Cardholder custom field.
Cardholder group	String	Name of the cardholder group the cardholder should belong to. If the cardholder group does not exist, it will be created in the same partition as the cardholder.
Credential <Field name>	As defined by the custom field	Credential custom field.
Credential card data	String	The card data field allows the user to fill in the data for both standard and custom card formats. When this field is specified, the facility code and the card number fields are ignored. For all standard card formats, the string must contain the facility code followed by the card number. The accepted separators are the '/' and '|' characters. For example "35/20508" corresponds to Facility code= 35 and Card number = 20508. For a custom card format, the data should be arranged according to the custom card format definition.

Field name	Field type	Description
👤 **Description**	String	Cardholder entity description.
👤 **Email**	String	Cardholder email address.
👤 **First name**	String	Cardholder first name. This field is part of the default cardholder key.
👤 **Last name**	String	Cardholder last name. This field is part of the default cardholder key.
💳 **Name**	String	Credential entity name. If no name is specified, the default value “Imported credential” or “Unassigned imported credential” is used.
👤 **Partition**	String	Name of the partition the cardholder should belong to. If the partition does not exist, it will be created. If it is not specified, the cardholder is put in the system partition.
💳 **Partition**	String	Name of the partition the credential should belong to. If the partition does not exist, it will be created. If it is not specified, the credential is put in the system partition.
👤 **Picture**	String	Path to a cardholder picture file (bmp, jpg, gif, or png). The path must reference a file located on the local machine or on the network.
💳 **PIN**	Unsigned integer	Credential corresponding to a PIN. Valid range is between 0 and 65535.
👤 **Status**	Boolean	Cardholder status. The following values are accepted (not case sensitive): • 1, True, Yes = Profile enabled • 0, False, No = Profile disabled
💳 **Status**	String	Credential status. The following values are accepted (not case sensitive): • Active • Inactive • Lost • Stolen • Expired

Related Topics
About partitions on page 282
CSV files and the Import tool on page 592
Creating custom card formats on page 569

Replacing credentials on page 598
How credential card formats work with Active Directory in Security Center on page 566

35

Testing access control system

This section includes the following topics:

Access troubleshooter tool

The Access troubleshooter tool allows you to test and troubleshoot your access control system after it is set up, such as your access rules, and door and elevator configurations.

If you have a large system, you might have multiple schedules (Office hours/Office closed/Holidays/Weekends/Special events), multiple areas and sub-areas, multiple cardholder groups, and so on. As you build your system, and continue to create entities, the basic access logic applied at a door can become more difficult to determine.

You can use the Access troubleshooter to find out the following:

- Who is allowed to pass through an access point at a given date and time
- Which access points a cardholder is allowed to use at a given date and time
- Why a given cardholder can or cannot use an access point at a given date and time

The Access troubleshooter is most accurate when examining an event that just occurred. When using the troubleshooter to investigate a past event (for example, an access denied event), keep in mind that your settings might have changed since that event occurred. The troubleshooter does not take past settings into consideration. It only evaluates a situation based on the current settings.

Testing access rules at doors and elevators

You can find out who has the right to pass through a *door side* or elevator floor at a given date and time, using the *Access troubleshooter* tool.

What you should know

The door troubleshooter does not examine each cardholder’s credentials. You can further diagnose the cardholder’s access rights by clicking the Access diagnosis tab ().

To test the access rules at a door or elevator:

1 From the home page, click **Tools** > **Access troubleshooter** .

2 In the *Access troubleshooter* dialog box, click the *Door troubleshooter* tab.

3 Select the date and time you want to the troubleshooter to base its evaluation on.
Only *access rules* are evaluated based on the specified date and time.

4 Select the access point that you want the troubleshooter to examine:

- If you select a door, specify a door side.
- If you select an elevator, specify a floor.

5 Click **Go**.

The active cardholders who have the rights to use the selected access point at the specified time, based on the current access rules, are listed.

Related Topics
Testing cardholder access rights based on credentials on page 607

Identifying who is granted access to doors and elevators

You can verify which cardholders are granted access to a particular *door side* or elevator floor at a specific date and time, using the *Door troubleshooter* report.

What you should know

This report is helpful, because it allows you to see what the configuration of a door or elevator is, and determine if their properties must be adjusted.The door troubleshooter does not examine each cardholder's credentials. You can further diagnose the cardholder's access rights using the *Access troubleshooter* tool.

To identify who is granted access to a door or elevator:

1. From the home page, open the **Door troubleshooter** task.
2. In the *Filters* tab, select a date and time for the report.
3. Select a door or elevator you want to investigate.
4. From the **Access point** drop-down list, select the access point (door side or elevator floor) you want to verify.
5. Click **Generate report**.

   All cardholders who can go through the selected access point at the specified time are listed in the report pane.

After you finish

If necessary, test your access control configuration.

Related Topics

Testing access rules at doors and elevators on page 604
Creating doors on page 511
Creating elevators on page 518
Searching for entities on page 58

Report pane columns for the Door troubleshooter task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Cardholder:** Cardholder entity name.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.

Identifying who is granted/denied access at access points

You can find out which cardholders are currently granted or denied access to selected areas, doors, and elevators, using the *Cardholder access rights* report.

What you should know

This report is helpful because it allows you to see where a cardholder can go, and when, and determine if their access rule properties must be adjusted.

TIP: Perform your query on one access point at a time, so your report is more specific.

To identify who is granted/denied access at an access point:

1. From the home page, open the **Cardholder access rights** task.
2. Set up query filters for your report. Choose one or more of the following filters:
   - **Doors - Areas - Elevators:** Restrict the search to activities that took place at certain doors, areas, and elevators.
3. Click **Generate report**.

   The cardholders associated with the selected access point through an access rule are listed in the report pane. The results indicate if the cardholder is granted or denied access, and by which access rule.
4. To show a cardholder in a tile, double-click or drag a cardholder from the report pane to the canvas.
5. To view additional cardholder information in the tile, click ⓘ.

After you finish

If necessary, modify the cardholder's access rights.

Related Topics
Assigning access rules to cardholders on page 538

Report pane columns for the Cardholder access rights task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Cardholder:** Cardholder entity name.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Denied access by:** Access rules denying access to at least one of the selected entities to the cardholder.
- **First name:** Cardholder or visitor’s first name.
- **Granted access by:** Access rules granting the cardholder access to at least one of the selected entities (area, door, etc.).
- **Last name:** Cardholder or visitor’s last name.
- **Member of:** All groups the cardholder belongs to.
- **Picture:** Cardholder or visitor’s picture.

Testing cardholder access rights

You can find out which access points a cardholder is allowed to use at a given date and time, using the *Cardholder troubleshooter* tab in the Access troubleshooter tool.

What you should know

The cardholder troubleshooter does not examine each cardholder's credentials. You can further diagnose the cardholder's access rights by clicking the Access diagnosis tab ().

To troubleshoot a cardholder's access rights:

1. From the home page, click **Tools** > **Access troubleshooter** .
2. In the *Access troubleshooter* dialog box, click the *Cardholder troubleshooter* tab.
3. Select the date and time you want to the troubleshooter to base its evaluation on. Only *access rules* are evaluated based on the specified date and time.
4. Select the cardholder that you want the troubleshooter to examine. Instead of a cardholder, you can also select a *credential* or a visitor.

   The entities that are currently inactive are greyed out.
5. Click **Go**.

The access points that the selected cardholder (or visitor) has the right to use at the specified time, based on the current access rules, are listed.

Testing cardholder access rights based on credentials

You can diagnose why a cardholder with a given credential can, or cannot access a given *door* or *elevator*, at a given date and time, using the *Access diagnosis* tab in the Access troubleshooter tool.

To test a cardholder's access rights based on their credential:

1. From the home page, click **Tools** > **Access troubleshooter** .
2. In the *Access troubleshooter* dialog box, click the **Access diagnosis** () tab.
3. Select the date and time you want to the troubleshooter to base its evaluation on.
4. Select the cardholder you want to examine. Instead of a cardholder, you can also select a credential or a visitor.
5. If the selected cardholder has more than one credential, specify the one you want to examine.
6. Select an access point to examine.
   - If you select a door, specify a door side.
   - If you select an elevator, specify a floor.
7. Click **Go**.

The troubleshooter produces a diagnosis based on the current system configuration, taking into consideration the access rules, and both the cardholder's and the credential's activation and expiration dates.

Viewing credential properties of cardholders

You can view credential properties (status, assigned cardholder, card format, credential code, custom properties, and so on) of cardholders, using the *Credential configuration* report.

What you should know

For example, the Credential configuration report is helpful if you requested a credential for a cardholder, and want to see if it was activated. If you search by cardholder, the *Credential status* column indicates whether the credential is in the *Requested* or *Active* state. You can also search if there are any credentials currently listed as lost or stolen.

To view the credential properties of a cardholder:

1. Open the **Credential configuration** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **Credential:** Specify whether or not the credential is assigned.
   - **Cardholders:** Restrict the search to certain cardholders.
   - **Credential information:** Restrict the search to specific card formats, facility codes, or card numbers.
   - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
   - **Status:** The status of the cardholder or visitor's profile: Active; Expired; Inactive; Lost; Stolen. Not all statuses are available for every task.
3. Click **Generate report**.

   The credential properties the selected cardholder are listed in the report pane.
4. To show a cardholder in a tile, double-click or drag a cardholder from the report pane to the canvas.
5. To view additional cardholder information in the tile, click ℹ.

Report pane columns for the Credential configuration task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Cardholder status:** The cardholder's profile status.
- **Credential:** Credential name used by the cardholder.
- **Credential activation date:** Time the cardholder's credential was activated.
- **Credential code:** Facility code and card number.
- **Credential expiration date:** Time the cardholder's credential expired.
- **Credential status:** The status of the cardholder or visitor's credential: Active; Inactive.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Email address:** Cardholder or visitor's email address.
- **First name:** Cardholder or visitor's first name.

- **Last name:** Cardholder or visitor’s last name.
- **Picture:** Cardholder or visitor’s picture.
- **PIN:** Credential PIN.

Viewing properties of cardholder group members

You can find out the members of a cardholder group, and view any associated cardholder properties (first name, last name, picture, status, custom properties, and so on) of the cardholders, using the *Cardholder configuration* task.

What you should know

You can search for a specific cardholder group to see which cardholders are members of that group. You also can search for expired or inactive cardholders to see if there are any in your system.

To view the properties of cardholder group members:

1. From the home page, open the **Cardholder configuration** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **Activation date:** Time the cardholder or visitor's profile was activated.
   - **Expiration date:** Specify a time range for when the cardholder or visitor's profile expired.
   - **Unused cards:** Specify a time range for how long a cardholder or visitor's credential has not been used.
   - **Status:** The status of the cardholder or visitor's profile: Active; Expired; Inactive; Lost; Stolen. Not all statuses are available for every task.
   - **First name:** Cardholder or visitor's first name.
   - **Last name:** Cardholder or visitor's last name.
   - **Email address:** Cardholder or visitor's email address.
   - **Description:** Restrict the search to entries that contain this text string.
   - **Picture:** Cardholder or visitor's picture.
   - **Partition:** Partition that the entity is a member of.
   - **Cardholder groups:** Restrict the search to specific cardholder groups.
   - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
   - **Credentials:** Restrict the search to specific credentials.
   - **Credential status:** The status of the cardholder or visitor's credential: Active; Expired; Inactive; Lost; Stolen. Not all statuses are available for every task.
   - **Credential information:** Restrict the search to specific card formats, facility codes, or card numbers.
3. Click **Generate report**.

   The cardholders that are members of the selected cardholder groups are listed in the report pane.
4. To show a cardholder in a tile, double-click or drag a cardholder from the report pane to the canvas.
5. To view additional cardholder information in the tile, click ⓘ.

Report pane columns for the Cardholder configuration task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Cardholder:** Cardholder entity name.
- **Cardholder activation date:** Time the cardholder's profile was activated.
- **Cardholder expiration date:** Time the cardholder's profile expired.

- **Cardholder status:** The cardholder’s profile status.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Email address:** Cardholder or visitor’s email address.
- **First name:** Cardholder or visitor’s first name.
- **Last name:** Cardholder or visitor’s last name.
- **Member of:** All groups the cardholder belongs to.
- **Picture:** Cardholder or visitor’s picture.

Identifying which entities are affected by access rules

You can find out which entities and access points are affected by a given *access rule*, using the *Access rule configuration* report.

What you should know

In the report results, you can see the members of the access rule, such as the cardholders, doors, and the associated schedule. This helps you determine if you must add or remove entities, or adjust the schedule.

To identify which entities are affected by an access rule:

1. Open the **Access rule configuration** task.
2. Set up the query filters for your report. Choose one or more of the following:
   - **Access rule:** Select the access rule to investigate.
   - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
3. In the **Expand cardholder groups** option, select **Enable** to list the members of the affected cardholder groups in the report instead of the cardholder groups themselves.
4. In the **Include perimeter entities** option, select **Enable** to include the perimeter entities of the affected areas in the report.
5. Click **Generate report**.

   The entities and access points affected by this access rule are listed in the report pane.

Related Topics

Creating access rules on page 533

Report pane columns for the Access rule configuration task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Access point:** Access point involved (only applicable to areas, doors, and elevators).
- **Access rules:** Name of the access rules.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Icon:** Graphical representation of the affected entity type.
- **Member:** Name of the affected entity.
- **Type:** Affected entity type.

Viewing I/O configuration of access control units

You can view the I/O configurations (controlled access points, doors, and elevators) of access control units, using the *I/O configuration* report.

What you should know

For example, you can use the I/O configuration report to search a for a specific door, and see how the access through each door side is configured (REX, readers, I/O modules, and so on).

To view the I/O configuration of an access control unit:

1 Open the I/O configuration task.

2 Set up the query filters for your report. Choose one or more of the following filters:
- **Access control units:** Select the access control units to investigate.
- **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
- **Devices:** Select the devices to investigate.
- **Location:** Specify the areas where the devices are located.

3 Click **Generate report**.

The input and output configurations of the selected access control units are listed in the report pane.

Related Topics

Viewing properties of units on page 76

Report pane columns for the I/O configuration task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Access point:** Access point involved (only applicable to areas, doors, and elevators).
- **Access Manager:** Access Manager controlling the unit.
- **Controlling:** Door controlled by the device.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **IP address:** IP address of the unit or computer that generated the event.
- **Manufacturer:** Manufacturer of the unit.
- **Physical name:** Device name.
- **Unit:** Access control, video, intrusion detection, or LPR unit involved.
- **Unit type:** Type or model of unit involved.

36

Troubleshooting access control

This section includes the following topics:

Viewing access control health events

You can view health events related to access control entities, using the *Access control health history* report.

What you should know

This report is similar to the Health history report, but the query only looks for events that cause warnings, and includes only access control entities. The access control entities that can produce warnings include access control units, doors, areas, elevators, and zones.

To search for access control health events:

1 Open the **Access control health history** task.

2 Set up the query filters for your report. Choose one or more of the following filters:

- **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the last week or the last month.
- **Source entity:** Source entity of the event.

3 Click **Generate report**.

The access control health events are listed in the report pane.

Report pane columns for the Access control health history task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **Firmware version:** Firmware version installed on the unit that generated the event.
- **IP address:** IP address of the unit or computer that generated the event.
- **Product type:** Model of the unit involved.
- **Source:** Source entity associated to the alarm or event.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, intrusion detection, or LPR unit involved.

Investigating events related to access control units

You can investigate events related to access control units, using the *Access control unit events* report.

What you should know

For example, you can use the *Access control unit events* report to see if any critical events happened relating to *access control unit* in the last week (for example, *Hardware tamper*), by searching for that event and setting the time range.

To investigate access control unit events:

1. From the home page, open the **Access control unit events** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
   - **Access control units:** Select the access control units to investigate.
   - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
   - **Events:** Select the events of interest. The event types available depend on the task you are using.
   - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the last week or the last month.
3. Click **Generate report**.

   The access control unit events are listed in the report pane.

   NOTE: If you have Access Managers that are offline when you launch the query, you'll get an error message for each one of them, even though they are not related to the selected access control units. This is because the system has no way of knowing whether the selected units were managed by one of them in the past or not.

Report pane columns for the Access control unit events task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **Occurrence period:** Period when the event occurred.
- **Product type:** Model of the unit involved.
- **Tamper:** Name of the interface module that has been tampered with.
- **Unit:** Access control, video, intrusion detection, or LPR unit involved.

Moving access control units to a different Access Manager

If you want a different Access Manager role to manage and control an access control unit, for load balancing or another purpose, you can move the unit to another Access Manager using the *Move unit* tool.

Before you begin

Do the following:

- Make sure that the Access Manager role is on the same LAN as the access control unit it controls.
- Create the unit manufacturer extension.

To move an access control unit to a different Access Manager:

1 Temporarily deactivate both Access Managers.
  a) In the **Access control** task, right-click the Access Manager, and click **Maintenance** > **Deactivate role** ( ).
  b) In the confirmation dialog box that opens, click **Continue**.
     The Access Manager and all the access control units it controls turn red.
2 From the home page, click **Tools** > **Move unit**.
3 From the **Unit type** drop-down list, select **Access control unit**.
4 Under **Access Manager**, select the units you want to move.
5 Under **Access Manager**, select the new Access Manager role to control the unit.
6 Click **Move** > **Close**.

Preparing to replace an access control unit

Before you replace an access control unit with a new one, there are steps you must perform first.

Before you begin

You can only replace an access control unit with a new one if the two are of the same brand and model. The only exception to this rule is if you are replacing an HID VertX V1000 unit with a Synergis™ unit. In every case, the exact same interface modules (brand and model) must be attached to the new unit. If there is any difference other than the above mentioned exception, the unit replacement will not be accepted.

Before you replace an access control unit:

1. Backup the Directory database from Server Admin.
2. Physically disconnect the old unit, and make sure it is offline in Security Center ().
3. (Synergis™ unit only) Assemble and install the Synergis™ unit and its hardware components. For information, see the *Synergis™ Cloud Link Hardware Installation Guide*.
4. Physically disconnect the interface modules from the old unit and connect them to the new unit using the exact same channels.

   IMPORTANT: Do not change the physical address of the interface modules.

   If you are replacing an HID VertX V1000 unit with a Synergis™ unit, connect the subpanels (interface modules) found on each side of the V1000 to two different channels of the Synergis™ unit, for two interface modules on the same channel cannot have the same physical address.
5. (Synergis™ unit only) Configure the Synergis™ unit according to the interface modules attached to it. For more information, see the *Synergis™ Appliance Configuration Guide*.

After you finish

Replace the old unit with the new one.

Replacing access control units

If an access control unit fails and is offline in Security Center (), you can replace the unit with a compatible one. This process copies the configuration settings, associations to doors, elevators, and zones, and event logs from the old unit, so you do not have to configure the new one.

Before you begin

Prepare to replace your access control unit.

CAUTION: Not all settings are copied by the Unit replacement tool. If you were using supervised inputs on the old unit, you will have to reconfigure the inputs on the new unit.

To replace an access control unit:

1 Add the fully wired new access control unit to the Access Manager controlling the old unit. For a Synergis™ unit, see the *Synergis™ Appliance Configuration Guide*.

2 Temporarily deactivate the Access Manager.

a) In the *Access control* task, select the Access Manager, and click **Maintenance** > **Deactivate role** ( ).

b) In the confirmation dialog box that opens, click **Continue**.

The Access Manager and all the access control units controlled by the role turn red.

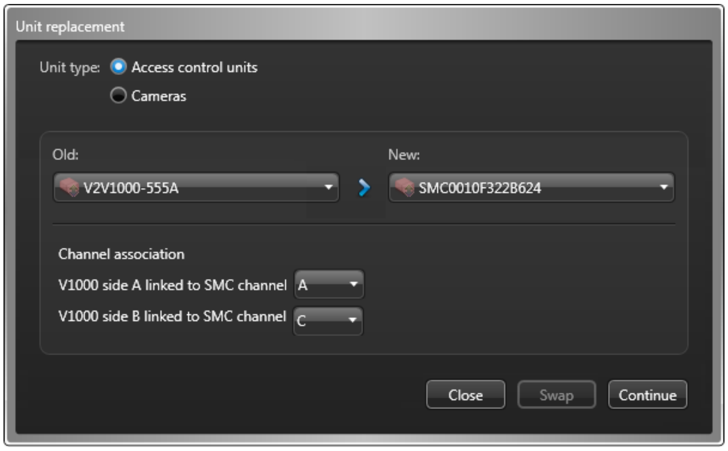
3 Click the home page, click **Tools** > **Unit replacement**.

4 In the **Unit type** option, select **Access control units**.

5 Select the **Old** and the **New** access control units.

6 Click **Swap**.

(V1000 to Synergis™ only) If the V1000 had subpanels (interface modules) using the same physical address, link the V1000 sides to the Synergis™ unit channels, and click **Continue**.



Unit replacement

Unit type: ● Access control units ○ Cameras

Old: V2V1000-555A

New: SMC0010F322B624

Channel association

V1000 side A linked to SMC channel A

V1000 side B linked to SMC channel C

The configuration settings of the old access control unit are copied to the new one.

7 In the **Access control** task, right-click the Access Manager, and click click **Maintenance** > **Activate role** ( ).

8 In the **Roles and units** view, select the new unit, and verify that the configuration settings are all correct.

9 Right-click the old unit, and click Delete ().

10 In the confirmation dialog box that opens, click **Continue**.

After you finish

If the inputs on the old unit were supervised, reconfigure them on the new unit.

Related Topics

Searching for entities using the search tool on page 58

Enabling or disabling support logs for access control units

The Synergis™ appliance can keep detailed logs for troubleshooting and support. You can manually enable or disable support logs if requested by Genetec™ Technical Assistance.

What you should know

You can enable or disable support logs for multiple units simultaneously in Security Center using the following instructions. You can also enable support logs for individual units in the Synergis™ Appliance Portal. For more information on configuring event logging options in the Synergis™ Appliance Portal, refer to the *Synergis™ Appliance Configuration Guide*.

To enable or disable support logs for access control units:

1 In Config Tool, open the *Access control* task and select the *Roles and units* view.

2 Under the Access Manager, select one or more access control units.

 NOTE: Clicking the Access Manager selects all control units enrolled under it.

3 From the right-click menu, or on the contextual command bar at the bottom of the screen, click **Maintenance**, and select **Enable unit support logs** or **Disable unit support logs**.

Troubleshooting: HID unit discovery and enrollment issues

If you cannot discover or enroll an HID access control unit, there are some common troubleshooting steps you can use to try and resolve the issues.

To troubleshoot why an HID unit cannot be discovered or enrolled:

1 Make sure that the computers Config Tool and *Access Manager* are running on are behind a firewall.

   Ports 4050 *TCP* and 4070 *UDP* must be unblocked.

2 Make sure that all Synergis-specific ports on page 624 are opened and unblocked.

3 *Make sure the HID VertX extension has been added to the Access Manager in Config Tool*.

4 Validate that the HID VertX extension is properly loaded in the Access Manager, as follows:

   a) To open a console session to the Access Manager, open a web browser, and go to the URL *http://(server name or IP)/Genetec/console*.

      NOTE: If you cannot connect to the console ensure that console access is enabled in the *Server Admin* , under the **Genetec Server** tab.

   b) Click the **Commands** tab at the top of the page.

   c) Under the column **User Commands** on the left, expand **Access Manager** and click **Status**.

   d) A status query is sent to the Access Manager and the response contains the extensions that are loaded.

   e) Ensure that the following line is shown in the status results: **HID VertX:4070** = X **units**.

5 Check if the unit has a static IP address.

6 If the unit's IP address is static, you must set the DNS, or the unit might have issues enrolling or connecting.

   a) To access the HID Configuration GUI, enter the unit's IP address in a web browser.

   b) In the HID Configuration GUI, set the primary and secondary DNS to the appropriate values.

      If you do not know your network's DNS, set the unit's own IP address as the primary and secondary DNS server.

7 Make sure there are no other applications blocking ports 4070, 4050, and 20:

   a) Stop the Access Manager.

   b) In Windows, click **Start** > **Run**, and type **cmd** to open the Command Prompt, and then run **netstat -na**.

Troubleshooting: HID units cannot be discovered

If you cannot discover an HID access control unit using the *Unit enrollment* tool, you can troubleshoot the cause of the issue.

Before you begin

Perform the common troubleshooting steps for resolving HID discovery and enrollment issues.

To troubleshoot why an HID unit cannot be discovered:

1 In the Advanced Setup of HID VertX web page, make sure the Host Name is set, and that is does not have more than 15 characters.

   The Host Name must be set, and it must have less than 15 characters to be discovered.

2 Make sure the unit is on the same network subnet as the computer where Config Tool is running.

   Discovery only works within the same *broadcast* domain.

3 Make sure the unit firmware is up to date.

For a list of supported firmware versions, see the *Security Center Release Notes*.

Troubleshooting: HID units cannot be enrolled

If you cannot enroll an HID access control unit, you can troubleshoot the cause of the issue.

Before you begin

Perform the common troubleshooting steps for resolving HID discovery and enrollment issues.

What you should know

If you are experiencing enrollment issues, the following can occur:

- Unit cannot be enrolled
- Unit is enrolled but its icon remains red
- Unit connects and disconnects continuously
- Unit begins enrolling and fails at 67%

To troubleshoot why an HID unit cannot be enrolled:

1 Check if there is connectivity to the unit, as follows:

   a) Ping the unit from the computer running the Access Manager: In Windows, click **Start** > **Run**, and type **cmd** to open the Command Prompt, and then run **ping w.x.y.z**.

      NOTE: w.x.y.z is the IP address of the unit.

      A report is generated. Make sure no packets were lost.

   b) Telnet the unit from the computer running the Access Manager to check its credentials: In Windows, click **Start** > **Run**, and type **cmd** to open the Command Prompt, and then run **telnet w.x.y.z**.

   c) Login to the unit (Default: user=root / password =pass).

      If the login is successful, there is connectivity to the unit.

2 Check if the unit is on the same network subnet as the computer where the Access Manager is running.

   If it is not, you can enroll the unit manually as long as you know its IP address (the unit must be set to use a static IP address).

3 Make sure the unit firmware and the interface board firmware is up to date.

   For a list of supported firmware versions, see the *Security Center Release Notes*.

4 Make sure the network card binding and *database* configuration for the Access Manager is set correctly.

5 If the Access Manager is behind a NAT, you must specify the translated host address for the Access Manager.

6 Make sure no other Access Manager is currently connected to the HID unit, as follows:

   a) Stop your Access Manager.

   b) Telnet the unit: In Windows, click **Start** > **Run**, and type **cmd** to open the Command Prompt, and then run **telnet w.x.y.z**.

   c) Login to the unit (Default: user=root / password =pass).

   d) At the prompt, type **netstat -na**.

      A list of network connections is shown. There should be no one connected to port 4050.

7 Make sure the HID units (and connected interfaces) are wired to not generate tamper or door held open alarms, access granted or access denied events.

Tamper and door held open alarms trigger repeatedly. Upon connection, any such alarms and events have to be downloaded from the unit which can slow-down the enrollment process. Symptoms of this is the unit is difficult to enroll, the unit connects and disconnects, or the unit beeps.

8 Upgrade the unit's firmware.

For a list of supported firmware versions, see the *Security Center Release Notes*.

Synergis-specific ports

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

Computer	Inbound	Outbound	Port usage
Access Manager	UDP/TCP 4070	UDP/TCP 4070	HID VertX/Edge controllers
			HID Vertx/Edge EVO controllers
	TCP 20	TCP 21, 23	HID VertX/Edge controllers
		TCP 4050	HID VertX/Edge controllers
			HID Vertx/Edge EVO controllers
		TCP 22	HID Vertx/Edge EVO controllers
		TCP 2000	Default Synergis™ unit discovery port (this port can be modified in Config Tool)

The *discovery port* of an HID unit is fixed at 4070. Once it is discovered, the unit is assigned to an *Access Manager* that uses the ports shown in the table above to control it.

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

Troubleshooting: Too many request to exit door events

If the logs for a door show far too many request to exit events for the actual amount of door activity, you can try to reduce the number of false request to exit events from the options in the door *Properties* tab.

What you should know

If your door is equipped with an automatic request to exit device (based on a *motion detection* sensor), sometimes a *request to exit* event is triggered when people are entering an area. Depending on the quality of the automatic request to exit device and how it is installed, the device might trigger on any activity near the door.

To reduce the number of request to exit door events:

1. From the Config Tool home page, open the *Area view* task.
2. Select the door that is causing the issues, and click the **Properties** tab.
3. Set the following **Request to exit** options as necessary:
   - **Time to ignore 'Request to exit' after granted access:** Ignore any requests to exits for this long after access has been granted.
   - **Unlock on request to exit:** Set to **ON** if a REX is being used, and you want to automatically grant the request to exit.
   - **Ignore 'Request to exit' events while door is open:** Do not generate REX when door is open.
   - **Time to ignore 'Request to exit' after door closure:** Once the door has closed, wait this long before generating any more *Request to exit* events.
4. Click **Apply**.

Troubleshooting: Credentials not working

If a *credential* does not work at a door or elevator, you can test the reason why access is denied.

What you should know

For a credential to be granted access at a given *door side* or elevator floor, the following conditions must be met:

- The credential's profile must be enabled
- The credential must be associated to a cardholder
- The cardholder's profile must be enabled
- There must be at least one *access rule* that specifically grants access for that cardholder or the cardholder's cardholder group.

If these settings are not correct, access is denied.

To troubleshoot why access is denied:

- Use the Access troubleshooter tool to determine why the cardholder does not have access to a door or elevator.

Troubleshooting: Cards not working at readers

If a card is not working at a door *reader*, you can troubleshoot the cause of this issue.

To troubleshoot why a credential is not working at a card reader:

1. Make sure you are using the right type of card technology for the reader.

   For example, some readers are multi-technology (can read 125 kHz and 13.56 MHz cards), and other readers can only read one card type.

2. Test if the card is defective by trying another card.
3. Test if the reader is installed too close to another reader by disconnecting the power to one reader.

   If the other reader starts to operate correctly, they were installed too closely. Readers emit an electromagnetic field that can interfere with other readers located nearby.

4. Test if your are using the proper cable for the reader by connecting a spare reader directly to the unit with a short cable.

   If the spare reader works, you should change the cable of the original reader. For the maximum cable length and type, see the reader and unit documentation.

Troubleshooting: Driver fails to install for HID OMNIKEY USB readers

If, each time you try to enroll a credential using an HID OMNIKEY USB reader, you see an error message from Windows indicating that the driver failed to install, there are some troubleshooting steps you can use to resolve the issue.

Before you begin

- Disconnect the OMNIKEY reader from your workstation.
- Close Security Desk and Config Tool.

What you should know

This issue typically occurs because Windows cannot find the appropriate driver for the reader. Because Windows will try to load the default USB driver, the reader can appear to work properly until you observe some undesirable behavior. To avoid such behaviors, it is recommended to install the driver that is specific to this type of readers provided by the manufacturer.

To troubleshoot the driver that fails to install:

1. Make sure that your OMNIKEY reader is compatible with Security Center and is configured properly.

   For a list of compatible devices and configuration settings, see Knowledge Base article KBA01374 on Genetec™ Technical Information Site.
2. Install the driver following the instructions provided in the *OMNIKEY Smart Card Reader User Guide*.

   You can obtain this guide by visiting HID's website at http://www.hidglobal.com/documents.
3. When installation is completed, start Security Desk, and then check that the reader is enabled.
4. Try to enroll a credential again.

The error message should not be displayed anymore.

Part VI

License plate recognition

This part includes the following chapters:

37

LPR at a glance

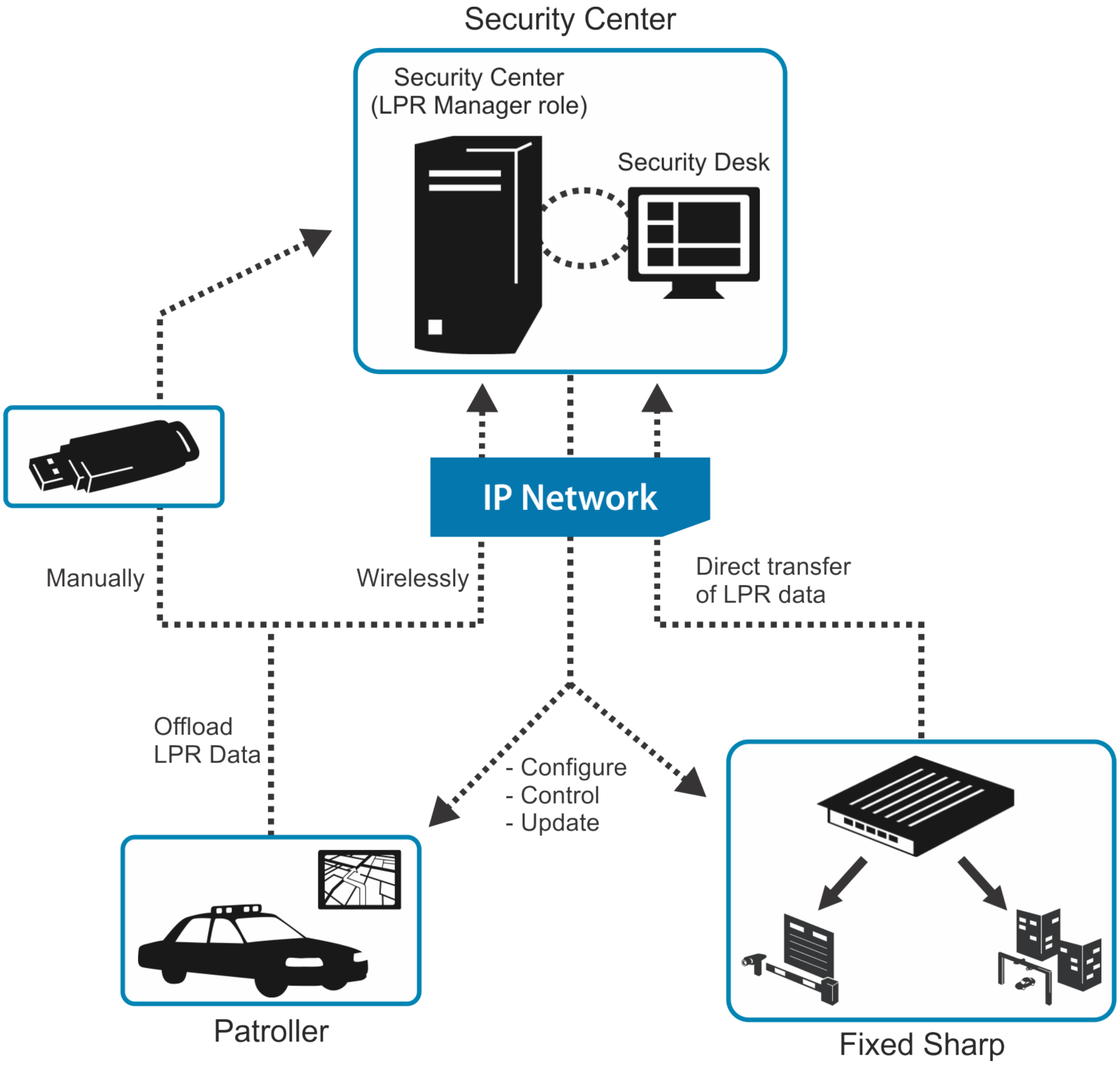
This section includes the following topics:

About AutoVu™

AutoVu™ is the IP license plate recognition (LPR) system of Security Center that automates the reading and verification of vehicle license plates.

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

The following diagram shows how a typical AutoVu™ system works:



Entities related to LPR

The LPR system supports many of the entities that are available in Security Center.

The following table lists the entities related to LPR.

Icon	Entity	Description
	LPR Manager	Role that stores all LPR data collected from the LPR units (fixed Sharps) and Patrollers that it manages.
	LPR unit	IP-based license plate recognition (LPR) device.
	Hotlist	List of wanted vehicles.
	Overtime rule	Type of hit rule that specifies a time limit for parking within a restricted area.
P	**Parking facility**	Defines a parking area or parking garage as a number of sectors and rows, to track vehicles inside that parking facility.
	Patroller	In-vehicle software that runs on board a mobile data computer (MDC), which verifies license plates.
	Permit	Defines a single parking permit holder list.
	Permit restriction	Type of hit rule that specifies where and when permit holders can park.
	User	Individual who uses Security Center applications.
	User group	Group of users sharing common characteristics.

About LPR Managers

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

Multiple instances of this role can be created on the system to provide scalability and partitioning. For example, different fleets of Patrollers can be managed by different *LPR Managers*, fixed Sharp units can be managed by different LPR Managers, and so on.

NOTE: For SharpX installations where LPR Processing Unit input/output control is required, you must also enroll the LPR Processing unit under the Archiver.

LPR Manager root folder

The root folder is the main folder on the computer hosting the LPR Manager. It is where all the configuration files are created, saved, and exchanged between the LPR Manager and the Patroller units it manages.

When you create a new LPR Manager role, the root folder is created automatically on your computer, located at: *C:\Genetec\AutoVu\RootFolder*. If you create multiple LPR Managers, new folders are created at the same location. For example, if you create three LPR Managers, Security Center automatically creates the following folders:

- *C:\Genetec\AutoVu\RootFolder1*
- *C:\Genetec\AutoVu\RootFolder2*
- *C:\Genetec\AutoVu\RootFolder3*

The LPR Manager root folder includes the following subfolders:

- **ManualTransfer:** Contains the configuration and data files to transfer to Patroller manually using a USB key or similar device.
- **Offload:** Contains the LPR data offloaded by Patroller.
- **Rules:** Contains the delta files used by Security Center to transfer hotlist and permit list changes. Do **not** copy or move anything in this folder.
- **Updates:** This folder appears when you first turn on the Update provider It contains Security Center and Patroller hotfixes, as well as Sharp service and firmware updates. Patroller hotfixes are automatically downloaded to Patroller whenever Patroller is connected to Security Center. Mobile Sharp units are updated through Patroller, and fixed Sharp units are updated through the network.

Configuring LPR Manager roles

To manage reads and hits collected by LPR units, you must first configure the LPR Manager role settings such as Patroller user groups, database retention periods, and so on.

Before you begin

Read the following before configuring the LPR Manager:

- If you are using SQL Server Express Edition, the database might be full before the retention period ends. Contact GTAP to help you evaluate whether SQL Server Express meets the requirements of your AutoVu™ system.

  NOTE: When using SQL Server Express, reducing retention period settings should not be used as a means to reduce the database size AFTER it has hit the 10GB upper limit. The retention cleanup algorithm is optimized to ensure that expired data is not presented to the user over rapidly reclaiming the used space on disk.
- If your computer is hosting more than one LPR Manager, each LPR Manager must have a different root folder.

What you should know

When you install Security Center, an LPR Manager role is created by default and assigned to the main server.

To configure the LPR Manager role:

1. From the home page, click **System** > **Roles**.
2. Select the LPR Manager you want to configure, and then click **Properties** > **General settings**.
3. To change the location of the LPR Manager's **Root folder**, browse to a different folder on the local machine, or create a new network folder (for example, your root folder can be on a network drive).
4. (Windows Vista or later only) If you have large hotlists or permit lists associated to individual Patroller units, turn on the **Optimize root folder disk space** option.

   IMPORTANT: If your root folder is on a network drive, the Genetec™ Server service must be configured to run using a domain user and not a local user.

   Turning this option on enables the use of symbolic links to reduce the Root folder's overall disk space, and optimize file transfer performance to the Patroller in-vehicle computer. After enabling this option in Security Center, you also must enable it in Windows on your server and client machines (you'll need administrator rights). On both the server and client machines, open Windows Command Prompt, and then type the following:

   - **To enable symbolic links:** Type `fsutil behavior set SymlinkEvaluation R2R:1`
   - **To disable symbolic links:** Type `fsutil behavior set SymlinkEvaluation R2R:0`.
5. From the **User group for Patrollers** drop-down list, select the user group that contains the list of users (and their passwords) who are allowed to log on to the Patrollers managed by the LPR Manager.

   This list is downloaded to the Patrollers. In Patroller Config Tool, if the Patroller *Logon type* is *Secure name* or *Secure name and password*, the Patroller user will be required to enter the username and password configured in Security Center. If secure logon names are in use, when a read or a hit occurs, in Security Desk you can view who was driving the vehicle.
6. In the **Retention period** section, specify how many days of LPR-related data Security Center can query:

   - **Patroller route retention period:** Number of days the Patroller *route* data (GPS positions) is kept in the database.

- **Hit retention period:** Number of days the hit data is kept in the database.
- **Read retention period:** Number of days the *license plate reads* are kept in the database.

  The Read retention period cannot exceed the Hit retention period. If the read retention is lower than the hit retention, only the reads that are associated with hits will be kept.
- **Event retention period:** Number of days the LPR events (License plate read, License plate hit) are to be kept in the database.
- **Hit image retention period:** Number of days the hit image data is kept in the database.

  The Hit image retention period cannot exceed the Hit retention period since an image is always associated to a hit.
- **Read image retention period:** Number of days the read image data is kept in the database.

  The Read image retention period cannot exceed the Read retention period.

The default value for each setting it 90, and the maximum is 4000 days. The LPR date that is older than the values specified do not appear in Security Center queries and reports (Hit reports, Read reports, and so on).

7 Click **Apply**.

The LPR Manager’s General settings are configured, and you can continue to customize your AutoVu™ system by configuring the other LPR Manager settings.

After you finish

If you have a large system, you can distribute the load by creating more LPR Manager roles and hosting them on separate *servers*.

Related Topics
LPR Manager - Properties tab on page 875
LPR Manager - Resources tab on page 881
About LPR Managers on page 633

About LPR units

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

The LPR device converts license plate numbers cropped from LPR and context camera images into a database searchable format.

AutoVu™ Sharp is the LPR unit used in Security Center AutoVu™ solutions. The Sharp includes license plate capturing and processing components, as well as digital video processing functions, enclosed in a ruggedized casing. Sharps can be deployed in mobile and fixed installations. A mobile installation is where the Sharp is mounted on a vehicle and is integrated into AutoVu™ Patroller (the in-vehicle software of the AutoVu™ LPR system), which in turn is integrated into Security Center. A fixed installation is where the Sharp is mounted in a fixed location, such as on a pole, and integrated directly into Security Center.

The LPR Manager automatically detects Sharps on the network and adds them to the Security Center system. It detects mobile Sharps through the AutoVu™ Patroller system they are connected to. It detects fixed Sharps directly through the Security Center *discovery port*.

LPR matcher

The LPR matcher is the AutoVu™ software engine that matches license plates captured by Sharp cameras to license plates in a data source such as a hotlist or permit list, or to previously captured license plates, such as for overtime enforcement. The LPR matcher determines if a plate read results in a hit.

Environment challenges, such as hidden plate characters or damaged plates, can affect the license plate read accuracy rate. The LPR matcher uses a variety of techniques to compensate for these challenges and improve the read accuracy rate. Think of each technique as opening a door wider to let in more possible plate matches. The wider you open the door, the more possible matches you allow, which affects the read accuracy rate.

How LPR matcher logic works

Real-world conditions make license plate recognition difficult. Some license plates may have characters that are hidden by dirt or snow, while other characters' paint may be faded or chipped. Some license plates have pictures, holograms, or even screws and rivets that can be misread as legitimate license plate characters.

If the LPR matcher were only capable of raising a hit based on an exact match, many plates that should be hits would instead be missed.

Example

A hotlist contains the plate ABC123. While on a patrol, a Sharp camera reads the license plate ABC12, but is unable to read the last character because the character's paint is chipped. If the LPR matcher were only capable of recognizing an exact match, it would ignore the plate read ABC12. If that last character was in fact a "3", then the patroller just drove past what should have been a legitimate hotlist hit.

The LPR matcher must be capable of more than just "yes/no" logic because the plate read ABC12 *might* be a match. It would be better to raise the hotlist hit, and let the Patroller operator decide whether or not the hit is legitimate. To do this, the LPR matcher uses different levels of "maybe" logic to allow for more possibilities for a plate match.

LPR matcher technique: OCR equivalence

The LPR matcher uses the "OCR equivalence" technique to improve plate read accuracy rate.

AutoVu™ uses Optical Character Recognition (OCR) to convert a license plate image into data that the LPR matcher can read. Depending on the font design, some plate characters can look very similar to other characters. These are called "OCR equivalent characters".

You can configure how the LPR matcher handles OCR equivalence by modifying the MatcherSettings.xml file. For more information, see MatcherSettings.xml file on page 643.

NOTE: You can also configure the following LPR matcher techniques in the MatcherSettings.xml file:

- Number of character differences (see LPR matcher technique: Number of character differences on page 639)
- Common and contiguous characters (see LPR matcher technique: Common and contiguous characters on page 640)

The default Latin-based OCR equivalent characters are the following:

- The number "0" and the letters "O", "D", and "Q".
- The number "1" and the letter "I".
- The number "2" and the letter "Z".

- The number “5” and the letter “S”
- The number “8” and the letter “B”.
- The number “6” and the letter “G”.

BEST PRACTICE: You should not allow more than two OCR equivalent characters because it results in too many false-positive matches.

Example

The following example uses a hotlist with the LPR matcher configured to allow for one OCR equivalent character:

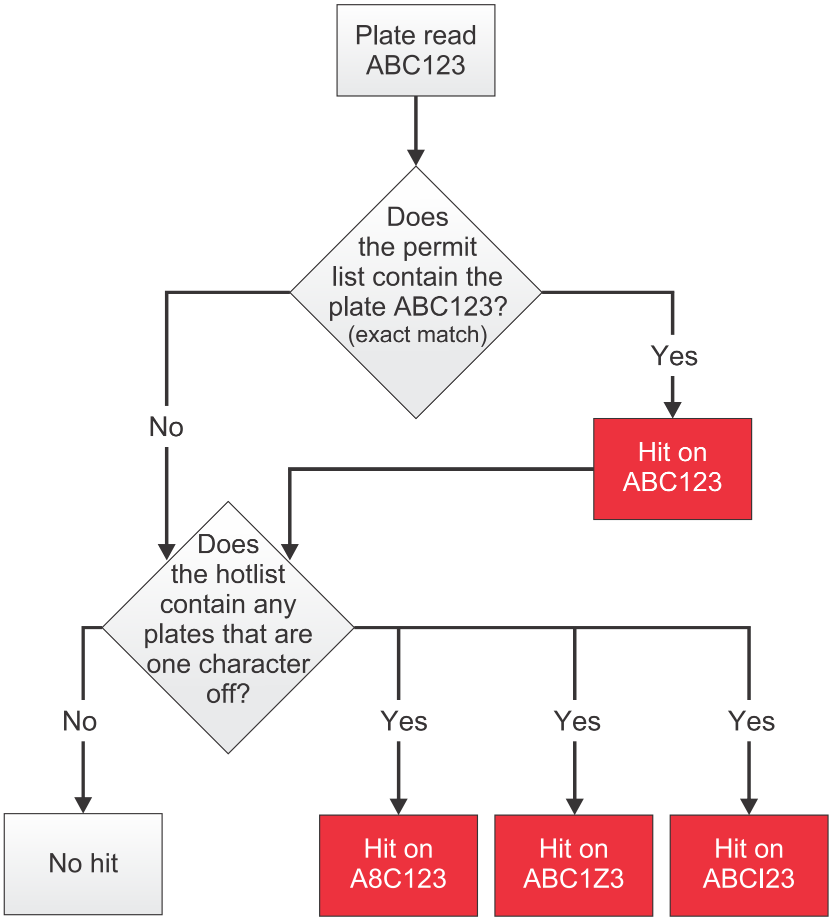


Plate read ABC123
Does the permit list contain the plate ABC123? (exact match)
Yes
No
Hit on ABC123
Does the hotlist contain any plates that are one character off?
No
Yes
Yes
Yes
No hit
Hit on A8C123
Hit on ABC1Z3
Hit on ABCI23

The LPR matcher finds the exact match ABC123 in the hotlist and raises a hit. It also looks for any plates that are one OCR equivalent character off, and finds A**8**C123, ABC1**Z**3, and ABC**I**23 in the hotlist, so it raises hits on them as well.

If the LPR matcher found the plate A**8**C**IZ**3 (three OCR equivalent characters off), it would not raise a hit. By configuring the LPR matcher to allow for only one OCR equivalent character, you've decided that anything more than that is not visually similar enough to the plate read for the LPR matcher to consider it a match.

LPR matcher technique: Number of character differences

The LPR matcher uses the "Number of character differences" technique to improve the plate read accuracy rate.

This technique allows for a difference in the number of characters between the plate read and the plate number in the data source (a hotlist for example). This allows the system to account for characters in the plate that cannot be read (faded paint, dirt, bad camera angle, and so on), and for objects on the plate that might be mistaken for legitimate characters (screws, rivets, pictures, and so on).

You can configure how the LPR matcher handles the "Number of character differences" by modifying the MatcherSettings.xml file. For more information, see MatcherSettings.xml file on page 643.

NOTE: You can also configure the following LPR matcher techniques in the MatcherSettings.xml file:

- OCR equivalence (see LPR matcher technique: OCR equivalence on page 637)
- Common and contiguous characters (see LPR matcher technique: Common and contiguous characters on page 640)

Example

The following example uses a hotlist with the LPR matcher configured to allow for *one* OCR equivalent character, and *one* difference in the number of characters allowed:

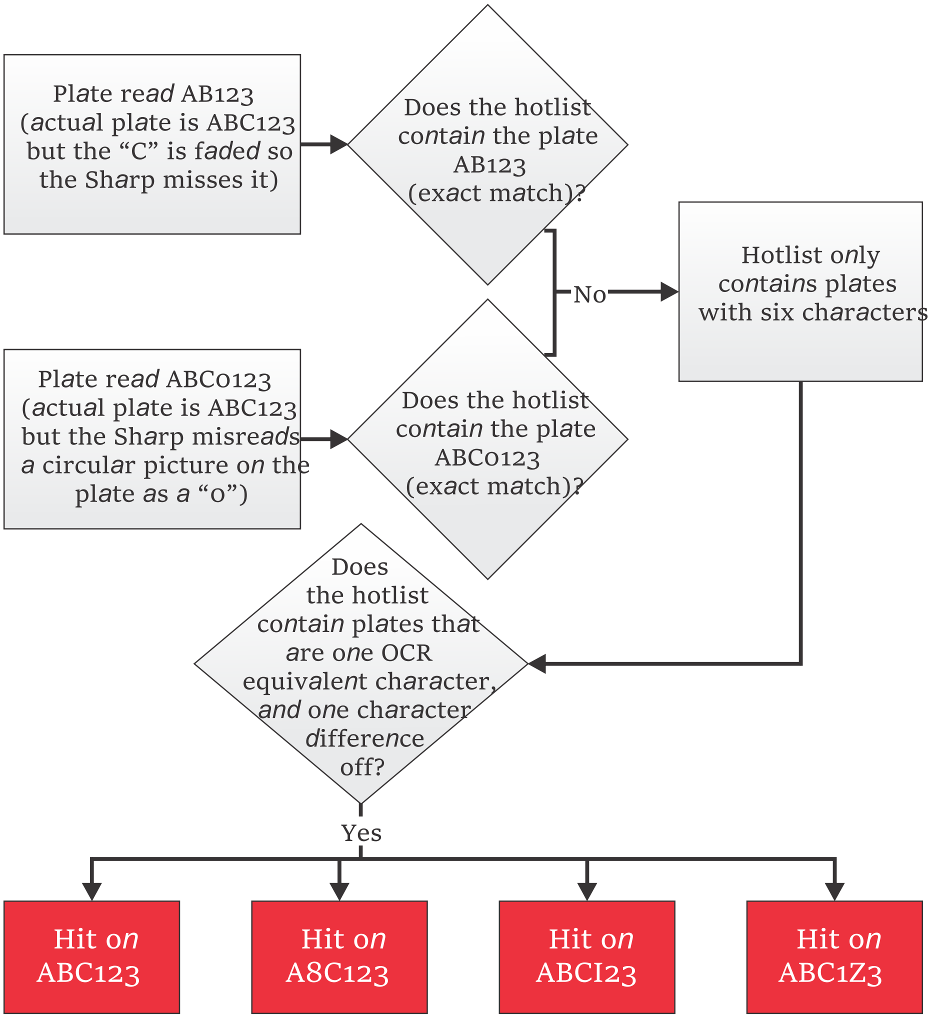


Plate read AB123 (actual plate is ABC123 but the "C" is faded so the Sharp misses it)
Does the hotlist contain the plate AB123 (exact match)?
Plate read ABC0123 (actual plate is ABC123 but the Sharp misreads a circular picture on the plate as a "o")
Does the hotlist contain the plate ABC0123 (exact match)?
No
Hotlist only contains plates with six characters
Does the hotlist contain plates that are one OCR equivalent character, and one character difference off?
Yes
Hit on ABC123
Hit on A8C123
Hit on ABCI23
Hit on ABC1Z3

Because you allowed for one OCR equivalent character *and* one character difference, the LPR matcher looks for both before it allows a match. This results in the following:

- There's no exact match possible for plate reads AB123 and ABC0123 because the hotlist contains only six-character plates.
- Both plate reads AB123 and ABC0123 match the plate ABC123 because you allowed for one character difference. It doesn't matter if it is one character more, or one character less than the matched plate.
- Both plate reads AB123 and ABC0123 match the plates A**8**C123, ABC**I**23, and ABC1**Z**3 because you allowed for one character difference, *and* one OCR equivalent character.

If you were using a permit list instead of a hotlist, *none* of the matched plates in the example would raise hits (you get a permit hit when a plate is *not* on the permit list).

LPR matcher technique: Common and contiguous characters

The LPR matcher uses the "Common and contiguous characters" technique to improve plate read accuracy rate. This allows you to define the number of common and contiguous characters that are allowed between two plate reads in order to generate a hit (sometimes called "fuzzy matching").

NOTE: This method is used for overtime parking enforcement only.

You can configure how the LPR matcher handles common and contiguous characters by modifying the MatcherSettings.xml file. For more information, see MatcherSettings.xml file on page 643.

NOTE: You can also configure the following LPR matcher techniques in the MatcherSettings.xml file:

- OCR equivalence (see LPR matcher technique: OCR equivalence on page 637)
- Number of character differences (see LPR matcher technique: Number of character differences on page 639)

The following settings are available when configuring common and contiguous characters:

- **Necessary common characters:** The minimum number of characters that need to be common to both the first and second plate read. The characters must also appear in the same order in the plate, but not necessarily in sequence.
- **Necessary contiguous characters:** Minimum character sequence length between the first and second plate read.

  In overtime enforcement, there is an extra margin of error because the LPR matcher is comparing a plate read against another plate read, not against a hotlist or permit list created by a human being.

Example

Here's an example with the LPR matcher configured to look for the default five common characters and four contiguous characters. The LPR matcher also allows for the default one OCR equivalent character, which can count as a common or contiguous character.

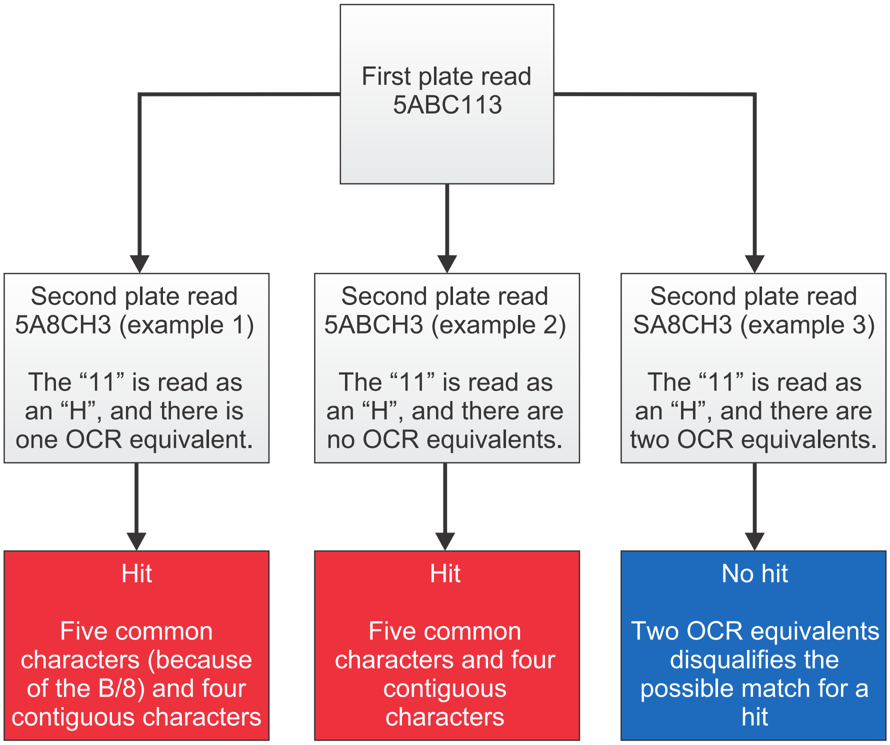

First plate read
5ABC113
Second plate read
5A8CH3 (example 1)
The “11” is read as an “H”, and there is one OCR equivalent.
Second plate read
5ABCH3 (example 2)
The “11” is read as an “H”, and there are no OCR equivalents.
Second plate read
SA8CH3 (example 3)
The “11” is read as an “H”, and there are two OCR equivalents.
Hit
Five common characters (because of the B/8) and four contiguous characters
Hit
Five common characters and four contiguous characters
No hit
Two OCR equivalents disqualifies the possible match for a hit

Plate read 5ABC113 matches with 5A8CH3 (example 1) and 5ABCH3 (example 2) because the following conditions are met:

- **OCR equivalence:** The OCR equivalents B and 8 are considered the same character and apply towards the common and contiguous character count.
- **Five common characters:** Both reads have 5, A, B/8, C, and 3 in common, and they all appear in the same order. The “3” is not in sequence, but it respects the order.

- **Four contiguous characters:** Both reads have 5, A, B/8, and C in sequence.

Plate read 5ABC113 does *not* match with SA8CH3 (example 3) because there are two OCR equivalents in the second read (S/5 and B/8). You allowed for only one OCR equivalent.

Using common and contiguous characters helps reduce the margin of error involved when both first and second plate reads are coming from the Sharp.

MatcherSettings.xml file

The *MatcherSettings.xml* file contains the settings for the techniques used by the LPR matcher: OCR equivalence, number of character differences, and common and contiguous characters.

The file is located on the computer hosting the Security Center Directory role, in the folder *C:\Program Files \Genetec Security Center 5.5*.

NOTE: If you have a mobile AutoVu™ system, a copy of the same file is located on the Patroller in-vehicle computer. You make your changes in the Security Center version of the file. The file on the Patroller computer is overwritten the next time Patroller connects to Security Center wirelessly, or when you manually transfer Patroller settings with a USB key.

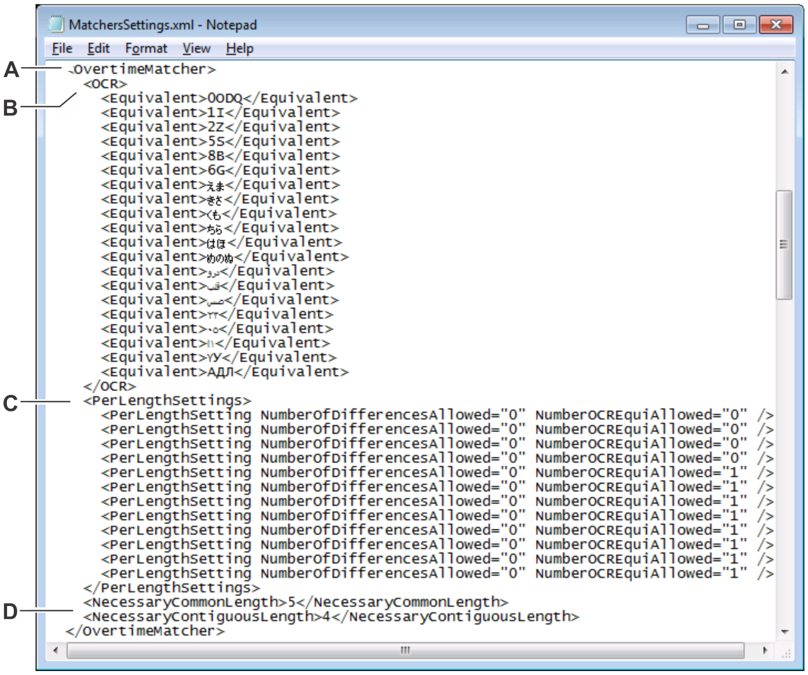
The *MatcherSettings.xml* file is composed of `<Matcher>` tags that define the settings for each type of matching scenario:

- <**HotlistMatcher**>**:** Settings for matching plate reads with hotlists.
- <**OvertimeMatcher**>**:** Settings for matching a plate read against all other plate reads in the Patroller database.
- <**PermitMatcher**>**:** Settings for matching plate reads with permit lists.
- <**MLPIMatcher**>**:** Settings for reconciling inventories in Security Desk.

The structure of the *MatcherSettings.xml* file allows you to have different behavior for the different enforcement scenarios. For example, to maximize your plate read accuracy rate in an enforcement scenario that includes both permits *and* hotlists, you'll typically want to use only OCR equivalence for the hotlist matcher, but also allow one difference in the number of characters for the permit matcher to decrease false-positives.

MatcherSettings.xml file example

The following is an example of the *MatcherSettings.xml* file:



```
<OvertimeMatcher>
  <OCR>
    <Equivalent>0ODQ</Equivalent>
    <Equivalent>1I</Equivalent>
    <Equivalent>2Z</Equivalent>
    <Equivalent>5S</Equivalent>
    <Equivalent>8B</Equivalent>
    <Equivalent>6G</Equivalent>
    <Equivalent>えま</Equivalent>
    <Equivalent>きさ</Equivalent>
    <Equivalent>くも</Equivalent>
    <Equivalent>ちら</Equivalent>
    <Equivalent>はほ</Equivalent>
    <Equivalent>めのぬ</Equivalent>
    <Equivalent>رو</Equivalent>
    <Equivalent>قب</Equivalent>
    <Equivalent>صس</Equivalent>
    <Equivalent>٢٣</Equivalent>
    <Equivalent>٠٥</Equivalent>
    <Equivalent>١ا</Equivalent>
    <Equivalent>YУ</Equivalent>
    <Equivalent>АДЛ</Equivalent>
  </OCR>
  <PerLengthSettings>
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
    <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  </PerLengthSettings>
  <NecessaryCommonLength>5</NecessaryCommonLength>
  <NecessaryContiguousLength>4</NecessaryContiguousLength>
</OvertimeMatcher>
```

A: Matcher-specific settings

Each enforcement type (hotlist, permit, overtime, and MLPI) has its specific settings listed between the opening and closing `<Matcher>` tags.

For example, overtime matcher settings are listed between `<OvertimeMatcher>` and `</OvertimeMatcher>`.

B: OCR equivalent characters

The default OCR equivalent characters for each enforcement type are listed as between `<OCR>` and `</OCR>`.

NOTE: The default OCR equivalent characters for each enforcement type are listed as between `<OCR>` and `</OCR>`.

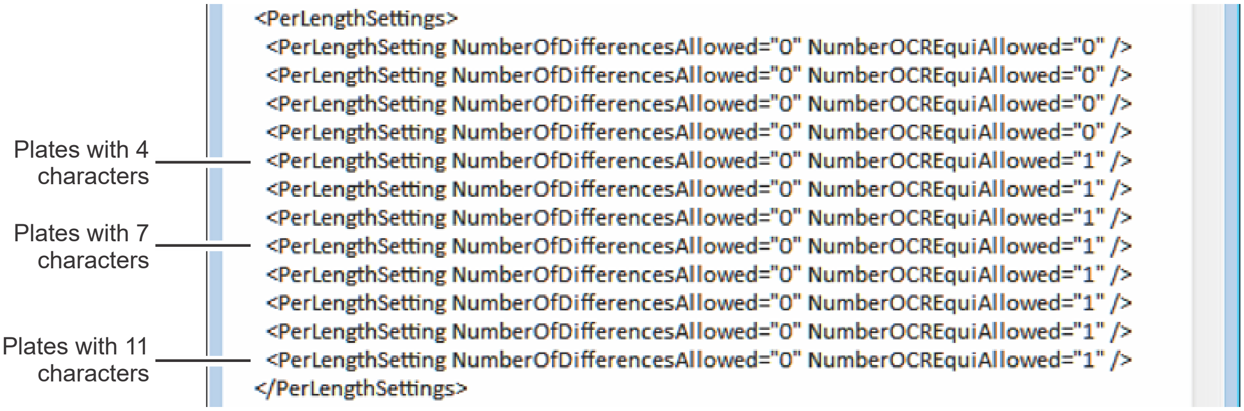
C: PerLength settings

For each matcher, specify the number of differences allowed, and the number of OCR equivalents allowed for license plates of different character lengths.

Here are some best practices for editing `PerLengthSettings`:

- There are 12 `PerLengthSetting` lines, each containing `NumberOfDifferencesAllowed` and `NumberOCREquiAllowed` tags.
- Each `PerLengthSetting` line corresponds to a plate character length. The line you edit depends on the number of characters on the license plates in your patrol region.
- Ignore the first line because it represents plates with zero characters. The second line represents plates with one character, the third line represents plates with two characters, and so on for a maximum of 11 possible plate characters.
- You can edit more than one line to apply settings to plates of different character lengths.

The default settings are `PerLengthSettings`. No differences are allowed, and one OCR equivalent is allowed for plates that have 5 to 11 characters.



```
<PerLengthSettings>
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="0" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
  <PerLengthSetting NumberOfDifferencesAllowed="0" NumberOCREquiAllowed="1" />
</PerLengthSettings>
```

D: Common and contiguous character settings

These settings apply to the Overtime matcher only.

- <**NecessaryCommonLength**>**:** Specify the minimum number of characters that need to be common to both the first and second plate read. The characters must also appear in the same order in the plate, but not necessarily in sequence.
- <**NecessaryContiguousLength**>**:** Minimum character sequence length between the first and second plate read.

Best practices for configuring LPR matcher settings

How you configure the LPR matcher depends on your enforcement scenario. In some AutoVu™ systems, you'll want an exact match only. In other systems, you'll benefit from having a false positive on a potential match because it decreases the chances of missing a vehicle of interest.

Use the following best practices when configuring LPR matcher settings:

- **Exact match:** The LPR matcher always looks for an exact match if possible, but you can configure it to allow *only* exact matches. This is typically used when you have very large hotlists (millions of entries). By limiting the number of possible matches, you lighten the processing load on the Patroller computer, and you decrease the amount of false positives that you would normally get from a list of that size. To allow only exact matches, turn on the *Simplematcher* feature in Patroller Config Tool, and turn off OCR equivalence.
- **OCR equivalence:** By default, the LPR matcher allows for one OCR equivalent character. You can allow as many as you want, but generally you should not allow more than two because you'll get too many false positives.
- **Number of differences allowed:** By default, the LPR matcher does not allow any number of differences. The number you allow depends on the plates in your region. The more characters on a plate, the more differences you can allow, but generally you should not allow more than two because you'll get too many false positives.
- **Common and contiguous characters:** (Used for overtime enforcement only) By default, the LPR matcher looks for five common, and four contiguous characters to generate an overtime hit. The number you specify depends on the plates in your region. The more characters on a plate, the more common and contiguous characters you can allow.

Related Topics

Configuring LPR matcher settings on page 646

Configuring LPR matcher settings

To adjust how license plates captured by Sharp are matched to license plates in a hotlist or permit list, you must configure the LPR matcher logic.

Before you begin

Read the best practices for configuring LPR matcher settings.

IMPORTANT: Test your system with the default LPR matcher settings. If the read accuracy rate meets your requirements, then do **not** adjust the LPR matcher settings.

What you should know

You configure LPR matcher settings in the *MatcherSettings.xml* file, and then apply your changes in Server Admin and the Server Admin console.

The overtime matcher is used as an example, but the same steps apply to all the matchers in the XML file.

To configure LPR matcher settings:

1 On the computer hosting the Security Center Directory role, open Windows Explorer and then go to *C:\Program Files\Genetec Security Center 5.5*.

2 Open *MatcherSettings.xml* in Notepad or a similar text editor.

3 Add or remove OCR equivalent characters from the list.

   The default OCR equivalent characters are listed between the `<OCR>` and `</OCR>` tags. Add new `<Equivalent>_____</Equivalent>` lines, or delete the lines you do not want.

4 Specify the number of character differences you want to allow.

   Edit the `PerLengthSetting` line that applies to the plates in your region. For example, Quebec plates typically have six or seven characters, so edit the `NumberOfDifferencesAllowed` value in the sixth and seventh `PerLengthSetting` lines.

   NOTE: A value of “0” turns the setting off.

5 Specify the number of OCR equivalent characters you want to allow by editing the `NumberOCREquiAllowed` value. This turns on OCR equivalence.

   NOTE: A value of “0” turns the setting off.

6 (Overtime only) Specify the number of common and contiguous characters.

   For common characters, edit the `NecessaryCommonLength` value. For contiguous characters, edit the `NecessaryContiguousLength` value.

7 Save and close the text editor.

8 Apply the LPR matcher settings in Server Admin, as follows:

   a) From a web browser, open Server Admin typing *http://<server>/genetec/console#/Commands*.
   b) From the **All commands** page, click **UpdateAutoVuGlobalSettings**.
   c) Close Server Admin.

9 Restart the Security Center Directory, as follows:

   a) From a web browser, open Server Admin by typing *http://<server>/genetec*.
   b) Click the **Directory** tab.
   c) Under **Directory status**, click **Restart**.
   d) After the Directory restarts, close Server Admin.

LPR matcher settings are now configured and applied to all the LPR Manager roles on your system. Patroller units are updated the next time they connect to Security Center wirelessly, or when you manually transfer Patroller settings using a USB key.

After you finish

Verify that your LPR Manager roles have been updated by looking at the *MatcherSettings.xml* file in their corresponding root folders (*C:\Genetec\AutoVu\RootFolder\ManualTransfer\General*). You can also tell by the XML file's *Date modified* field that it has been updated.

Related Topics
MatcherSettings.xml file on page 643

38

Hotlists

This section includes the following topics:

About hotlists

A hotlist is a type of entity that defines a list of wanted vehicles, where each vehicle is identified by a license plate number, the issuing state, and the reason why the vehicle is wanted (stolen, wanted felon, Amber alert, VIP, and so on). Optional vehicle information might include the model, the color, and the vehicle identification number (VIN).

Hotlists are used by both the AutoVu™ Patroller and the AutoVu™ LPR Manager role to check against license plates captured by LPR units to identify vehicles of interest.

The hotlist entity is a type of hit rule. A hit rule is a method used by AutoVu™ to identify vehicles of interest. Other types of hit rules include *overtime*, *permit*, and *permit restriction*. When a plate read matches a hit rule, it is called a hit. When a plate read matches a plate on a hotlist, it is called a hotlist hit.

Creating hotlists

To use hotlist entities in Security Center, you must create the hotlist, map it to its source text file, and configure it for your enforcement scenario.

Before you begin

Create the hotlist source text file (*.txt* or *.csv*).

What you should know

Hotlists can be used with any type of AutoVu™ fixed or mobile system.

NOTE: The source text file must be located on a drive that is accessible from the computer hosting the LPR Manager.

To create a hotlist:

1 From the home page, click **LPR** > **Hotlists**, then click **Hotlist** (➕).

The **Creating a hotlist** wizard opens.

2 On the **Basic information** tab, in the **Entity name** field, type a name for the hotlist and click **Next**.

NOTE: The **Entity description** is optional.

3 Set the priority of the hotlist using the Priority slider.

Zero (0) is the highest priority setting and 100 is the lowest. If a plate read matches more than one hotlist, the hotlist with the highest priority is displayed first in the list of hotlist matches.

4 Enter the **Hotlist path** on the computer where the hotlist's source text file is located.

If you start typing a path to a network drive, you may have to enter a **Username** and **Password** to access the network drive. The fields will appear if this is the case.

5 If the attribute fields in the source text file vary in length, switch the **Use delimiters** option to **ON**, and enter the type of character (delimiter) used to separate each field.

By default, **Use delimiters** is set to **ON**, and the delimiter specified is a **semi-colon** (;). If your source text file is made up of fixed length fields, set **Use delimiters** to **Off**. Security Center supports the following delimiters:

- Colon (:)
- Comma (,)
- Semi-colon (;)
- Tab (type "Tab")

IMPORTANT: If your source list file uses Tab as a delimiter, only use one Tab space. Do not use more than one Tab space to align columns in your file, or Security Center might not be able to parse the hotlist.

6 (Optional) Turn off **Visible in editor**, if you don't want users to be allowed to edit this hotlist in Security Desk.

NOTE: To edit a hotlist in Security Desk, users must have the *Hotlist and permit editor* privilege.

7 Configure the hotlist **Attributes**, and click **Next**. See Configuring hotlist and permit attributes on page 664.

8 On the **LPR Manager assignment** page, choose one of the following, then click **Next**.

- **All LPR Managers**. All LPR Managers and any entities configured to inherit hotlists from them will synchronize the new hotlist.

NOTE: Future LPR Managers will not automatically synchronize the new hotlist.

- **Specific LPR Managers**. Only the selected LPR Managers and the entities that inherit hotlists from them will synchronize the new hotlist.

  NOTE: Entities created in the future that are configured to inherit hotlists from one of the selected LPR Managers will also synchronize the hotlist.

- **Assign later**. No existing LPR Managers and associated entities will synchronize the new hotlist. For more information on how to assign a hotlist to an LPR Manager at a later time, see Selecting which hotlists and permit lists to monitor on page 652.

9 In the **Unit specific assignment** page, select the specific Patrollers and or Sharps that will synchronize the new hotlist, and click **Next**.

10 (Optional) If you have custom fields, enter the appropriate values on the **Custom fields** page and click **Next**.

NOTE: The **Custom fields** page does not appear if there are no custom fields in your hotlist.

11 In the **Creation summary** window, check to see that your hotlist information is correct and click **Next**.

12 In the **Entity creation outcome** window, you will receive a notification whether or not your operation is successful.

13 (Optional) Choose one of the following:

- **Edit this hotlist**. Opens the **Hotlist and permit editor** task so you can edit the hotlist.

  NOTE: To edit a hotlist, you must have the *Hotlist and permit editor* privilege.

- **Create a hotlist based on this hotlist:** Create a new hotlist that uses the same settings as the hotlist you just created. You only need to specify the **Entity name**, **Entity description**, and **Hotlist path**.

14 Click **Close**.

The hotlist entity is configured and enabled in Security Center.

Selecting which hotlists and permit lists to monitor

For hotlists and permit lists to be monitored by Patrollers, they must be activated and managed by at least one LPR Manager.

What you should know

The LPR Manager sends the active hotlists and permit lists to the Patrollers it manages. The LPR Manager also matches the hotlists against the reads collected from Sharp units to produce hits. When you create a new hotlist or permit list, they are active for all LPR Managers by default.

Only Patrollers configured for parking enforcement require permits.

NOTE: You can also associate permits to individual Patrollers, and hotlists to individual Patrollers and Sharp units.

To select which hotlists and permit lists to monitor:

1. From the home page, click **System** > **Roles**, and then click the LPR Manager you want to configure.
2. Click the **Properties** tab.
3. Under **File association**, select the hotlists and permits you want the LPR Manager to manage.
4. Click **Apply**.

Filtering out invalid characters from hotlists and permit lists

When a hotlist or permit is created or modified, you can specify the character set that applies to the license plates in the list based on a selected language, and what the LPR Manager does if it detects a list with invalid characters (non-alphanumeric characters).

What you should know

To view detailed information about how many invalid entries were deleted or modified, you can also save the logs of the filtering process.

To filter out plates when modifying hotlists and permit lists:

1. From the home page, click **System** > **Roles**, and then click the LPR Manager you want to configure.
2. Click the **Properties** tab.
3. Under **Plate filtering**, select the types of characters to filter on from the **Character set** drop-down list (Latin, Arabic, or Japanese).
4. In the **Invalid plate number** section, select one of the following options to specify how the LPR Manager handles invalid records:
   - **Modify record:** Deletes any non-alphanumeric characters from the plate number. For example, the plate number “ABC#%3” becomes “ABC3”.
   - **Remove record:** Deletes the entire entry that contains invalid characters from the list.
5. To log the filtering process, select the **Log filtering** option.

   The plate filtering logs will be saved in the AutoVu™ root folder: *C:|Genetec|AutoVu|RootFolder*.
6. Click **Apply**.

Adding privacy settings to reads and hits

You can configure Patroller to obscure plate numbers, or to exclude plate, context, or wheel images from reads and hits that are received in Security Center, so that the information is not stored in the LPR Manager database.

What you should know

Obscuring license plate numbers or excluding data from reads or hits allows you to comply with privacy laws in your region.

If you need to send an email with LPR data to a specific recipient, then you can override the privacy settings for individual hotlists.

To add privacy settings to reads and hits:

1. From the home page, click **LPR** > **General settings** > **Applications**.
2. Under **Privacy**, turn **ON** the data types that you want to hide from reads and hits:
   - **License plate, context, or wheel images:** Images are not sent to Security Center or included in offloaded data.
   - **License plate:** Replaces the text string of the license plate number with asterisks (*) when sent to Security Center or in the offloaded data.
3. Click **Apply**.

Adding privacy settings to hotlists

To obscure license plate numbers, or exclude plate, context, or wheel images from reads and hits that are received in Security Center from a specific hotlist, you can set the hotlist as private.

Before you begin

You must obtain a special DLL file from Genetec. For more information, contact your Genetec representative.

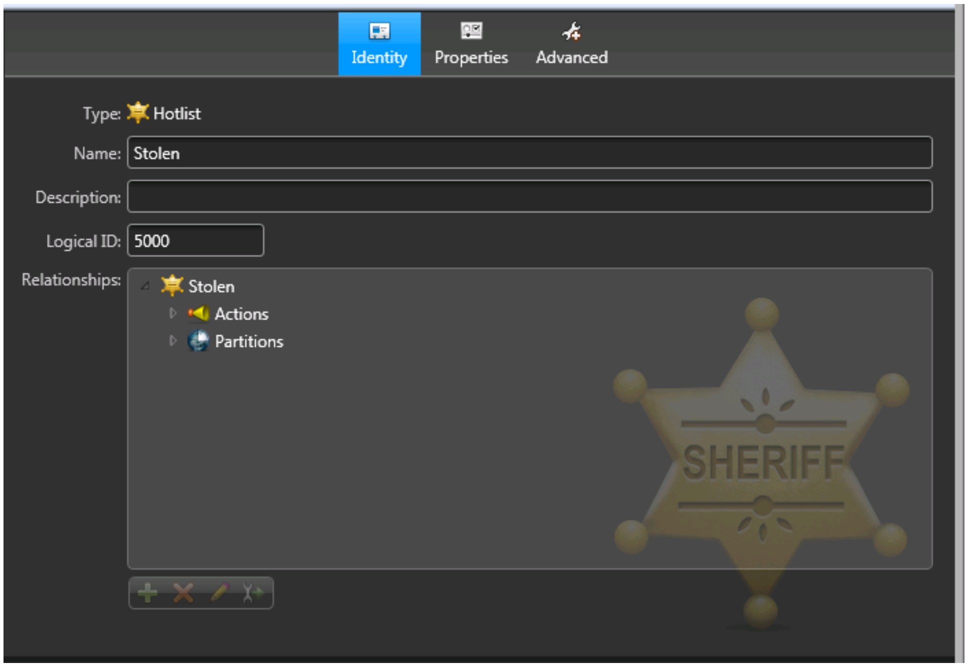
What you should know

If you add privacy settings to a hotlist, Security Center keeps the LPR data (for example, plate numbers, GPS coordinates, date/time, and so on), but disassociates that data from the hotlist that generated the hit. For example, if Patroller generates a hit from a hotlist called "StateWideFelons", you can keep all the LPR data on that hit, but you won't be able to see that the matched license plate was on the "StateWideFelons" hotlist.

The privacy settings of specific hotlists take precedence over the global privacy settings configured at the LPR Manager level. However, it is best practice to turn off all the privacy settings at the LPR Manager level to avoid conflicts.

To add privacy settings to reads and hits:

1. Copy the DLL file you received from Genetec Inc. to the Security Center root folder (for example, *C:|Program Files|Genetec Security Center 5.5*).
2. Restart the Directory role from Server Admin, as follows:
   a) Open Internet Explorer.
   b) In the address bar, type *http://server IP address:port/Genetec* and press **Enter**.
   c) Log on to Server Admin.
   d) Under **Directory status**, click **Restart**.
3. From the Config Tool home page, click **LPR** > **General settings** > **Applications**.
4. Under **Privacy**, turn **OFF** all the settings.
5. Click **Apply**.
6. From the home page, click **LPR** > **Hotlists.**
7. Select the hotlist that you want to make private, and then click the **Identity** tab.



Type: Hotlist

Name: Stolen

Description:

Logical ID: 5000

8 In the **Logical ID** field, enter the value *5000*.

This marks the hotlist, and tells Security Center to make the LPR data private.

9 Click **Apply**.

After you finish

Repeat for as many hotlists as you want.

Allowing users to edit hotlists and permits

When you are configuring properties of a hotlist or permit, you can select whether users are allowed to edit the list using the *Hotlist and permit editor* task in Security Desk.

What you should know

To edit a hotlist or permit list in Security Desk, users must have the *Hotlist and permit editor* privilege.

IMPORTANT: Please note the following about the Hotlist and permit editor:

- Only the first 100,000 rows of a list are loaded into the Hotlist and permit editor.
- If an error occurs while the hotlist is being loaded, the loading process is cancelled and an error message is displayed. However, you will not lose any of the data loaded before the error occurred, and you can still edit the data loaded into the editor.

To allow users to edit hotlists and permits:

1 From the home page, do one of the following:
    - Click **LPR** > **Permits**, and select the permit to configure.
    - Click **LPR** > **Hotlists**, and select the hotlist to configure.

2 Click the **Properties** tab.

3 Switch the **Visible in editor** option to **ON**, and click **Apply**.

Receiving notifications when hotlist hits occur

You can configure Security Center to send you an email notification when hotlist hits occur.

Before you begin

To make sure that the email notification is sent, do the following:

- Configure the mail server in Server Admin - Overview page.
- Make sure the **Email notification** option is switched to **ON** in the LPR Manager - Properties tab.

What you should know

You can configure Security Center to send an email notification when either of the following occurs:

- When any license plate on a hotlist generates a hit.
- When an individual license plate on a hotlist generates a hit. You can specify a different email address for as many individual plates on a hotlist as you want.

The email contains the hit information (matched plate number, Patroller name, user, hotlist name, and priority) in the message body, and optional image attachments.

To receive notifications when a hotlist hit occurs:

1 From the home page, click **LPR** > **Hotlists**.
2 Select the hotlist you want to configure, and click the **Advanced** tab.
3 In the **Email addresses** field, specify the email addresses you want to notify.

   NOTE: If you are entering more than one email address, separate them with a comma, a semicolon, or a space.

4 Click **Apply**.

   When any license plate in the selected hotlist generates a hit, a notification email is sent to the address you specified.

To receive notifications when a license plate generates a hit:

1 Add an email attribute to the hotlist as follows:
   a) From the home page, click **LPR** > **Hotlists**.
   b) Select the hotlist you want to configure, and click the **Properties** tab.
   c) Under **Attributes**, add a new email-related attribute (for example, *Email*) so that Security Center knows to look for email addresses in the hotlist's source file.
   d) Click **Apply**.

      Security Center will now look for email addresses in the hotlist source file.
2 Turn on **Email notification** and configure the related settings as follows:
   a) From the home page, click **System** > **Roles**.
   b) Select the LPR Manager you want to configure, click the **Properties** tab, and then click **Email notification**.
   c) In the **Email attribute name** field, type the same attribute name you created in the first step.
   d) (Optional) Under **Email attachments**, specify what information you want the email to contain.

      For example, you might want to send only the license plate text string without any images to keep the email's file size small.

   e) (Optional) In the **Log emails in** field, select where to store the email notification logs.

      The logs will be saved in the AutoVu™ root folder: *C:\Genetec\AutoVu\RootFolder*, and will help you keep track of who received email notifications.

   f) Click **Apply**.

      The LPR Manager now knows that some hotlists contain email addresses for individual license plate entries.

3. Add email addresses in the hotlist source file.

   NOTE: Since you added the *Email* attribute to the hotlist entity, you can now use the *Hotlist and permit editor* to add email addresses. You can also add them directly to the source file if you prefer.

   a) From the home page, click **Hotlist and permit editor**.

      NOTE: The **Visible in editor** option must be turned on to edit the hotlist.

   b) Select the hotlist you want to configure, then click **Load**.
   c) Add email addresses to as many license plates as needed.
   d) Click **Save**.

If a license plate with an email address generates a hit, an email will be sent to the specified recipient.

Related Topics
Server Admin - Overview page on page 83
Allowing users to edit hotlists and permits on page 657

Receiving *Match* and *No match* events in Security Desk

To receive *Match* and *No match* license plate events in Security Desk, you need to turn on hotlist matching so that the Sharp units can match license plates against active hotlists and permit lists.

Before you begin

The hotlist or permit list must be active and managed by an LPR Manager so that the events are monitored.

What you should know

When hotlist matching is turned on, you can configure event-to-actions in Security Desk, based on *Match* events (license plate read by the Sharp was on a hostlist) and *No match* events (license plate read by the Sharp was not found on a specific hotlist).

Typically, *No match* events are used in access control scenarios. For example, you can associate a hotlist to a specific Sharp unit that is monitoring access to a parking lot or similar location. In this scenario, a Security Center event-to-action for a *License plate hit* grants the vehicle access (opens a gate, raises a barrier, and so on), and an event-to-action for a *No match* could trigger an alarm, or send an email to security personnel.

To receive *Match* and *No match* events in Security Desk:

1. From the home page, click **System** > **Roles**.
2. Select the LPR Manager you want to configure, and then click the **Properties** tab.
3. Turn the **Matching** option **ON**.
4. (Optional) To generate “no match” events when a license plate is read by a Sharp and it is not part of a hotlist or permit list, turn the **Generate “No match” events** option to **ON**.
5. Click **Apply**.

Wildcard hotlists

Wildcard hotlists contain entries with only partial license plate numbers. They can be used in situations where witnesses did not see or cannot remember the complete license plate number. This allows the officer to potentially intercept wanted vehicles that may not have been detected using standard hotlists.

A wildcard hotlist includes entries that have either one or two asterisks (*) in the license plate number field. The asterisks are the wildcards you use when you don't know the character. Only the plate number field accepts wildcard characters. If the asterisk is found in any other field (e.g. state or province), it is considered as a normal character.

Note the following about wildcard hotlists:

- If you activate wildcards on a hotlist, Patroller will ignore all hotlist entries that do not contain a wildcard, or that have more than two wildcard characters.
- It is the number of wildcards in the *PlateNumber* field, and not the location of the wildcard character, that determines how many mismatched characters are allowed before a match can occur.
- The position of the wildcards cannot be enforced because, typically, when witnesses report a partial plate number, they do not remember the position of the characters they missed. The sequence of the normal characters in the *PlateNumber* is respected, such that the three patterns "S*K3*7", "**SK37", and "SK37**" are equivalent.

  If a wildcard hotlist contains the license plate entry S*K3*7:

  - Plate reads **N**SK3**5**7 and **ASD**K37 *will* generate a hit because both reads have no more than two mismatched characters (in bold) and the sequence "SK37" is respected.
  - Plate read SUKA357, *will not* generate a hit because it contains three mismatched characters (in red).
  - Plate read SKU573 read will not generate a hit because the sequence of characters SK37 is not found in the read.

BEST PRACTICE: When using wildcard hotlists, observe the following best practices:

- Do not use more than one wildcard hotlist per Patroller.
- Use only one wildcard hotlist per LPR Manager.
- Limit the number of wildcard entries in a hotlist to 100 plates.

Activating wildcard hotlists

To read partial license plates, you must set a hotlist as a wildcard hotlist.

Before you begin

The hotlist must be active and managed by an LPR Manager.

To activate wildcard hotlists:

1. From the home page, click **LPR** > **Hotlists**, and then click the hotlist you want to configure.
2. Click the **Advanced** tab, and turn the **Use wildcards** option to **ON**.
3. Click **Apply**.

Related Topics
Wildcard hotlists on page 661

Default hotlist and permit attributes

The following hotlist and permit attributes are created by default in Security Center:

- **Category (Mandatory):** The name of the parking permit. This field in the permit list's source text file *must* match the permit entity name exactly for the entry to be downloaded to Patroller. If you have multiple categories in the same source file, you can use the same permit list for different permit entities in your system.

  For example, here is a simple permit list with three different permit categories (*Students*, *Faculty*, and *Maintenance)*. You can use this same permit list for three different permit entities (a *Students* permit entity, a *Faculty* permit entity, and a *Maintenance* permit entity) Each entity can point to the same source text file. Security Center extracts the license plates (and related information) whose category is the same as the name of the permit entity.

Category field	Students	`QC;DEF228;2012-01-31;2012-05-31;PermitID_1`
	Faculty	`QC;345ABG;2012-01-31;2012-07-25;PermitID_2`
	Maintenance	`QC;244KVF;2012-01-31;2012-03-31;PermitID_3`

- **PlateState (Optional):** Issuing state (or province, or country) of the license plate.
- **PlateNumber (Mandatory):** The license plate number.
- **EffectiveDate (Optional):** Date from which the particular permit on the list starts to be effective.
- **ExpiryDate (Optional):** Date after which the particular permit on the list is no longer valid.
- **PermitID (Optional - *Shared permit enforcement, typically University Parking Enforcement and some City enforcement applications*):** Used when multiple entries in a permit list share the same permit (e.g. car pool permits). Can be used to identify the number of the permit issued to the vehicle whose license plate is identified in *PlateNumber*. In the case of shared permits, normally up to four separate vehicles would all have the same permit number.

  A violation results in a *Shared Permit* hit in Patroller.

Related Topics

About permits on page 712

Configuring hotlist and permit attributes

You must configure the attributes of a hotlist or permit in Security Center the way it is written in its source text file, so Patroller can parse the information in the list.

What you should know

- There cannot be any spaces within an attribute name.
- Hotlist and permit list text file must include the *Category*, and *PlateNumber* fields (attributes). These are mandatory fields, and they cannot be deleted.

To configure hotlist or permit attributes:

1. From the home page, do one of the following:

   If you are configuring attributes from the **Creating a hotlist** or **Creating a permit** wizard, skip ahead to Step 3.

   - Click **LPR** > **Permits**, and select the permit to configure.
   - Click **LPR** > **Hotlists**, and select the hotlist to configure.
2. Click the **Properties** tab.
3. Under the **Attributes** section, do one of the following:
   - To configure a default attribute, select it in the list, and click **Edit the item** (✎).
   - To add a new attribute, click **Add an item** (➕).
4. If you are adding a new attribute, type a **Name** for the attribute.

   The name can contain spaces.
5. If you want to use a default value for the field, type in the **Value** option.

   The default value is interpreted differently depending on whether delimiters are used or not.

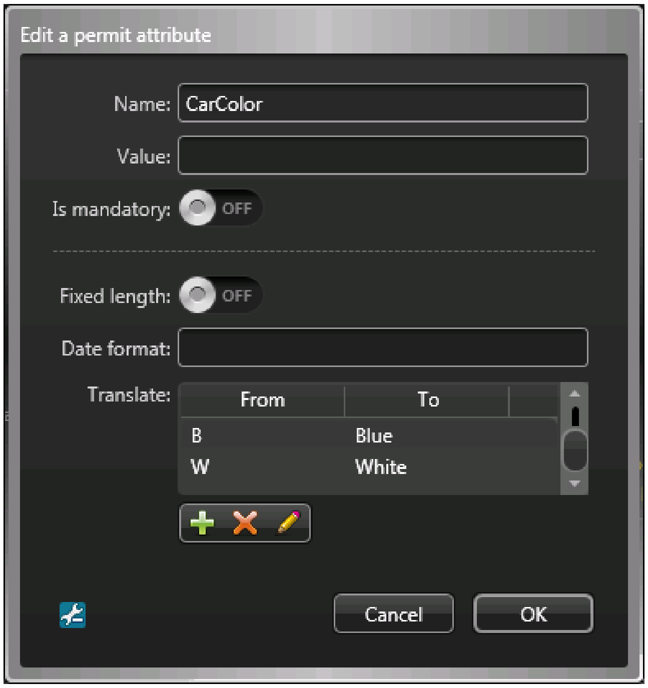
   - If delimiters are used and you add a default value for this field, the populated field in the source file is overwritten.
   - If delimiters are not used and the field is empty in the source file, the default value you add here is used for the field. However, if the field is populated in the source file, it will not be overwritten.
6. If you are adding a new attribute and it is mandatory in the source file, switch the**Is mandatory** option to **ON**.

   Example: If you add a mandatory attribute called *CarColor*, the column for *CarColor* in the source file must have text in it.
7. To show additional attribute fields, click ⊕.
8. If the source file is using fixed length data fields instead of delimiters, switch the **Fixed length** option to **ON**, set the **Start** character position of the attribute in the file, and its **Length**.

   The position of the first character in the source file is zero (0).
9. If the field contains a date or time value in the source file, specify a **Date format**.

   All standard date and time format strings used in Windows are accepted. If nothing is specified, the default time format is “yyyy-MM-dd”.
10. If you want to transform the values read from the data file, click **Add an item** (➕) under **Translate**, select a **From** and **To** value, and click **OK**.

    Example: In the following example, the new field is CarColor and B will be translated to Blue and W will be translated to White.



Edit a permit attribute

Name: CarColor

Value:

Is mandatory: OFF

Fixed length: OFF

Date format:

Translate:

From	To
B	Blue
W	White

11 Click **OK**.

12 To delete an attribute that you are not using in the source file, select it in the list, and click **Delete** (✖).

Example: If the permits on your list don't expire, you can delete the *ExpiryDate* attribute.

The attribute fields from your hotlist and permit list source text files should now match the attributes in the entity's Properties tab. Patroller can now download the information from the information in the list.

Example

The following source file uses variable field length data, and a semicolon (;) as a delimiter. It uses the following attributes: *Category*, *PlateState*, *PlateNumber*, *EffectiveDate*, *ExpiryDate*, and *PermitID*.

```
MyPermit;QC;DEF228;2012-01-31;2012-05-31;PermitID_1
MyPermit;QC;345ABG;2012-01-31;2012-07-25;PermitID_2
MyPermit;QC;067MMK;2012-03-31;2012-09-11;PermitID_1
MyPermit;QC;244KVF;2012-01-31;2012-03-31;PermitID_3
```

Related Topics

Default hotlist and permit attributes on page 663

Configuring advanced hotlist settings

The **Advanced** tab is where you configure the advanced properties of a hotlist such as the color of a hotlist hit and the sound file that plays when a hotlist hit occurs. These properties are not required for all hotlists, but allow you to customize hotlists for specific scenarios.

Before you begin

Create the hotlist.

To configure advanced hotlist settings:

1. From the home page, click **LPR** > **Hotlists**, and select the hotlist you want to configure.
2. Click the **Advanced** tab.
3. Beside **Color**, click the colored block and use the **Select color** dialog box to assign a new color to the permit.

   The map symbol that marks the location of the hotlist hit in Security Desk and Patroller will appear in that color, as well as the Hotlist Hit and Review Hits screen in Patroller.
4. Turn on **Use wildcards** to activate wildcard hotlists.
5. Turn on **Covert** if you want to set the hotlist to a covert hotlist. When you choose this setting, Patroller users are not alerted when a hit occurs. Only users with sufficient privileges can view covert hit in Security Desk
6. Enter an **Email address** that receives a notification when the hotlist you're configuring generates a hit.
7. Enter the path for the **Sound file** Patroller plays when a hotlist hit occurs. If you leave this field blank, Patroller plays its default sounds. The path (you must include the filename) indicates the file's location on the Patroller in-vehicle computer.
8. Turn on **Override privacy for emails** if you want to bypass any privacy settings you applied at the Directory level, and send an email with real LPR data to the email address you specified for this particular hotlist.
9. Turn on **Disable periodic transfer** if you only want permit changes to be downloaded to Patroller when the user logs on to the application. This option requires a wireless connection between Patroller and Security Center.

   Turn on **Enable transfer modification** if you want to transfer hotlist modifications to Patroller as soon as they occur. For example, you can use this option on a hotlist to force Patroller to query for changes more frequently than the periodic transfer period (which applies to all hotlists). This can be useful for Amber alerts because they can be added to a specific hotlist and sent to a Patroller almost immediately. This option requires a continuous wireless connection between Patroller and Security Center.

39

AutoVu™ fixed systems

This section includes the following topics:

Preparing to deploy fixed AutoVu™ systems

To make sure that your fixed AutoVu™ deployment goes smoothly, you must perform a series of pre-configuration steps.

Before deploying a fixed AutoVu™ system:

1. Have the information from your initial site survey on hand before you install the AutoVu™ hardware.

   For example, you should already know how high to install a fixed Sharp before you begin the installation.

2. Install the following Security Center software components:
   a) Security Center Server software on your main server.

      The *main server* is the computer hosting the *Directory* role.

   b) (Optional) Security Center Server software on expansion servers.

      An *expansion server* is any other server on the system that does not host the Directory role. You can add expansion servers at any time.

   c) Security Center Client software on at least one workstation.

      For more information about installing Security Center, see the *Security Center Installation and Upgrade Guide*.

3. Install the fixed Sharp hardware (see the *AutoVu™ Hardware Installation Guide*).
4. Upgrade Sharp units to the latest software and firmware (see the *Sharp Administrator Guide*).

   NOTE: You can perform certain upgrades from Security Center Config Tool.

Deploying fixed AutoVu™ systems

To integrate a variety of LPR capabilities, you can deploy your fixed AutoVu™ system.

Before you begin

Perform the pre-configuration steps.

What you should know

Information about how to set up a typical fixed AutoVu™ deployment is provided here. Your process might be different, depending on your specific installation requirements.

NOTE: Settings that are pre-configured during your installation are not listed in this task. For example, when you install Security Center, the LPR Manager root folder is automatically created on your computer at the location *C:\Genetec\AutoVu\RootFolder*.

To deploy a fixed AutoVu™ system:

1 Log on to the Sharp Portal, and configure the Sharp for a fixed AutoVu™ system.

For information about logging on to the Sharp Portal, see the *Sharp Administrator Guide*.

2 Configure the LPR Manager so that Security Center can discover and communicate with fixed Sharp units.

NOTE: For SharpX installations where LPR Processing Unit input/output control is required, you must also enroll the LPR Processing unit under the Archiver.

3 Configure the LPR Manager server and database settings.

NOTE: You can also add additional server to act as failover server for the LPR Manager.

4 If you are using hotlists with your fixed deployment, then create and configure the hotlist entities, and turn on hotlist matching.

5 If you are using AutoVu™ as an access control solution, then configure the Sharp cameras to grant or deny access to a parking lot or similar facility.

6 Specify the Sharp's location and time zone.

Configuring LPR Managers for fixed AutoVu™ systems

To receive LPR data in Security Center with a fixed AutoVu™ system, you must configure the LPR Manager listening and discovery port to find Sharp units on the network and send the data to Security Center, and select which LPR images fixed Sharp units should send to Security Center when reading a plate.

Before you begin

You must know the *IP address* of the computer that is hosting the LPR Manager role.

What you should know

These instructions explain the preferred method of adding a Sharp camera if the Sharp and Security Center are on the same subnet. If they are not on the same subnet, or if they must communicate across the Internet where the network topology includes NATs, you must use a different connection method. For more information, see Sharp, SharpV, or SharpX camera connections to Security Center on page 671.

To configure an LPR Manager for a fixed AutoVu™ system:

1 From the home page, click **System** > **Roles**, and then select the LPR Manager you want to configure.
2 Click the **Properties** tab, and then click **Live**.
3 Under **Network**, configure the following ports:
   - **Listening port:** Port used to listen for connection requests coming from fixed Sharps (and Patrollers). After the connection is established, the LPR Manager can receive live updates from the LPR units it manages. The default listening port number is 8731.
   - **Sharp discovery port:** Port used by the LPR Manager to find fixed Sharp units on the network.

     IMPORTANT: Each LPR Manager must use a unique discovery port.

     NOTE: When setting the discovery port, do not use port 5050 as it is reserved for the logger service.
4 Under **Send on read (fixed Sharp only)**, configure the following:
   - **License plate image:** Include the high resolution close-up image of the license plate along with the plate read data.
   - **Context image:** Include the wide angle context image of the vehicle along with the plate read data.

   These images are displayed in Security Desk when monitoring LPR events.

After you finish

- Make sure the Sharp discovery port matches the port number in the Sharp Portal. For more information, see the *Sharp Administrator Guide*.
- To guarantee that the license plate reads collected from the Sharp units are associated with the correct timestamp, configure the time zone of fixed Sharp units.
- To plot the LPR events (reads and hits) associated to the Sharp units on the *map* in Security Desk, configure the geographical location of the Sharp units.

Sharp, SharpV, or SharpX camera connections to Security Center

If you are using the Security Center extension to send LPR data from a Sharp, SharpV, or SharpX camera to Security Center, you must first enroll the camera in the Security Center *LPR* task under *Roles and units*.

The easiest way to add a Sharp, SharpV, or SharpX camera in Security Center is to configure the LPR Manager to discover the camera. If this connection method is not possible, you can add the camera manually in Security Center or in the camera's web portal.

You can add a camera to Security Center in one of the following ways:

Connection Method	When to use this method	Requirements
Configure the LPR Manager to discover the camera: You can configure the LPR Manager's *Discovery port* to find the camera on the subnet.	This is the preferred method if the camera and Security Center are on the same subnet.	To use this method, you must set the same *Discovery port* in the LPR Manager's *Properties* tab and in the camera's web portal. The camera and Security Center must be on the same subnet. For more information on configuring LPR Managers for fixed AutoVu™ system, see About LPR Managers on page 633.
Manually add the camera in Security Center: You can add the camera to the LPR Manager in Config Tool's *LPR* task.	Use this method when the camera and Security Center are on different subnets within the same LAN. You can use this method if the *Discovery port* is not available, however the *Discovery port* can be changed in Security Center and in the camera's web portal. **NOTE:** • You cannot use this method if communication must go across the Internet. • If the camera is behind a NAT, you must configure port forwarding.	To use this method, you must know the IP address and port (control port) for the camera. The camera and Security Center must be on the same network.
Add a Sharp, SharpV, or SharpX from the camera's web portal: You can force a connection from the camera's web portal when you select the *Security Center* extension and select **Connect to Security Center**. For assistance, contact your Genetec™ representative.	Use this method if the camera and Security Center must communicate across the Internet and where the network topology includes NATs. **NOTE:** If the camera is behind a NAT, you must configure port forwarding.	To use this method, you must enter the *Hostname* or *IP address* and *port* (listening port) of the Security Center computer.

Adding a Sharp, SharpV, or SharpX camera to the LPR Manager

To send LPR data from the camera to Security Center, you must add the camera to an LPR Manager.

Before you begin

To add a camera in Security Center, you must first configure an LPR Manager role.

What you should know

The easiest way to add a camera in Security Center is to add the camera automatically using the Unit enrollment tool. If the system cannot discover the camera, use the following method to add the it manually.

To manually add a camera in Security Center:

1 From the Config Tool home page, click the *LPR* task and select **Roles and units**.

2 Click ✚ **LPR unit**.

The **Creating a unit** dialog box opens.

3 Enter a **Name** for the camera.

4 Enter the **IP address** and **Port** of the camera.

This information should match what is displayed in the camera's web portal.

5 Select the **LPR Manager** role from the drop-down list, and click **Next**.

6 Complete all other settings as necessary, and click **Create**.

The new camera is added under the selected LPR Manager.

Adding a Sharp, SharpV, or SharpX camera to the Archiver

If you want to view the context camera video feed in Security Center, you must add the camera to the Archiver.

Before you begin

- To add a camera in Security Center, you must first configure an Archiver role.
- Log on to the camera's web portal and change the default password.

What you should know

The easiest way to add a camera in Security Center is to add the camera automatically using the Unit enrollment tool. If the system cannot discover the camera, use the following method to add the it manually.

To manually add a camera to a Security Center Archiver:

1. From the Config Tool home page, open the **Video** task.
2. If you have multiple Archiver roles, select the Archiver role to manage the unit from the Archiver drop-down list.
3. Click ✚ **Video unit**.

   The **Manual add** dialog box opens.
4. From the **Manufacturers** drop-down list, select **Genetec AutoVu**.
5. From the Product type drop-down list, select **All**.
6. Enter the static IP address of the camera.

   TIP: Use a range (⊕) of IP addresses to add multiple units in a single operation.
7. Enter the **HTTP port** number.
   - **SharpV:** The port number is 8080.
   - **Sharp and SharpX:** The port number is 80.
8. Select the **Authentication** method for the camera.
   - **Default logon:** The camera uses the default logon defined for the Archiver in the *Extensions* tab. Using this method, you can define the same logon credentials for multiple cameras.
   - **Specific:** Enter the logon credentials for the camera. Turn on **Use HTTPS** if you have applied a self-signed or signed certificate to the camera connection.
9. From the **Location** drop-down, assign the camera to an area entity.
10. Click **Add**.

    The notification tray displays the message "Adding unit started". If successful, it displays the message "Unit added successfully".

The camera is added under the selected Archiver.

Replacing fixed Sharp units

You can replace a fixed Sharp unit without losing any of its associated plate reads by swapping the connection parameters of the old unit with a new unit.

Before you begin

- In Security Desk, run a *Reads* report and a *Hits* report on the Sharp unit you want to replace. You need these reports to verify that the data has been transferred to the new Sharp unit.

To replace a Sharp unit:

1 Add the new Sharp entity in the LPR Manager.

NOTE: The name you use for the new entity is not important. At the end of the camera replacement procedure, the connection parameters of the entities will be switched and you will delete the entity you are adding now.

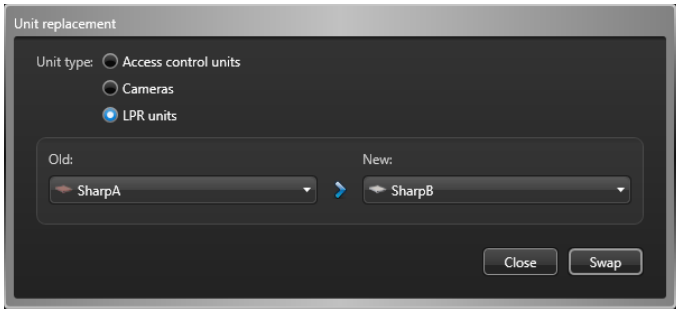
2 Copy the configuration settings of the old Sharp entity to the new Sharp entity using the Copy configuration tool.

3 Power down the old Sharp unit.

4 Click the *Home* tab, and then click **Tools** > **Unit replacement**.

5 In the **Unit type** option, select **LPR units**.

6 Select the **Old** and the **New** Sharp units.



Unit replacement

Unit type: ○ Access control units
○ Cameras
● LPR units

Old: SharpA

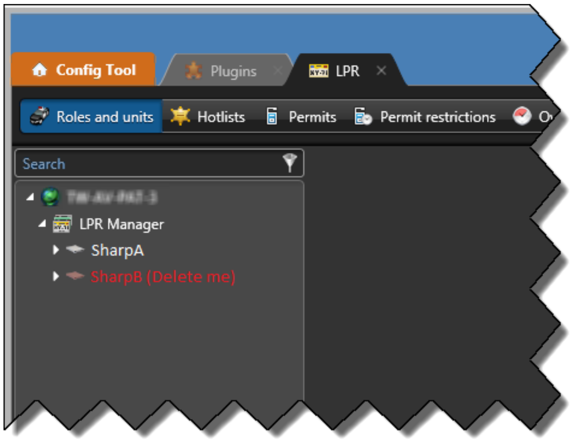
New: SharpB

7 Click **Swap**.

When the Sharp unit has been replaced, the system displays the message: "The operation was successful". The connection parameters of the new Sharp unit are now associated with the reads and hits from the old Sharp unit.

8 Verify that the reads and hits are still associated with the old Sharp entity by running a Security Center *Reads* report and a *Hits* report. Compare these reports to the ones you ran before the swap operation to ensure that the data has been successfully transferred.

9 The Sharp entities have been swapped in Security Center. The old Sharp unit now has the new entity name and is displayed in the LPR Manager with the message: "Delete me". Right-click the Sharp entity and select **Delete**. In the confirmation dialog box that opens, click **Delete**.



Related Topics

Copying configuration settings from one entity to another on page 60
Configuring LPR Managers for fixed AutoVu™ systems on page 670

LPR-based access control

AutoVu™ License Plate Recognition technology can be used for access control, by installing Sharp cameras at a facility's entry points (for example, parking lots, university campuses, and so on), which match license plates to one or more hotlists, and then grant or deny access to vehicles that want to enter the facility.

How LPR-based access control works

In an LPR-based access control scenario, you use Sharp cameras, hotlists, and Security Center event-to-actions to automate access to a parking lot or similar facility.

You begin by installing your Sharp cameras at a facility's entry points to capture the plates of vehicles attempting to enter. You then create the hotlists that contain the license plates of the vehicles which are allowed to enter, and assign them to the Sharp units as needed in Security Center Config Tool. Each Sharp is responsible for the vehicles on the hotlist(s) assigned to it.

After creating and assigning your hotlists to the Sharp cameras, you then create Security Center event-to-actions for the *License plate hit* and *No match* events generated by the Sharps and hotlists to grant or deny access to the vehicles.

For example, if a plate matches one or more hotlists assigned to a Sharp, Security Center triggers an action that lifts a gate or opens a garage door, while a *No match* event (plate does not match any assigned hotlist) triggers an action that sounds an alert, or sends a message to security personnel so they can question the vehicle's driver.

You can also trigger event-to-actions on hotlists of stolen vehicles, scofflaws, or other vehicles of interest. These hotlists are typically assigned to the LPR Manager so that the event-to-action can be triggered by any of the Sharps capturing the plate.

About assigning hotlists to Sharp cameras

Hotlists are lists of vehicle license plates that can be assigned either to an LPR Manager role, or to individual Sharp units. When you assign a hotlist to an LPR Manager, all the Sharp units controlled by the LPR Manager can match against the hotlist. When you assign a hotlist to an individual Sharp unit, only that specific Sharp unit can trigger hits.

In LPR-based access control, a Sharp camera acts as a gatekeeper for a specific facility entry point. Depending on your deployment, you may want to allow only specific vehicles access to certain sections (for example, VIP parking, staff parking, and so on).

This is why you need the option of assigning hotlists to specific Sharp cameras. For example, this allows you to assign a VIP hotlist to a Sharp camera that is installed at the entrance to the VIP parking garage. The Sharp will then allow only the vehicles on its associated VIP hotlist to enter that section of the garage. Any vehicle that is not on the Sharp's hotlist doesn't get in.

This feature is particularly useful for large and complex parking facilities, such as university campuses which have multiple parking lots, each with multiple entry points, and each allowing access to different groups of vehicles.

Events used in LPR-based access control

There are two main types of Security Center events used in an LPR-based access control system, *License plate hit* and *No match*.

NOTE: You can also use *License Plate Read* events to trigger actions such as starting video recording for the Sharp's context camera. However, only the *License plate hit* and *No match* events are described here.

- **License plate hit events:** When you turn on *Matching* for an LPR Manager in Security Center Config Tool, Security Center tries to match the plates captured by Sharp cameras to plates on loaded hotlists. If a plate is matched to a hotlist, Security Center generates a *License plate hit* event. By creating an event-to-action that triggers on this event, Security Center can grant access to a facility by opening a gate, a garage door, and so on.

- **No match events:** You can also turn on *No match* events for an LPR Manager in Security Center Config Tool. A *No match* event is generated when a plate is *not* matched to a hotlist. For example, you can use a *No match* event to account for guests, delivery vehicles, or other vehicles not typically registered ahead of time on a hotlist. Event-to-actions for *No match* events can either have a hotlist or a Sharp camera as the source of the event. If the hotlist is the source, it means the plate is not found on that particular hotlist. However, if the Sharp is the source, it means that the plate is not found on *any* of the hotlists assigned to the Sharp. This is a subtle but important difference you should keep in mind when configuring your system because you can have more than one hotlist assigned to a single Sharp.

No match events are not generated against hotlists assigned to the LPR Manager because they would apply to all the Sharps controlled by the role. For example, if you have a hotlist of stolen vehicles assigned to the LPR Manager, any plate read not on that list would generate a *No match* event. Since the majority of the plates read by the Sharp will not be stolen vehicles, *No match* events would be generated for nearly every plate read.

Configuring AutoVu™ for access control

To grant or deny access to vehicles in a parking facility (parking lot, gate, entrance, and so on) based on their license plates, you can configure a custom LPR-based access control solution.

Before you begin

Do the following:

- Install Sharp cameras at each parking lot entry point (see the *AutoVu™ Hardware Installation Guide*).
- Get a fixed AutoVu™ system up and running.

What you should know

You can deploy an LPR-based access control solution in a variety of ways. The example of a university campus is used to show you how you can customize a solution that is specific to your deployment.

In the hypothetical university campus, the following parking rules apply:

- **Faculty:** Can park in Lot A and Lot B.
- **Students:** Can park in Lot B.
- **Management:** Can park in Lot C.
- **Maintenance:** Can park in Lot B on weekdays from 6:00 PM to 10:00 PM.
- **Guests:** Can park in any lot with approval from security.
- **Scofflaws:** Cannot park anywhere on campus, and security must be alerted if seen.

To set up access rules for parking facilities:

1 Name the Sharp entities.

Security Center automatically detects all Sharps connected to the network, but you should name each Sharp entity according to its function or location. In our example, use the names *Sharp Lot A*, *Sharp Lot B*, and *Sharp Lot C*.

NOTE: Configuration is simpler when all Sharps are on the same LPR Manager. However, if the Sharps are on multiple LPR Managers, you'll have to assign your hotlists accordingly.

2 Turn on hotlist matching for the LPR Manager controlling your Sharps.

3 Create and configure the hotlists you're going to use.

Name each hotlist according to its contents. In the university campus example, use the names *Faculty*, *Students*, *Management*, *Maintenance*, and *Scofflaws.*

NOTE: In the university example, *Guests* represent anyone that shows up unannounced. Therefore, they are they are not included on any hotlist.

4 Create a schedule.

For example, if you want the *Maintenance* staff to only have access to your parking lot between 6:00 PM and 10:00 PM, you must create a schedule in Security Center that reflects that. You'll use this schedule later on when you create your event-to-actions.

5 Assign your hotlists to Sharps and the LPR Manager as follows:

- *Faculty* to *Sharp Lot A* and to *Sharp Lot B*.
- *Students* to *Sharp Lot B*.
- *Management* to *Sharp Lot C*.
- *Scofflaws* and *Maintenance* to the LPR Manager.

   NOTE: The *Maintenance* hotlist must be assigned to the LPR Manager because it depends on a schedule. All hotlists that you combine with schedules must be assigned to the LPR Manager.

6. (Optional) If you have only one LPR Manager on your system, unassign the *Faculty*, *Students*, and *Management* hotlists from the LPR Manager.

   When you have only one LPR Manager, new hotlists are assigned to that LPR Manager by default (new hotlists are left unassigned if you have multiple LPR Managers). When you assign a hotlist to a Sharp, Security Center does not automatically unassign it from the LPR Manager; you must do it manually. Otherwise you will get duplicate match events from the other Sharps.

   Example: If you assign the *Students* hotlist to *Sharp Lot B*, but forget to unassign it from the LPR Manager, a plate read from that list by *Sharp Lot B* will also trigger matches on *Sharp Lot A* and *Sharp Lot C*.
7. Configure event-to-actions for the *Sharp Lot A*, *Sharp Lot B*, and *Sharp Lot C* units.
8. Configure event-to-actions for the *Scofflaws* and *Maintenance* hotlists.

Access to the parking lot is now automated for permitted vehicles, and actions are taken when unknown or scofflaw vehicles are detected.

Creating event-to-actions for Sharp-related events

To make sure that some vehicles are granted access to the parking facility, and that other actions are taken for unknown or scofflaw vehicles, you must create event-to-actions that are triggered based on *License plate hit* and *No match* events generated by Sharps.

What you should know

For fixed SharpX systems, you can configure event-to-actions to control the inputs and outputs of the LPR Processing Unit. LPR Processing Units are generally enrolled under the LPR Manager, however, in order for the outputs to be selectable when creating event-to-actions, you must **also** enroll the LPR Processing unit under the Archiver.

To create event-to-actions for Sharp-related events:

1. Open the **System** task, and click the **General settings** view.
2. Click the **Actions** tab, and click ✚.
3. In the **Entity type** page, select **LPR unit**, and click **Next**.
4. In the **Source** page, select which Sharp unit will be the source of the event, and then click **Next**.
5. In the **Event** page, do the following:
   a) From the main list, select an **License plate hit** or **No match**.
   b) From the **Entity** drop-down list, select **Unassigned**.
   c) From the **Schedule** drop-down list, select **Always**.
   d) Click **Next**.
6. In the **Action** page, select the action and attributes for each type of event, and then click **Next**.
   - For *License plate hit* events, select **Trigger output**, and then select the **Output pin** and **Output behavior** required to grant access to the parking lot (for example, open a gate).
   - For *No match* events, select the action you want Security Center to take. For example, you could send a message to a particular Security Center user, or use another *Trigger output* action to activate a security intercom at the gate.
7. In the **Creation summary** page, review your event-to-action, and then click **Save** to proceed, or **Back** to make changes.

Related Topics

LPR-based access control on page 676
Creating event-to-actions on page 177

Creating event-to-actions for hotlist-related events

To make sure that some vehicles are granted access to the parking facility, and that other actions are taken for unknown or scofflaw vehicles, you must create event-to-actions that are triggered based on *License plate hit* events generated by hotlists assigned to the LPR Manager (for example, list of wanted vehicles, or vehicles with scheduled access).

Before you begin

Create a schedule for the *Maintenance* staff.

What you should know

For fixed SharpX systems, you can configure event-to-actions to control the inputs and outputs of the LPR Processing Unit. LPR Processing Units are generally enrolled under the LPR Manager, however, in order for the outputs to be selectable when creating event-to-actions, you must **also** enroll the LPR Processing unit under the Archiver.

To create event-to-actions for hotlist-related events:

1. Open the **System** task, and click the **General settings** view.
2. Click the **Actions** tab, and click ✚.
3. In the **Entity type** page, select **Hotlist**, and click **Next**.
4. In the **Source** page, select the *Scofflaws* or *Maintenance* hotlist, and click **Next**.
5. In the **Event** page, do the following:
   a) From the main list, select an **License plate hit**.
   b) From the **Entity** drop-down list, select one of the following:
      - For the *Scofflaws* list: **Unassigned**.
      - For the *Maintenance* list: **Sharp Lot B** (the Sharp responsible for Lot B entry point).

   c) From the **Schedule** drop-down list, select one of the following:
      - For the *Scofflaws* list: **Always**.
      - For the *Maintenance* list: **Weekdays 6:00 PM to 10:00 PM** (the schedule you created).

      IMPORTANT: This may result in a limitation where a Maintenance vehicle is read correctly between 6:00 PM to 10:00 PM (the gate to Lot B will open), but an intervention message will still be generated because of No Match events to faculty and student vehicles.

   d) Click **Next**.
6. In the **Action** page, select the action and attributes for each type of event, and then click **Next**.
   - For *License plate hit* events on the *Maintenance* list, select **Trigger output**, and then select the **Output pin** and **Output behavior** required to grant access to the parking lot (for example, open a gate).
   - For *License plate hit* events on the *Scofflaws* list, select the action you want Security Center to take. For example, you could send a message or email to a security personnel.
7. In the **Creation summary** page, review your event-to-action, and then click **Save** to proceed, or **Back** to make changes.

Related Topics

LPR-based access control on page 676
Creating event-to-actions on page 177

40

AutoVu™ mobile systems

This section includes the following topics:

Preparing to deploy mobile AutoVu™ systems

To make sure that your mobile AutoVu™ deployment goes smoothly, you must perform a series of pre-configuration steps.

Before deploying a mobile AutoVu™ system:

1 Install the following Security Center software components:

   a) Security Center Server software on your main server.

      The *main server* is the computer hosting the *Directory* role.

   b) (Optional) Security Center Server software on expansion servers.

      An *expansion server* is any other server on the system that does not host the Directory role. You can add expansion servers at any time.

   c) Security Center Client software on at least one workstation.

      For more information about installing Security Center, see the *Security Center Installation and Upgrade Guide*.

2 Install the mobile Sharp hardware (see the *AutoVu™ Hardware Installation Guide*).

3 Install Patroller and related hotfixes (see the *Patroller Administrator Guide)*.

4 Upgrade AutoVu™ Patroller and Sharp units to the latest software and firmware (see the *Patroller Administrator Guide* and the *Sharp Administrator Guide.*

   NOTE: You can perform certain upgrades from Security Center Config Tool.

Deploying mobile AutoVu™ systems

To integrate a variety of LPR capabilities, you can deploy your mobile AutoVu™ system.

Before you begin

Perform the pre-configuration steps.

What you should know

Information about setting up a typical mobile AutoVu™ deployment is provided here. Your process might be different, depending on your specific installation requirements.

NOTE: Settings that are pre-configured during your installation are not listed in this task. For example, when you install Security Center, the LPR Manager root folder is automatically created on your computer at the location *C:\Genetec\AutoVu\RootFolder*.

To deploy a mobile AutoVu™ system:

1. Log on to the Sharp Portal, and configure the Sharp for a mobile AutoVu™ system. For information about logging on to the Sharp Portal, see the *Sharp Administrator Guide*.
2. Connect Patroller to Security Center so that Patroller is discovered by the LPR Manager.
3. Connect mobile Sharp units to Patroller (see the *Patroller Administrator Guide)*.
4. Configure the LPR Manager server and database settings.

   NOTE: You can also add an additional server to act as failover server for the LPR Manager.

5. Create and configure hotlist entities.
6. Configure Patroller (see the *Patroller Administrator Guide)*.

After you finish

Configure the additional settings for your AutoVu™ mobile installation type:

- Law Enforcement.
- City and University Parking Enforcement.
- Mobile License Plate Inventory.

About AutoVu™ Patroller

Type of entity that represents a patrol vehicle equipped with the Patroller software.

A *Patroller* entity represents the in-vehicle software that runs on board a *mobile data computer* (MDC). It verifies license plates captured by LPR units mounted on the vehicle against lists of vehicles of interest and vehicles with permits. It also collects data for time-limited parking enforcement. The *Patroller* interface alerts users of license plates matching the above rules so that immediate action can be taken.

Depending on your AutoVu™ solution, Patroller can be used to do the following:

- Verify license plates read from LPR cameras against lists of vehicles of interest (hotlists) and vehicles with permits (permit lists).
- Alert you of hotlist, permit, or overtime hits so that you can take immediate action.
- Collect data for time-limited parking enforcement.
- Collect license plate reads to create and maintain a license plate inventory for a parking facility.

Connecting Patroller to Security Center

You need to configure Patroller and Security Center so the LPR Manager can discover and communicate with the Patroller units it controls.

To connect a Patroller to Security Center:

1. From the home page in Security Center Config Tool, click **System** > **Roles**, and then select the LPR Manager you want to configure.
2. Click the **Properties** tab, and then click **Live**.
3. In the **Listening port** option, select the port to listen for connection requests coming from Patrollers.
4. To encrypt the communication between Security Center and Patroller Config Tool, select the **Encrypt communication channel** option.

   IMPORTANT: This setting also needs to be applied in Patroller Config Tool.
5. To allow Security Center to still accept incoming connections from Patrollers that do not have the encryption option enabled, select the **Access non encrypted messages** option.
6. Click **Apply**.
7. Open Patroller Config Tool.
8. Go to Security Center, and turn on the **Connect to Security Center** option.
9. Enter the IP address of the Security Center machine hosting the LPR Manager role.
10. Enter the Port number Patroller should use to connect to the LPR Manager role.
11. If you chose the Encrypt communication channel option in Security Center Config Tool, turn the on the Encrypt communication channel option.
12. Enter the Update provider port that Security Center uses to send updates to Patroller and connected Sharp units.

    NOTE: Enter the same Update provider **Listening port** that is configured in Security Center Config Tool.
13. Select which **Live events** you want to send to Security Center.
14. Beside **Periodic transfer**, specify how often hotlist and permit list changes are downloaded to Patroller (if you have a live connection). The default transfer period is every 240 minutes. You can disable Periodic transfer on specific hotlists (not permit lists) in Security Center Config Tool on the hotlist's Advanced page.

Configuring Patroller

In the **Properties** tab, you can configure sound management, acknowledgment buffer settings, and a hit delay for the Patroller unit.

Before you begin

Connect Patroller to Security Center.

What you should know

Information about the computer hosting the Patroller entity under **Properties** cannot be modified.

To configure :

1. Open the **LPR** task.
2. Select the Patroller you want to configure, and click the **Properties** tab.
3. Under **File association**, select how the Patroller behaves with hotlists and/or permit lists.
   - **Inherit from LPR Manager role:** Patroller uses the hotlists and permit lists associated with its parent LPR Manager. This is the default setting.
   - **Specific:** Associate specific hotlists or permit lists with the Patroller unit rather than the LPR Manager. If you later want to move the Patroller entity to another LPR Manager on your system, the hotlist or permit list will follow.
4. Under **Sound management**, configure Patroller to play a sound when reading a plate and/or generating a hit, and choose whether sounds should be played even when Patroller is minimized
   - **Play sound on hit:** Plays a sound when Patroller generates a hit.
   - **Play sound on read:** Plays a sound when Patroller reads a plate.
   - **Play sounds even when minimized:** Play sounds even if the Patroller window is minimized.
5. Under **Acknowledgment buffer**, specify a buffer restriction that limits how many hits can remain unacknowledged (not accepted or rejected) before Patroller starts automatically rejecting all subsequent hits. You can also choose (by priority) which hotlists should comply with this restriction
   - **Reject count:** How many unacknowledged hits are allowed.
   - **Reject priority:** When you create a hotlist entity, you can specify a priority for that hotlist. This setting tells Patroller which hotlist(s) should comply with the buffer restriction.
6. Under **Hotlist and permit**, specify the Duplicate hotlist or permit hit delay that tells Patroller to disregard multiple hits on the same plate for the duration of the delay. For example, if you set a delay of 10 minutes, no matter how many times Patroller reads the same plate during those 10 minutes, it will generate only one hit.

The Patroller unit is configured in Security Center, and is downloaded to Patroller the next time it connects to Security Center.

After you finish

Configure Patroller using Patroller Config Tool (see the *Patroller Administrator Guide)*.

Adding user custom fields to reads and hits

To associate a user's metadata with individual Patroller reads and hits so you can query and filter for those user custom fields in Security Desk *Reads* and *Hits* reports, you can add user custom fields to LPR annotation fields.

Before you begin

Configure Patroller to require a username and/or password to log on (see the *Patroller Administrator Guide*).

What you should know

You cannot add custom fields to reads and hits if Patroller is set to "No logon", because the reads and hits must be attached to a valid username.

To add-user-related custom fields to reads and hits:

1 Create the custom field that applies to user entities.
2 Define the custom field for your Patroller users.
3 Add the custom field as an annotation field.

The custom field is now available as two separate columns in Security Desk "Reads" and "Hits" reports. One is a *Custom field* column that displays the latest value configured for the User entity. The other column is an *Annotation field* column that displays the value for the User entity when the read or hit was stored by the LPR Manager role. For more information about Viewing LPR events in Security Desk, see the *Security Desk User Guide*.

Example

You have several Patroller users that alternate between different patrol teams, such as police officers moving between different city zones. By defining each patrol team as a user custom field, you can generate a report in Security Desk that displays the reads or hits collected when the officer was in patrol team A, patrol team B, and so on.

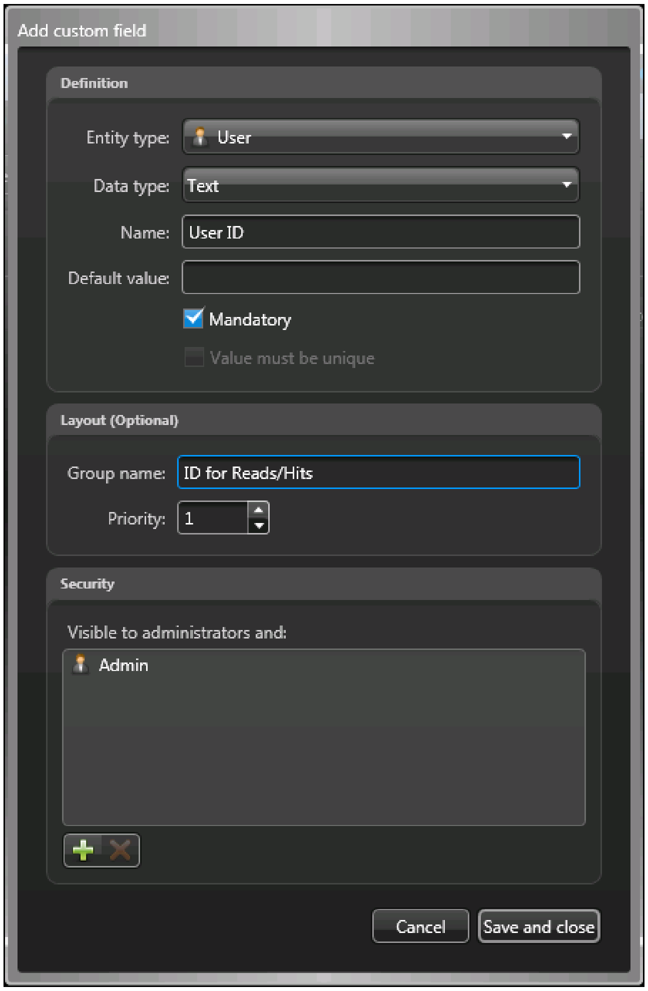
Related Topics
About custom fields on page 69

Creating user custom fields

To use custom fields with hits and reads, you must first create a custom field that applies to user entities.

To create a user custom field:

1 Open the **System** task, and click the **General settings** view.
2 Click the **Custom fields** page, and click ✚ at the bottom of the custom field list.
3 From the **Entity type** drop-down list in the **Add custom field** dialog box, select **User**.



Add custom field

Definition

Entity type: User

Data type: Text

Name: User ID

Default value:

☑ Mandatory

☐ Value must be unique

Layout (Optional)

Group name: ID for Reads/Hits

Priority: 1

Security

Visible to administrators and:

Admin

4 From the **Data type** drop-down list, select a standard or custom data type for the custom field.

For example, select **Text**.

5 In the **Name** field, type the name for the custom field.

For example, type **User ID**.

6 (Optional) In **Default value** field, type or select the default value for this field.

7 Depending on the selected data type, the following additional options appear:

- **Mandatory:** Select it if this custom field cannot be empty.
- **Value must be unique:** Select it if the value of this custom field must be unique.

  NOTE: The *unique value* option can only be enforced after the field is created. To enforce this option, you must first make sure that all entities in your system have a distinct value for this custom field, then come back to this tab to apply the unique value option to it.

8 (Optional) Under the **Layout** section, type the **Group name,** and select the **Priority** from the drop-down list.

These two attributes are used when displaying the field in the **Custom fields** tab of associated entity. The group name is used as the group heading, and the priority dictates the display order of the field within the group.

9 (Optional) Under the **Security** section, click + to add users and user groups that will be able to see this custom field. By default, only administrative users can see a custom field.

10 Click **Save and close**.

The new user custom field **User ID** is available in your users' **Custom fields** tab.

Defining custom fields for Patroller users

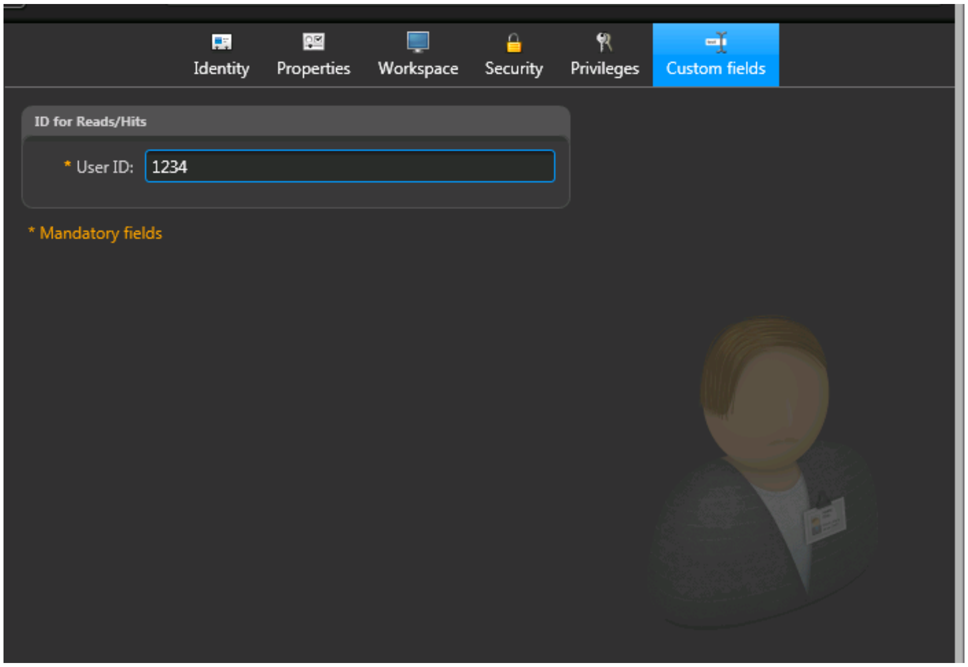
After user custom fields are created in Security Center, you can define them in the *Custom fields* tab of the Patroller users.

To define a custom field for a Patroller user:

1 From the home page, click **Security** > **Users**, and then select the user you want to configure.

2 Select the **Custom fields** tab.

Custom fields that are already created for user entities are displayed.



* User ID: 1234

* Mandatory fields

3 Type the **User ID** for the current Patroller user.

For example, type **1234**.

4 Click **Apply**.

This Patroller user now has a User ID of 1234. You can now add this custom field as an annotation field for reads and hits.

Related Topics
Creating user custom fields on page 687

Adding custom fields as annotation fields

After you have created and defined custom fields for Patroller users, you must add those custom fields to the list of annotation fields for Patroller reads and hits.

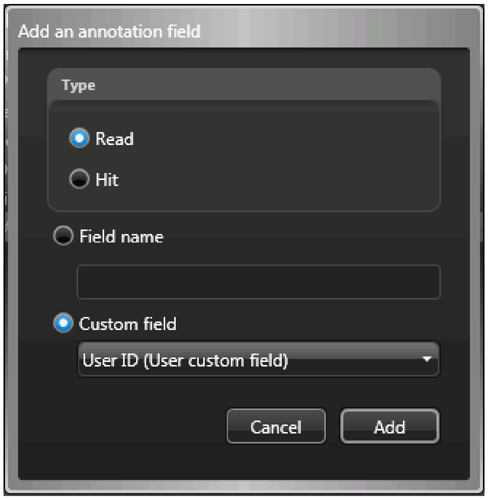
To add a custom field as an annotation field:

1 From the home page, click **LPR** > **General settings** > **Annotation fields**.

2 Click **Add an item** (✚).

The **Add an annotation field** window appears.

3 Under **Type**, in the **Add an annotation field** dialog box, select **Read** or **Hit**.



● Read
○ Hit

○ Field name

● Custom field
User ID (User custom field)

4 Select **Custom field**, and then select the user custom field you created.

5 Click **Add**.

Your user custom field is added to the list of annotation fields for all Patroller reads or hits, depending on what you selected for the *Type* option (read or hit). Security Center now associates reads or hits with the user custom field (the **User ID** in this case**)** that was logged on to Patroller at the time the event occurred. This value is stored in the database for each read or hit.

NOTE: If you want the same user custom field for reads *and* hits, you must define it as an annotation field twice, once for reads and once for hits.

Related Topics

Creating user custom fields on page 687

Default Patroller sound files

There are four default sound files that Patroller uses for LPR events, which are located on the in-vehicle computer in *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds* (default location).

The default sound files are the following:

- **HotlistHitEvent:** Used for hotlist hits.
- **OvertimeHitEvent:** Used for overtime hits.
- **PermitHitEvent:** Used for permit hits or shared permit hits.
- **VehicleEvent:** Used for plate reads.

You must know the following about the default sound files:

- Sounds for overtime hits, permit hits, and plate reads must use the filenames *OvertimeHitEvent*, *PermitHitEvent*, and *VehicleEvent*, and the files must be located in the *Sounds* folder. Patroller will not play new sounds for these events if they have different filenames or if they are in different locations.

  Example: If you have a file called *alert.wav*, and you want to use it for a permit hit, you must rename your file to *PermitHitEvent* before copying it to the *Sounds* folder (either manually or through the updater service). This way it overwrites the default sound file, and Patroller can play it.
- Sounds for hotlist hits have more flexibility. You can overwrite the default sound *HotlistHitEvent* in the *Sounds* folder, or you can use a different filename for each hotlist loaded in Patroller, as long as you specify the path to each hotlist's sound file in Security Center Config Tool.

  BEST PRACTICE: New hotlist sound files can be stored anywhere on the in-vehicle computer, but you should keep them in the same *Sounds* folder as the default sound files. This makes it easier to update them later.

Changing sound files for LPR events

You can add new sound files to Patroller to use for LPR events, by manually copying the sounds to the Patroller in-vehicle computer.

What you should know

The sound files must be *.wav* format.

To change the sound files for LPR events:

1 Log on to the Patroller in-vehicle computer.

2 To overwrite the default sound files, do the following:

   a) Open the folder *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds*.

   b) Rename your sound file to match the default file you want to overwrite.

   c) Copy your new sound file to the *Sounds* folder so that it overwrites the default file.

3 (Optional) To use a sound file with a different filename for hotlists, do the following:

   a) Copy your new sound file to any location on the in-vehicle computer.

   b) Open Config Tool.

   c) From the home page, open the **LPR** task.

   d) Select the hotlist to configure, and click the **Advanced** tab.

   e) In the **Sound file** field, specify the path and filename to the sound file on the in-vehicle computer.

   f) Repeat Step d and e for as many hotlists as you want.

4 Restart Patroller for your changes to take effect.

Patroller uses the new sound file for the LPR event.

Related Topics

Default Patroller sound files on page 691

Changing sound files for LPR events using the updater service

You can send different sound files to the Patroller's *MobileClient* folder using the Security Center updater service.

What you should know

The sound files for permit hits, overtime hits, and plate reads must be in the default *Sounds* folder for Patroller to be able to play them.

After sending the files to the *MobileClient* folder, you can manually move the files to the *Sounds* folder if you choose, but you can also zip your sound file so that Windows extracts it to the *Sounds* folder automatically.

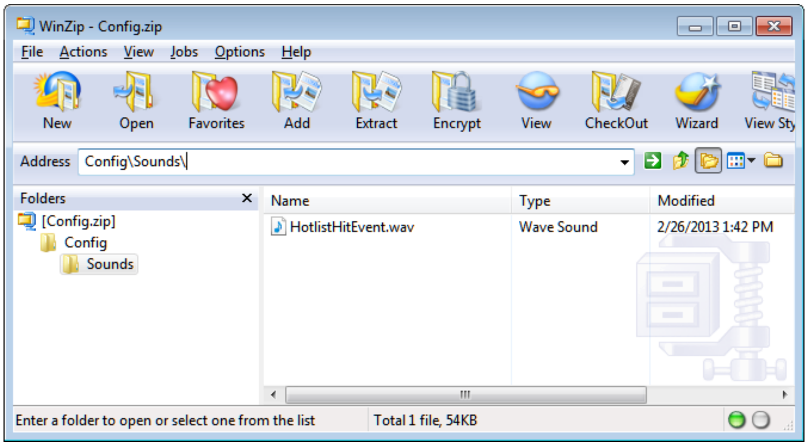
To change the sound files for LPR events using the updater service:

1 (Optional) If you want to overwrite a default sound file, rename your new sound file to match the name of the default file you want to replace (for example, *HotlistHitEvent.wav*).

2 On the Security Center computer, create the same Windows Explorer file structure found on the Patroller in-vehicle computer (for example, *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds*).

3 Copy your new sound file to the *Sounds* folder you created.

4 Zip the sound file at the *Config* level so that it mirrors the relative path from the *MobileClient* folder to the *Sounds* folder on the in-vehicle computer.



Address Config\Sounds\

Name	Type	Modified
HotlistHitEvent.wav	Wave Sound	2/26/2013 1:42 PM

Enter a folder to open or select one from the list | Total 1 file, 54KB

The file extracts to the destination defined in the zip file path (*Sounds* folder).

5 (Optional for hotlist sounds) If the file has a different filename than the default *HotlistHitEvent*, you must specify the full path to the file, including the new filename:

a) From the Config Tool home page, open the **LPR** task.

b) Select the hotlist to configure, and click the **Advanced** tab.

c) In the **Sound file** field, specify the path and filename to the sound file on the in-vehicle computer.

d) Repeat the steps for as many hotlists as you want.

6 Send the sound file to Patroller as if you were installing an update wirelessly.

Patroller restarts after installing the update, and now uses the new sound file for your chosen LPR event.

Related Topics

Default Patroller sound files on page 691

41

AutoVu™ Law Enforcement systems

This section includes the following topics:

About Law Enforcement

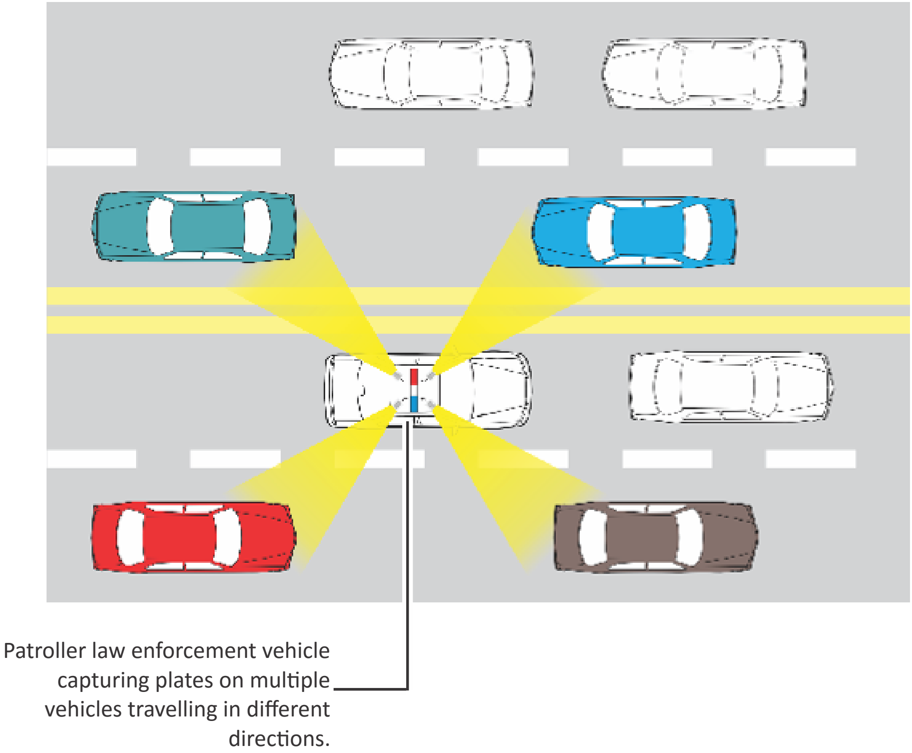
Law Enforcement is a Patroller software installation that is configured for law enforcement: the matching of license plate reads against lists of wanted license plates (hotlists). The use of maps is optional.

As you patrol, the Sharp cameras installed on the vehicle automatically read plates and send the information to Patroller. If a plate is on a loaded hotlist, Patroller alerts you, and you can take immediate action.

Hotlists typically contain information on stolen vehicles, scofflaw suspects, amber alerts, and so on. The use of in-vehicle mapping with a Law Enforcement installation is optional.

Example

You can have up to six Sharp cameras installed on a Patroller vehicle. This allows you to capture the maximum number of plates on vehicles in different lanes and even those travelling in the opposite direction. The following diagram shows a Patroller law enforcement vehicle outfitted with four cameras:


Patroller law enforcement vehicle capturing plates on multiple vehicles travelling in different directions.

Creating hit accept and hit reject reasons

You can create customized reasons to appear in Patroller that a user can select from when rejecting or accepting a hit.

What you should know

The settings are downloaded along with the selected hotlists and permit lists to Patrollers when the Patroller user logs on. Hit reject and accept reasons are applied at the Directory level, which means that all the LPR Managers in your ssytem share the same settings.

- **Hit reject reasons:** List of reasons for rejecting hotlist hits. These values also become available as Reject reason filter options for generating hit reports in Security Desk. Several categories are pre-configured for you when you install Security Center.
- **Hit accept reasons:** A form that contains a list of questions that Patroller users must answer when they accept a hit. The information from the hit form can be queried in the Security Desk Hit report. There are no pre-configured categories.

The attributes you create are also available as filter options for hit reports in Security Desk.

To create hit accept and hit reject reasons:

1. From the home page, click **LPR** > **General settings** > **Hotlist**.
2. Add **Hit accept reasons** or **Hit reject reasons** as needed.
3. Click **Apply**.

The new hit accept and reject reasons are downloaded to Patroller the next time it is connected to Security Center.

Creating New Wanted attributes and categories

You can create customized license plate attributes and categories to appear in Patroller, that a user can select from when they are adding a *New wanted* license plate.

What you should know

The *New wanted* feature allows you to manually add a license plate to Patroller's local hotlist file on the in-vehicle computer. This is helpful if you are searching for a specific plate that is not on the hotlists loaded in Patroller, but you cannot download the new vehicle's information because you are not wirelessly connected to headquarters.

- **New wanted attributes:** Attributes other than the standard ones (plate number, plate issuing state, category) that a Patroller user is asked to specify when entering a new wanted item in the Patroller. One category is pre-configured for you when you install Security Center.
- ***New wanted* categories:** List of categories that a Patroller user can pick from when entering a new wanted item. The category is the attribute that says why a license plate number is wanted in a hotlist. Several categories are pre-configured for you when you install Security Center.

  NOTE: BOLO is an acronym for "be on the lookout", sometimes referred to as an all-points bulletin (APB).

New wanted categories and attributes are applied at the Directory level, which means that all the LPR Managers in your system will share the same settings.

To create *New wanted* attributes and categories:

1. From the home page, click **LPR** > **General settings** > **Hotlist**.
2. Add **New wanted attributes** or **New wanted categories** as needed.
3. Click **Apply**.

The *New wanted* attributes and categories are downloaded to Patroller the next time it is connected to Security Center.

After you finish

Configure the *New wanted* attributes and categories in Patroller Config Tool. For more information, see the *Patroller Administrator Guide*.

42

AutoVu™ City and University Parking Enforcement systems

This section includes the following topics:

About City Parking Enforcement

City Parking Enforcement is a Patroller software installation that is configured for the enforcement of parking permit and overtime restrictions.

In City Parking Enforcement, Patroller matches plates on parked vehicles to overtime rules alone (rules about how long vehicles are allowed to park), permit lists alone (lists of vehicles that are allowed to park), or both together.

You can also use City Parking Enforcement with wheel imaging with to provide additional evidence of whether or not a vehicle has moved.

Example

Here are some examples of when you would use each type of enforcement rule:

- **Overtime rule alone:** To maximize turnover, and avoid free parking abuse in a commercial area, vehicles are allowed to park for only two hours on main streets between 8:00 A.M. and 6:00 P.M. Any vehicles parked for more than two hours are in violation of the overtime rule. This results in an overtime hit in Patroller. In this example, you don't need a permit list because there are no exceptions to the rule.
- **Permit list alone:** Some residential areas allow only permit holders to park on neighborhood streets. Any vehicle parked in the area without a permit is in violation of the permit list. This results in a permit hit in Patroller. In this example, you don't need an overtime rule because there are no time limits. Any vehicle parked without a valid permit (e.g. expired permit, no permit at all, etc) is in violation, regardless of the day or time.
- **Overtime rule and permit list together:** Some residential areas allow permit holders to park indefinitely, and non-permit holders to park for a limited time. Any vehicle without a permit, that is parked in the area longer than the limit allows, is in violation of the overtime rule. This results in an overtime hit. In this example, you need both an overtime rule, and a permit list to determine if a parked vehicle is in violation.

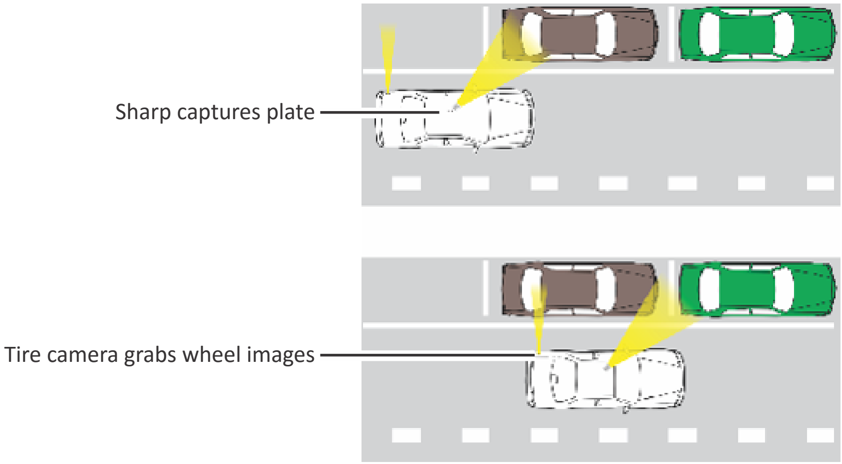
About City Parking Enforcement with Wheel Imaging

In a City Parking Enforcement with Wheel Imaging system, Patroller uses wheel images taken by "tire cameras" as additional evidence of whether or not a parked vehicle has moved even a small distance.

For example, when you get an overtime hit, you can look at the vehicle's wheels and see by the valve stem or other reference point (e.g. crack in the hubcap), that the vehicle hasn't moved. This photographic evidence can help prove the overtime offense if the driver claims to have moved the vehicle, and then parked again in the same area.

Example

Here is a Patroller vehicle with a Sharp camera and a single tire camera.



You cannot do wheel imaging on both sides of a street at the same time.

For wheel imaging to be effective, you must have the AutoVu™ Navigator box installed in the vehicle. The Navigator box comes with a GPS receiver that receives satellite positioning information, but it also taps into the vehicle's odometer readings and has an internal gyroscope. This provides greater accuracy than GPS alone.

For example, drive through a long tunnel and you'll lose the GPS satellite signal, but the Navigator box still knows how far and how fast you're driving (odometry signal), and if you change direction (gyroscope). The Navigator box is installed in the vehicle, and is connected to the vehicle's odometry signal and in-vehicle computer. To calibrate the Navigator box, see the the *AutoVu Hardware Installation Guide*.

Long term overtime

Long term overtime is used for long term parking; that is, where vehicles can park in the same space for over 24 hours. With long term overtime, you can specify a time limit between 2 to 5 days. This option automatically sets the overtime rule category to *Same position*, which means that the vehicle is in violation if it is parked in the same parking space beyond the time limit specified.

IMPORTANT: You can only enforce one long term overtime rule per Patroller. If you have more than one Long Term Overtime zone configured in Security Center, you must specify the name of the zone you want Patroller to display. This setting is configured in the advanced overtime settings of Patroller Config Tool (see the *Patroller Administrator Guide*.

About University Parking Enforcement

University Parking Enforcement is a Patroller software installation that is configured for university parking enforcement: the enforcement of scheduled parking permits or overtime restrictions. The use of maps is mandatory. Hotlist functionality is also included.

Unlike with City Parking Enforcement, the following also applies to University Parking Enforcement:

- You apply a permit restriction to one or more permit lists, to specify where and when the permits apply.
- You can enforce overtime rules or permit restrictions for a selected parking lot, but not both at the same time.
- Wheel imaging is not supported.

Example

The following examples show when you would use an overtime rule, and when you would use a permit restriction:

- **Overtime rule:** A university campus has several parking lots reserved for students and faculty, but also has conveniently located parking areas that are used by delivery vehicles for the loading or unloading of equipment.

  Using an overtime rule, you can allow any vehicle to park in the loading area at any time of day, but only for a limited time (e.g. 20 minutes). A vehicle parked over that time is in violation of the overtime rule. This results in an overtime hit in Patroller. In this example, you don't need a permit restriction because any vehicle can park, but only for a limited time.
- **Permit restriction:** A university parking lot can be used by both faculty and students, but at different times. Faculty can park on weekdays from 8:00 A.M. to 6:00 P.M., while students can park from 10:00 A.M. to 4:00 P.M. This reserves the prime parking spaces for the university's faculty, but still allows students convenient parking during peak class hours. You wouldn't be able to create this parking scenario with an overtime rule. You need a permit restriction and associated permit lists. Vehicles without a permit, with an expired permit, or parked at the wrong time, are in violation of the permit restriction. This results in a permit hit in Patroller.

Related Topics

About permits on page 712

Differences between City and University Parking Enforcement

The parking rules that you use , and how you configure them, depend on whether you have City or University parking enforcement type.

The following table shows you which parking enforcement concepts and features are used with each type of system:

Concept or feature	City Parking Enforcement	University Parking Enforcement
Enforce permits and overtime simultaneously	Yes	No
District overtime	Yes	Yes
Block face overtime	Yes	Supported but not typically used.
Same position overtime	Yes	Supported but not typically used.
Multiple violations	Yes	Yes
Permits	Yes	Yes[1]
Permit restrictions	No	Yes
Shared permits	Yes	Yes
Parking lots (“zones”)	Yes	Yes
Wheel imaging	Yes[2]	No
Long term overtime	Yes[3]	No
Hotlist hits	Yes	Yes

[1] Permits must have permit restrictions applied to them in University Parking Enforcement.

[2] Used to provide additional evidence that a vehicle has moved.

[3] Requires the City Parking Enforcement with Wheel Imaging option to determine if a parked vehicle has not moved for the duration of the overtime period.

Deploying AutoVu™ City and University Parking Enforcement systems

You can configure your mobile AutoVu™ system specifically for City Parking Enforcement (with or without wheel imaging) or University Parking Enforcement.

Before you begin

Perform the general configuration tasks for mobile AutoVu™ systems.

To deploy an AutoVu™ City or University Parking Enforcement system:

1. Create the overtime rules.
2. Create the permit lists.
3. (*University Parking Enforcement* only) Create the permit restrictions.
4. Create parking lots for your overtime rules and permit restrictions.
5. (*City Parking Enforcement with Wheel Imaging* only) To provide accurate odometry readings to Patroller, calibrate the Navigator box (see the *AutoVu™ Hardware Installation Guide*).
6. Enable and configure overtime settings in Patroller. For more information, see the *Patroller Administrator Guide*.
7. Enable and configure permit lists in Patroller. For more information, see the *Patroller Administrator Guide*.
8. (*City Parking Enforcement with Wheel Imaging* only) Configure the Patroller settings related to wheel imaging. For more information, see the *Patroller Administrator Guide*.
9. Configure the Patroller GPS and Map settings. For more information, see the *Patroller Administrator Guide*.

   All parking enforcement systems require GPS and mapping capability.

About overtime rules

An overtime rule is a type of entity that defines a parking time limit and the maximum number of violations enforceable within a single day. Overtime rules are used in city and university parking enforcement. For university parking, an overtime rule also defines the parking zone where these restrictions apply.

The overtime entity is downloaded to Patroller. In Patroller, an overtime hit occurs when the time between two plate reads of the same plate is beyond the time limit specified in the overtime rule. For example, your overtime rule specifies a four hour parking limit within a city district. The Patroller operator does a first pass through the district at 9:00 A.M. collecting *license plate reads*. The operator then does a second pass through the district at 1:05 P.M. If a plate was read during the first and second pass, Patroller will generate an overtime hit.

The overtime rule is a type of hit rule. A hit rule is a method used by AutoVu™ to identify vehicles of interest. Other types of hit rules include *hotlist*, *permit*, and *permit restriction*. When a plate read matches a hit rule, it is called a hit. When a pair of plate reads (same plate read at two different times) violates an overtime rule, it is called an overtime hit.

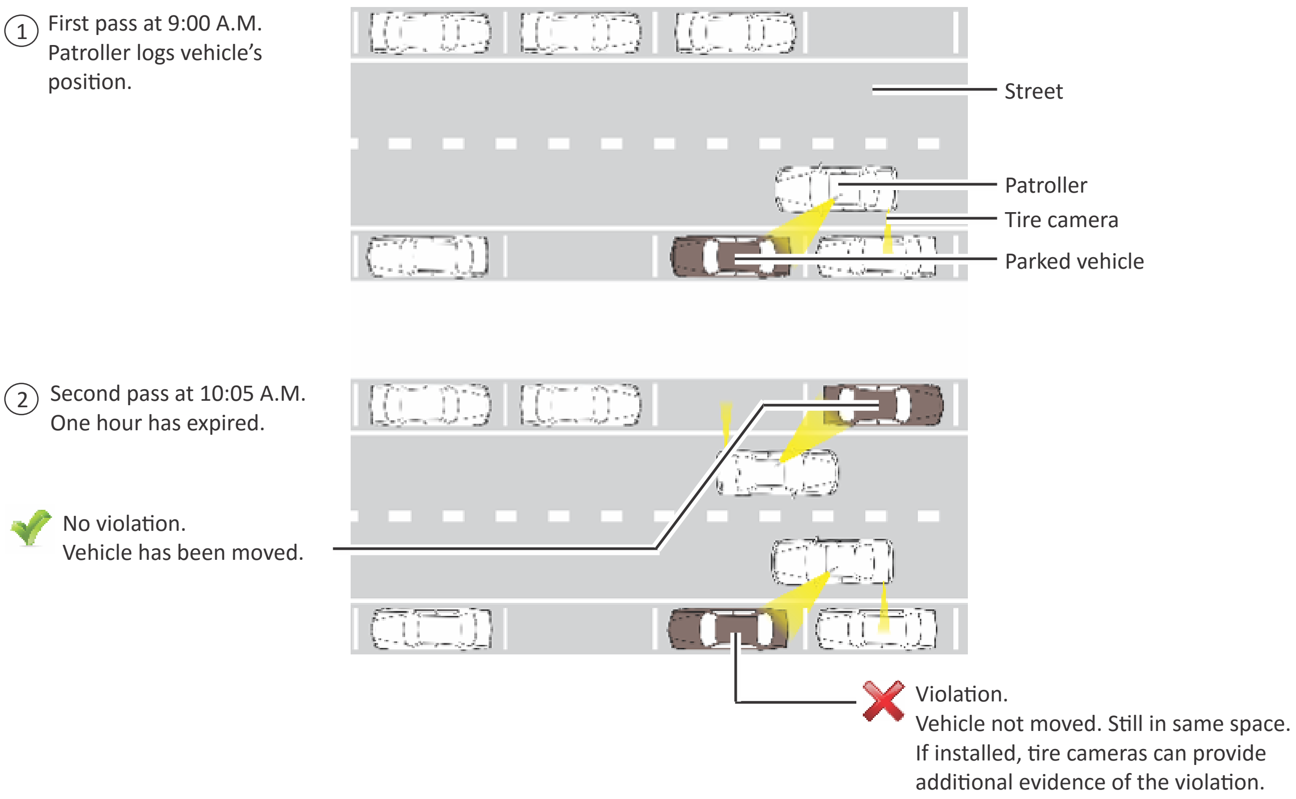
In City enforcement the wheel imaging option can be used to provide additional evidence of the violation by showing whether or not the vehicle has moved even a small distance.

Same position overtime rules

Same position overtime rules specify how long a vehicle is allowed to park in a *single parking space* on a particular street.

Example

The overtime rule states that vehicles can park for one hour in any parking space on Street X. You do a first pass at 9:00 A.M. collecting license plate reads. You then do a second pass at 10:05 A.M. If Patroller reads the same plate in the same parking space, Patroller generates an overtime hit.



1 First pass at 9:00 A.M. Patroller logs vehicle's position.

2 Second pass at 10:05 A.M. One hour has expired.

✓ No violation. Vehicle has been moved.

✗ Violation. Vehicle not moved. Still in same space. If installed, tire cameras can provide additional evidence of the violation.

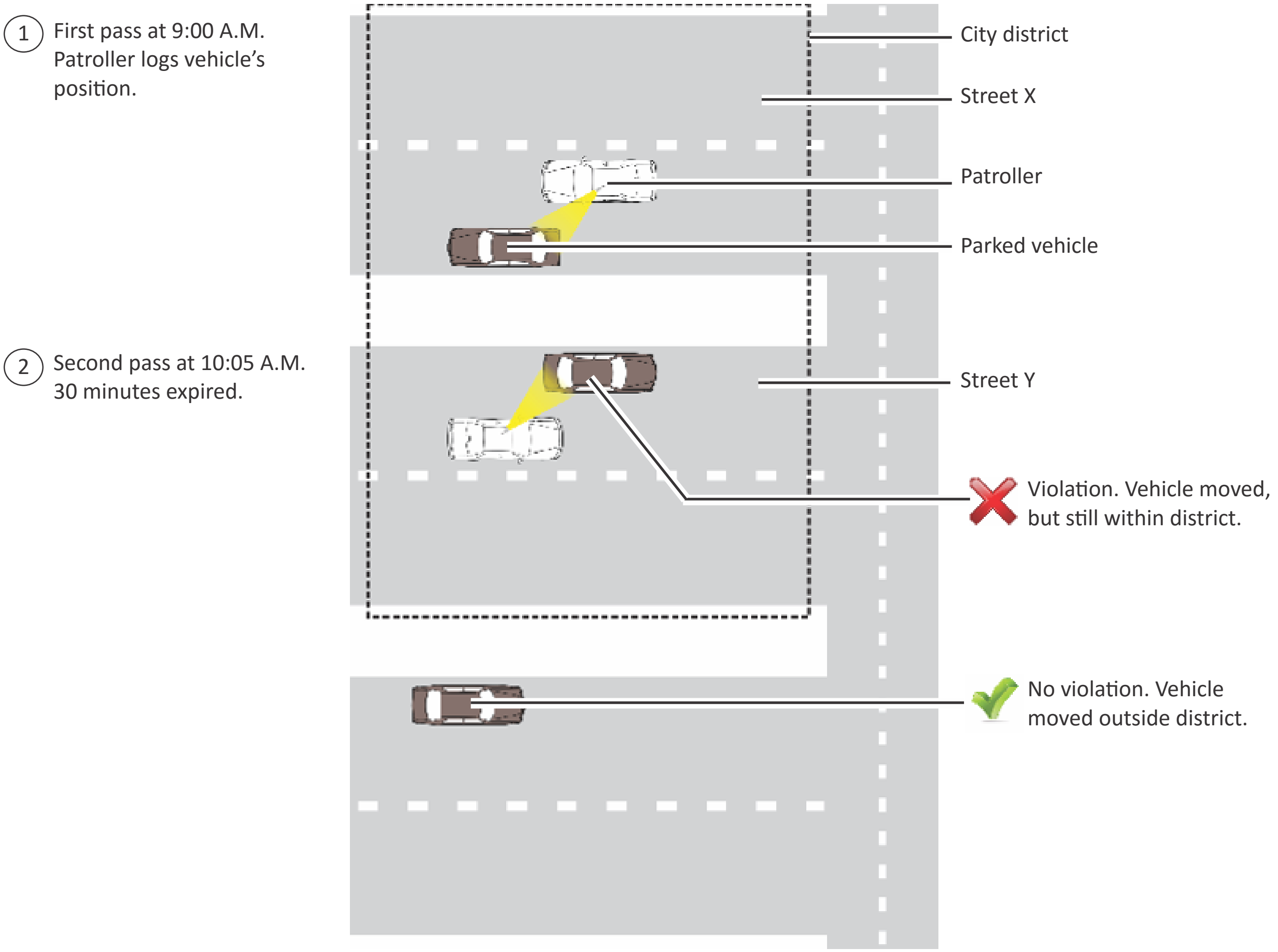
District overtime rules

District parking enforcement is a type of overtime rule that specifies when a vehicle is allowed to park *within a specific geographic location* (for example, a city district).

The borders of a "district" are not defined in Security Center Config Tool (for example, by drawing a polygon on a map), and there is no correlation with a city's formal boroughs or municipalities. A district exists where the Patroller user chooses to enforce it.

Example

The overtime rule states that between 9:00 A.M. and 5:00 P.M. on weekdays, vehicles can park for only 30 minutes within the district defined by Street X and Street Y. You do a first pass through the district at 9:30 A.M. collecting license plate reads. You then do a second pass through the district at 10:05 A.M. If Patroller reads the same plate within the same district (regardless if the vehicle has moved or not), the vehicle is in violation of the overtime rule, and you get an overtime hit.


1 First pass at 9:00 A.M. Patroller logs vehicle's position.
2 Second pass at 10:05 A.M. 30 minutes expired.
City district
Street X
Patroller
Parked vehicle
Street Y
Violation. Vehicle moved, but still within district.
No violation. Vehicle moved outside district.

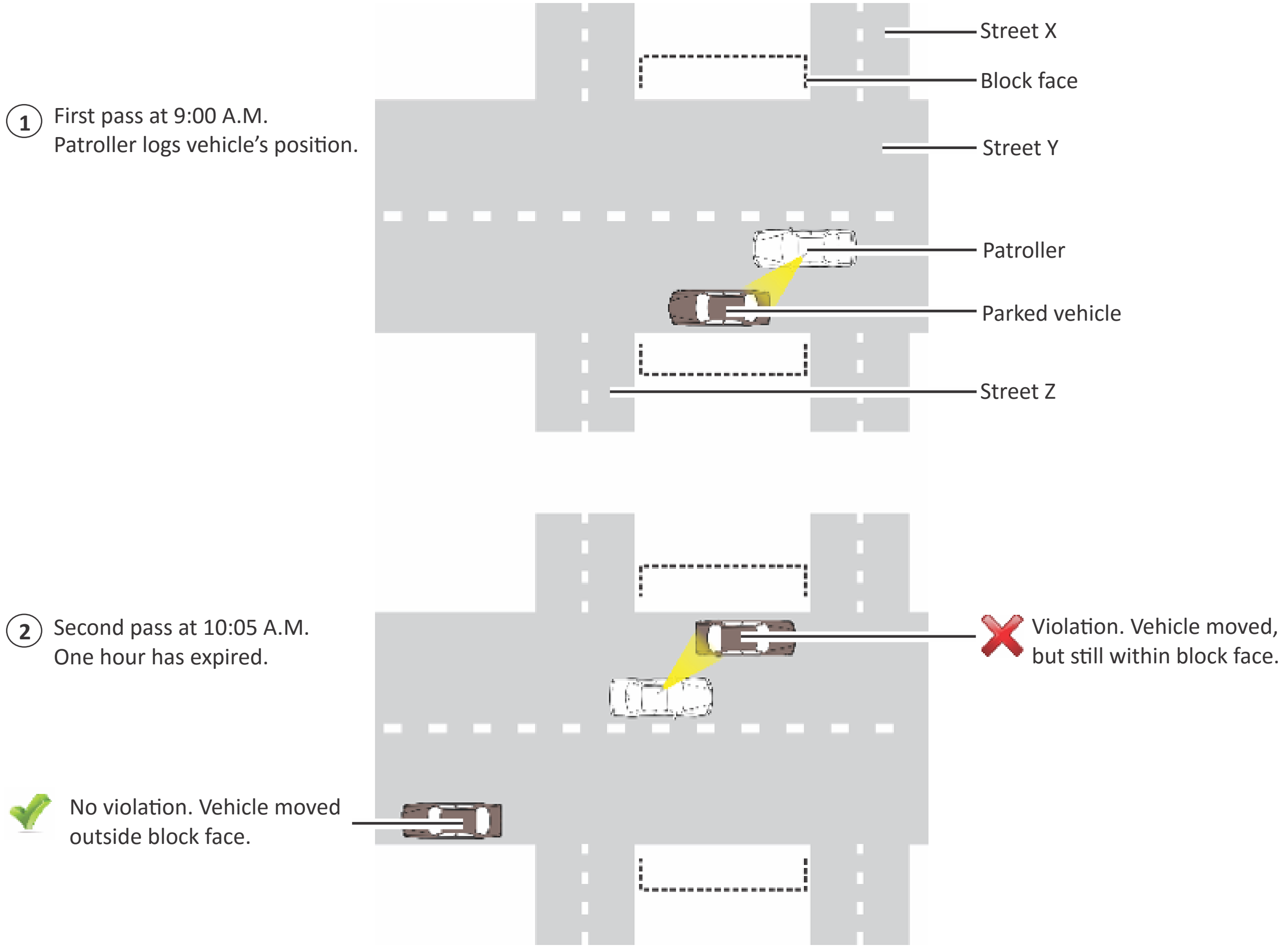
Block face overtime rules

Block face parking enforcement is a type of overtime rule that specifies when a vehicle is allowed to park *on both sides of a street*, between intersecting cross-streets.

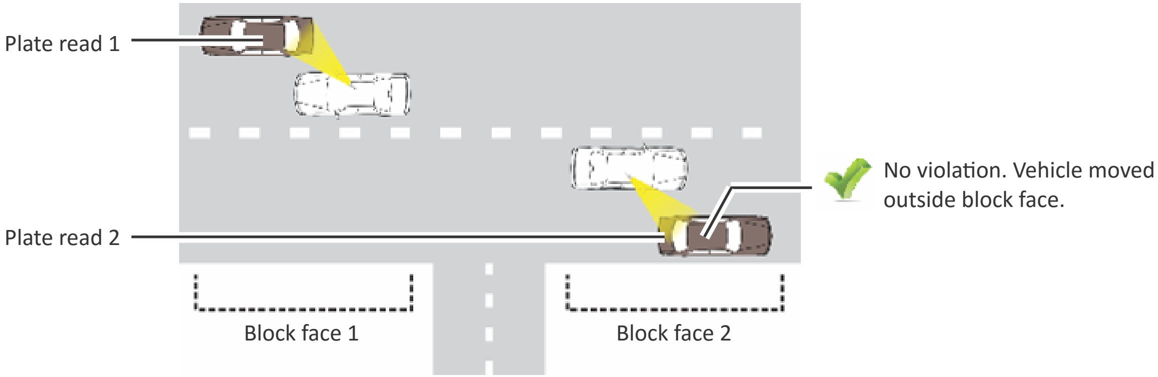
The borders of a "block face" are not defined in Config Tool (for example, by drawing a polygon on a map). They are defined on the spot for each individual plate read. For example, when a Patroller user selects a block face overtime rule, and then reads a license plate, Patroller uses GPS to determine the block face for that particular plate read based on the intersecting cross-streets closest to the parked vehicle's position.

Example

The overtime rule states that vehicles can park for one hour on either side of Street Y, between Street X and Street Z. You do a first pass through the block face at 9:00 A.M. collecting license plate reads. You then do a second pass down the block face at 10:05 A.M. If Patroller reads the same plate within the same block face, the vehicle is in violation of the overtime rule, and you get an overtime hit.


Street X
Block face
1 First pass at 9:00 A.M.
Patroller logs vehicle's position.
Street Y
Patroller
Parked vehicle
Street Z
2 Second pass at 10:05 A.M.
One hour has expired.
Violation. Vehicle moved, but still within block face.
No violation. Vehicle moved outside block face.

NOTE: Patroller considers "T intersections" to be valid borders of a block face. For example, in the following scenario, Patroller would *not* raise an overtime hit because the T intersection is seen as the end of *Block face 1*, and the beginning of *Block face 2*.



Multiple overtime violations

You can add multiple parking regulations to an Overtime rule to specify the maximum number of citations that can be issued to the same vehicle for the same offence.

Example

Here are two examples to explain the difference between having an overtime rule with one violation, and an overtime rule with multiple violations:

- **Overtime rule with one violation:** Your overtime rule allows vehicles to park for one hour on a specific street. If a vehicle is parked in that area longer than an hour, it is in violation of the overtime rule. This results in an overtime hit in Patroller. However, because the overtime rule allows only one violation for the offense, even if the vehicle is parked in the same place all day, you'll only get one overtime hit for it. In this scenario, you would issue one ticket for the offense.
- **Overtime rule with multiple violations:** Your overtime rule allows vehicles to park for one hour on a specific street, but your system is configured to allow multiple violations (e.g. three) of that one hour rule. If a vehicle is parked in that area all day, and you patrol the area three times during your shift, you'll get three violations of the overtime rule, and three separate overtime hits in Patroller. In this scenario, you would issue three tickets for the same offense.

BEST PRACTICE: When configuring multiple violations, the start time of a violation should be greater than or equal to the start time of the previous violation, and the end time of the violation should be less than or equal to the end time of the previous violation.

Example

Violation #1 = 8:00 - 16:00

Violation #2 = 10:00 - 16:00

Violation #3 = 10:00 - 13:00

Creating overtime rules

You create a overtime rule entity in Security Center Config Tool. After you create the entity, you'll configure its settings for your enforcement scenario.

What you should know

You can use overtime rules for both City Parking Enforcement and University Parking Enforcement.

To create an overtime rule:

1. From the home page, click **LPR** > **Overtime rules**, then click **Overtime rule** (✚).
2. In the **Identity** tab, enter the required information:
   - **Name:** In City Parking Enforcement, this name appears in Patroller on the overtime rule selection page. In University Parking Enforcement, this name appears appended to the parking lot name on the zone selection page.

     TIP: Choose a name that describes the details of the enforcement scenario. This makes it easier to select it in Patroller when you have more than one available.
   - **(Optional) Description:** You can add a longer description for the rule. This field does not appear in Patroller.
   - **(Optional) Logical ID:** Enter a Logical ID if applicable.
3. Click **Apply**.

The overtime rule appears in a flat list view that displays all the overtime rules on your system. Patroller downloads overtime rules when it connects to Security Center.

After you finish

Configure the overtime rule.

Configuring overtime rules

To use an overtime rule entity after you have added in Security Center, you must configure it for your enforcement scenario.

Before you begin

Create the overtime rule.

To configure an overtime rule:

1 From the home page, click **LPR** > **Overtime rules**, and select the overtime rule you want to configure.

2 Click the **Properties** tab.

3 Select a **Color** for the overtime rule.

This will be the color of the overtime hit screen in Patroller and Security Desk, as well as the plate reads due for enforcement on the Patroller map.

4 (City Parking Enforcement with Wheel Imaging only) Select the **Vehicle parking position**.

This option tells Patroller which parameters to use for wheel imaging: Parallel or Angled (45-degree).

NOTE: You cannot use the same overtime rule for both Parallel and Angled parking enforcement. If you're doing both types of enforcement, you must create separate overtime rule entities for each.

5 (Optional) Select **Long term overtime** to allow vehicles to park in the same spot for over 24 hours.

When selected, the parking time limit is specified in days (2 to 5 days), and the *Parking enforcement* option is automatically set to *Same position*.This option automatically sets the parking regulation to same position, meaning the vehicle has parked overtime when it stays in the same parking space beyond the parking time limit set for such parking space.

NOTE: This setting applies to AutoVu™ Patroller City Parking Enforcement with or without wheel imaging. *Wheel imaging* is recommended if you plan to use this rule to detect vehicles parked long term so that you can distinguish between someone who parks in the same position and a vehicle which has been abandoned.

IMPORTANT: You can have only one Long term overtime rule per Directory.

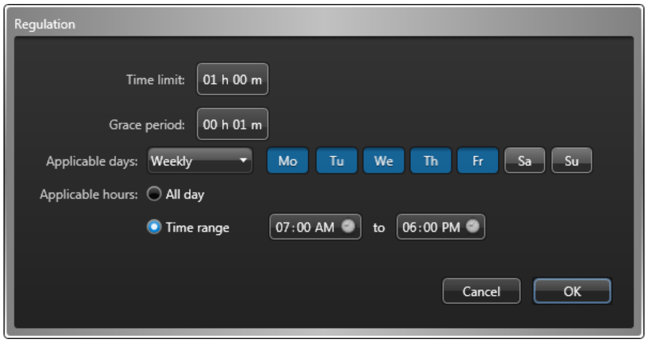
6 From the **Parking enforcement** list, select the type of restricted parking area that applies to the time limit: a single parking spot, a district within a city, or both sides of a city block:

- **Same position:** A vehicle is parked overtime if it parks in the same spot beyond the time limit specified. For example, your overtime rule specifies a one hour parking limit for a single parking space. The Patroller operator does a first pass through the district at 9:00 A.M. collecting license plate reads. The operator does a second pass at 10:05 A.M. If Patroller reads the same plate in the same spot both times, it results in an overtime hit.

  IMPORTANT: For this feature to work, Patroller needs GPS capability.
- **District:** A vehicle is parked overtime if it is parked anywhere within a city district (a geographical area) beyond the specified time limit. For example, your overtime rule specifies a four hour parking limit within a city district. The Patroller user does a first pass through the district at 9:00 A.M. collecting license plate reads. The operator does a second pass through the district at 1:05 P.M. If Patroller reads the same plate in the same district both times, it results in an overtime hit.
- **Block face (2 sides):** A vehicle is parked overtime if it is parked on both sides of a road between two intersections beyond the specified time limit. For example, your overtime rule specifies a 1hour parking limit within a city block face.The Patroller operator does a first pass through the block face at 9:00 A.M. collecting license plate reads. The operator does a second pass down the block at 10:05 A.M. If Patroller reads the same plate in the same block face both times, it results in an overtime hit.

7 Under **Regulation**, click **Add an item** (➕) to define the parameters of the overtime rule (for example, time limit, grace period, applicable days, and so on).

8 In the **Regulation** dialog box, configure the following, then click **OK**:



Regulation

Time limit: 01 h 00 m

Grace period: 00 h 01 m

Applicable days: Weekly — Mo Tu We Th Fr Sa Su

Applicable hours: ○ All day

● Time range 07:00 AM to 06:00 PM

- **Time limit:** The parking time limit in hours and minutes.
- **Grace period:** Time beyond the parking time limit during which overtime violation is waived. For example, Patroller will generate an overtime hit on a plate when time between the capture of the same plate exceeds the Time limit plus the Grace period.
- **Applicable days:** Days of the week when the time limit is enforced. You can select a weekly time frame from the drop-down list: Always (7 days), Weekdays (Monday to Friday), Weekends (Saturday and Sunday), and Custom. To create a custom time frame, click on the days.
- **Applicable hours:** Select when the time limit is enforced. You can choose All day or Time range. To define a time range, click in the date picker field, and use the text field or the graphical clock to specify the time.

9 (Optional) Under **Regulation**, configure multiple violations as needed.

This specifies the maximum number of citations that can be issued to the same vehicle for the same overtime offence.

BEST PRACTICE: When configuring multiple violations, the start time of a violation should be greater than or equal to the start time of the previous violation, and the end time of the violation should be less than or equal to the end time of the previous violation.

Violation #1 = 8:00 - 16:00

Violation #2 = 10:00 - 16:00

Violation #3 = 10:00 - 13:00

10 Click **Apply**.

The overtime rule is configured, and is downloaded to Patroller the next time it connects to Security Center.

About permits

A permit is a type of entity that defines a single parking permit holder list. Each permit holder is characterized by a category (permit zone), a license plate number, a license issuing state, and optionally, a permit validity range (effective date and expiry date). Permits are used in both city and university parking enforcement.

The permit entity belongs to a family of methods used by AutoVu™ to identify vehicles of interest, called hit rules. Other types of hit rules include *hotlist*, *overtime*, and *permit restriction*. When a plate read matches a hit rule, it is called a hit. When a read fails to match any permit loaded in the Patroller, it generates a *permit hit*.

Permits in City Parking Enforcement

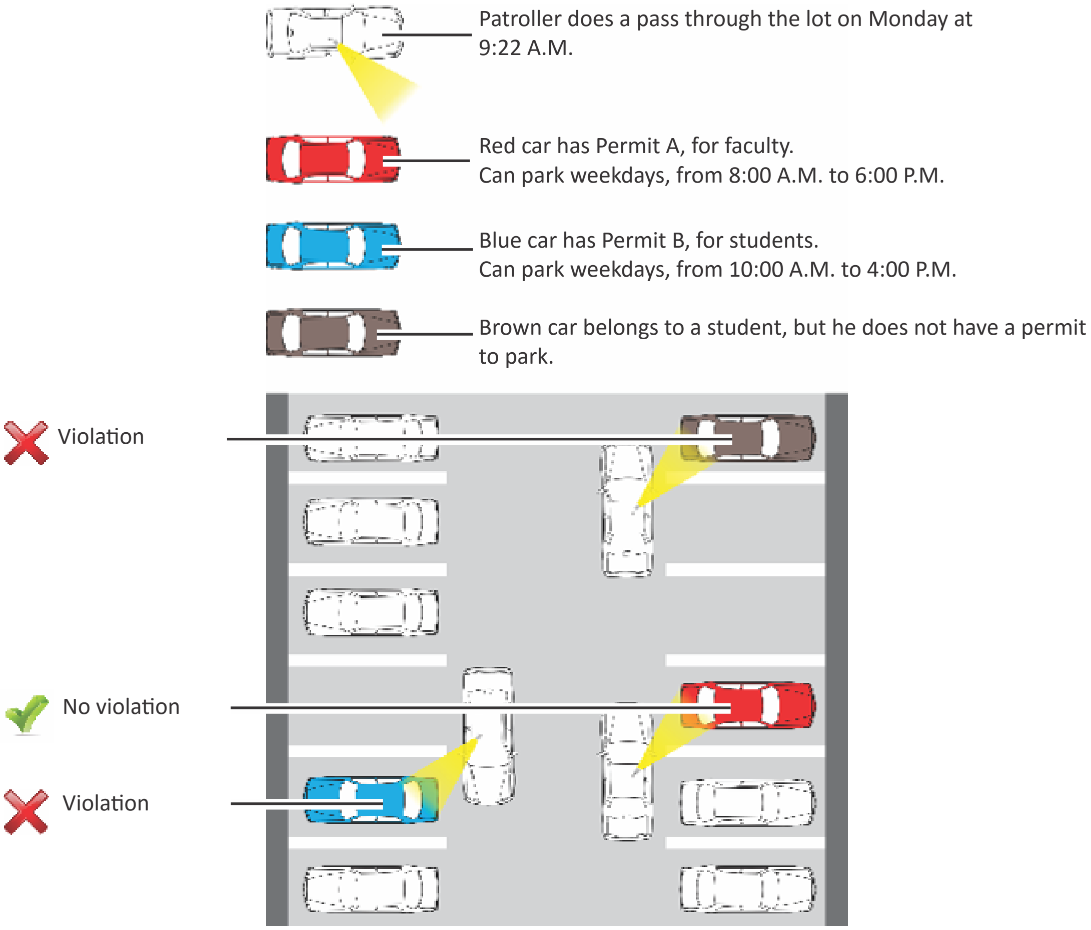
In City Parking Enforcement, you create the permit list and configure its basic properties, but you do not need to define a parking lot or permit restriction. It is the city or municipality that decides when and where the permit is applicable. When you're patrolling, you choose which permit to enforce in Patroller based on where you are in the city (for example, by looking at street signs).

Permits in University Parking Enforcement

In University Parking Enforcement, you create and configure a permit list the same way you would in City Parking Enforcement, but you also need to assign *permit restrictions* and parking lots to create an enforcement "zone" that is downloaded to Patroller. This additional configuration is needed because you're patrolling individual parking lots, not city streets with specific regulations already in place.

Example

In this example, you use a permit restriction to specify different time limits for different permit holders.


Patroller does a pass through the lot on Monday at 9:22 A.M.
Red car has Permit A, for faculty.
Can park weekdays, from 8:00 A.M. to 6:00 P.M.
Blue car has Permit B, for students.
Can park weekdays, from 10:00 A.M. to 4:00 P.M.
Brown car belongs to a student, but he does not have a permit to park.
Violation
No violation
Violation

Shared permits

A permit list includes a field called *Permit ID*, which allows different vehicles to share the same permit by having the same *Permit ID* value in the permit list's source file. For example, a car pool permit could be shared amongst several vehicles (usually up to four). Each member of the car pool takes a turn driving the other members to work or school, therefore each member needs to share the same permit to park.

However, the permit still applies to *one vehicle at a time*. For example, if all four members of the car pool decide to take their own vehicles one day, they can't all use that car pool permit to park at the same time. Patroller will allow one vehicle with the car pool permit to park (the first one it sees), but will raise a *Shared permit* hit for every other vehicle seen with the same permit.

Related Topics

About permit restrictions on page 717

Creating permits

To use permit entities in Security Center, you must create the permit, map it to its source text file, and configure it for your enforcement scenario.

What you should know

If you are using University Parking Enforcement, you must also apply restrictions to permits to create an enforcement rule.

To create a permit:

1. From the home page, click **LPR** > **Permits**, then click **Permit** (+).

   The **Creating a permit** wizard opens.
2. On the **Basic information** page, in the **Entity name** field, type a name for the permit.

   This name appears in Patroller on the permit selection page.

   IMPORTANT: The permit entity name must match the **Category** field from the permit list source file.
3. (Optional) In the **Entity description** field, enter a description for the new permit, and click **Next**.
   This field does not appear in Patroller.
4. Enter the **Path** on the computer where the source file for the permit list is located.

   If you start typing a path to a network drive, the **Username** and **Password** fields appear and you'll need to type the username and password to access the network drive.

   NOTE: The maximum number of entries is 1.8 million when using Patroller in 64-bit mode. Adding more entries causes the system to respond slowly.
5. If the attribute fields in the source text file vary in length, switch the **Use delimiters** option to **ON**, and enter the type of character (delimiter) used to separate each field.

   By default, **Use delimiters** is set to **ON**, and the delimiter specified is a **semi-colon** (;). If your source text file is made up of fixed length fields, set **Use delimiters** to **Off** .Security Center supports the following delimiters:

   - Colon (:)
   - Comma (,)
   - Semi-colon (;)
   - Tab (type "Tab")

   IMPORTANT: If your source list file uses Tab as a delimiter, only use one Tab space. Do not use more than one Tab space to align columns in your file, or Security Center might not be able to parse the permit list.
6. (Optional) Turn off **Visible in editor**, if you don't want users to be allowed to edit this permit in Security Desk.

   NOTE: To edit a permit in Security Desk, users must have the *Hotlist and permit editor* privilege.
7. Configure the permit **Attributes** and click **Next**. See Configuring hotlist and permit attributes on page 664.
8. On the **LPR Manager assignment** page, choose one of the following, then click **Next**.
   - **All LPR Managers**. All LPR Managers and any entities configured to inherit permits from them will synchronize the new permit.

     NOTE: Future LPR Managers will not automatically synchronize the new permit.

- **Specific LPR Managers**. Only the selected LPR Managers and the entities that inherit permits from them will synchronize the new permit.

  NOTE: Entities created in the future that are configured to inherit permits from one of the selected LPR Managers will also synchronize the permit.
- **Assign later**. No existing LPR Managers and associated entities will synchronize the new permit. For more information on how to assign a permit to an LPR Manager, see Selecting which hotlists and permit lists to monitor on page 652.

9 In the **Unit specific assignment** page, select the specific Patrollers and or Sharps that will synchronize the new permit, and click **Next**.

10 (Optional) If you have custom fields in your permit, enter the appropriate values on the **Custom fields** page and click **Next**.

   NOTE: The **Custom fields** page only appears if there are custom fields in your hotlist.

11 In the **Creation summary** window, check to see that your permit information is correct and click **Next**.

12 In the **Entity creation outcome** window, you will receive a notification whether or not your operation is successful.

13 (Optional) Choose one of the following:

- **Edit this permit**. Opens the **Hotlist and permit editor** task so you can edit the permit.

  NOTE: To edit a permit, you must have the *Hotlist and permit editor* privilege.
- **Create a permit based on this permit:** Create a new permit that uses the same settings as the permit you just created. You only need to specify the **Entity name**, **Entity description**, and **Permit path**.

14 Click **Close**.

The permit entity is configured and enabled in Security Center.

Configuring permits

You can modify your permit configuration settings after a permit entity has been added to Security Center.

Before you begin

Create the permit.

What you should know

The source text file must be located on the LPR Manager computer's local drive (for example, the C drive), or on a network drive that is accessible from the computer hosting the LPR Manager

To configure a permit:

1. From the home page, click **LPR** > **Permits**, and select the permit you want to configure.
2. In the **Identity** tab, enter a **Description** for the permit, and click **Apply**.

   You can add a longer description for the permit. This field does not appear in Patroller.
3. Click the **Properties** tab.
4. Enter the **Path** on the computer where the permit list's source text file is located.

   If you start typing a path to a network drive, the **Username** and **Password** fields appear and you'll need to type the username and password to access the network drive.
5. If the attribute fields in the source text file vary in length, switch the **Use delimiters** option to **ON**, and enter the type of character (delimiter) used to separate each field.

   By default, **Use delimiters** is set to **ON**, and the delimiter specified is a **semi-colon** (;). If your source text file is made up of fixed length fields, set **Use delimiters** to **Off** .Security Center supports the following delimiters:

   - Colon (:)
   - Comma (,)
   - Semi-colon (;)
   - Tab (type "Tab")

   IMPORTANT: If your source list file uses Tab as a delimiter, only use one Tab space. Do not use more than one Tab space to align columns in your file, or Security Center might not be able to parse the permit list.
6. Decide whether users are allowed to edit this permit in Security Desk.
7. Configure the **Attributes** for the permit list's text file so that Patroller can parse the information in the list.
8. Click **Apply**.

About permit restrictions

A permit restriction is a type of entity that applies time restrictions to a series of parking permits for a given parking zone. Permit restrictions are only used by AutoVu™ Patrollers configured for University Parking Enforcement.

Different time restrictions can be applied to different *permits*. For example, a permit restriction may limit the parking in zone A from Monday to Wednesday for permit P1 holders, and from Thursday to Sunday for permit P2 holders.

The permit restriction entity is a type of hit rule. A hit rule is a method used by AutoVu™ to identify vehicles of interest. Other types of hit rules include *hotlist, overtime*, and *permit*. When a plate read matches a hit rule, it is called a hit. When a plate read matches a permit restriction, it generates a permit hit. Additionally, a shared *permit hit* occurs when two plates sharing the same permit ID are read in the same parking zone within a specific time period.

Related Topics

About permits on page 712

Creating permit restrictions

You can add a permit restriction entity in Security Center Config Tool to apply restrictions to a permit. After you create the entity, you'll configure its settings for your enforcement scenario.

Before you begin

Create the permit and configure the permit.

What you should know

In University Parking Enforcement, you need to apply restrictions to the permits you add, to create an enforcement rule. Patroller downloads permit restrictions when it connects to Security Center.

To create a permit restriction:

1. From the home page, click **LPR** > **Permits restrictions**, and then click **Permit restriction** (➕).

   A new permit restriction entity is added in the list of all the permit restrictions on your system.
2. In the **Identity** tab, enter the required information:
   - **Name:** In City Parking Enforcement, this name appears in Patroller on the overtime rule selection page. In University Parking Enforcement, this name appears appended to the parking lot name on the zone selection page.

     TIP: Choose a name that describes the details of the enforcement scenario. This makes it easier to select it in Patroller when you have more than one available.
   - **(Optional) Description:** You can add a longer description for the rule. This field does not appear in Patroller.
   - **(Optional) Logical ID:** Enter a Logical ID if applicable.
3. Click **Apply**.

After you finish

Configure the permit restrictions.

Configuring permit restrictions

After you have created a permit restriction entity in Security Center Config Tool, you need to configure it for your enforcement scenario.

Before you begin

Create the permit restriction.

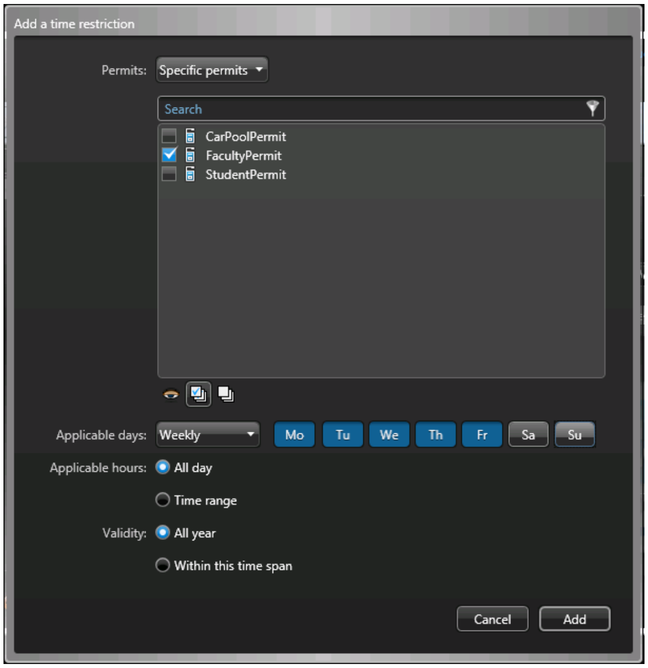
To configure a permit restriction:

1. From the home page, click **LPR** > **Permit restrictions**.
2. Select the permit restriction you want to configure, then click the **Properties** tab.
3. To assign a color to the permit restriction, click the **Color** icon, select a color, and click **OK**.

   The color is displayed in the permit hit screen in Patroller and Security Desk, as well as the plate reads due for enforcement on the Patroller map.

4. To select when this restriction applies, click **Add an item** (➕).

   The **Add a time restriction** window opens.



Add a time restriction

Permits: Specific permits

Search

□ CarPoolPermit
☑ FacultyPermit
□ StudentPermit

Applicable days: Weekly — Mo Tu We Th Fr Sa Su

Applicable hours: ● All day ○ Time range

Validity: ● All year ○ Within this time span

Cancel | Add

5. From **Permits** drop-down list, select which permits the restriction applies to:
   - **Everyone:** Parking is available to everyone, regardless of whether they have a permit or not. No restriction is enforced during the specified time period. This restriction is used with other restrictions as a temporary override. For example, if a university is hosting a football game, parking would be made available to everyone during the game instead of specific permit holders.
   - **No permit:** Only vehicles without permits can park. For example, you can use this type of restriction to reserve a zone for visitors parking. A plate read that matches any of the permits downloaded to the Patroller raises a hit.
   - **All permits:** Only vehicles with a permit can park. A plate read that does not match any of the permits downloaded to the Patroller raises a hit.
   - **Specific permits:** Only vehicles having one or more of the specified permits can park. A plate read that does not match any of the specified permits raises a hit.

When multiple time restrictions apply at a given time, conflicts are resolved by evaluating the restrictions in the following order: 1. *Everyone*, 2. *No permit*, 3. *All permits*, 4. *Specific permits*. Moreover, a hit is raised when a matched permit is not valid (either not yet effective or already expired).

6 In the **Applicable days** option, select the days of week when parking is allowed.
   - **Always:** Seven days a week.
   - **Weekly:** Monday to Friday.
   - **Weekend:** Saturday and Sunday.
   - **Custom:** Select the days that apply.

7 In the **Applicable hours** option, select the times during the day when parking is allowed.

8 In the **Validity** option, select the dates during the year when parking is allowed.

   Choose **All year**, or select a specific time span using the date picker.

   NOTE: The date span must be longer than one day.

9 Click **OK**.

The permit restriction entity is configured and enabled in Security Center.

After you finish

Configure a parking lot in Security Center for the permit restriction.

Configuring parking lots in Security Center

You must configure an enforcement area (or parking lot) for each enforcement rule (permit, permit restriction, or overtime rule) that you create.

What you should know

- Once you have a parking rule and a parking lot defined, this makes up the *parking zone* that is displayed in Patroller. You create parking lots in Security Center Config Tool by drawing a polygon around the parking lot's geographical location on the map. You can add multiple parking lots to a map.
- You can also import KML files to your map that have been created in another map application such as Google Earth. For more information, see Importing KML files in Security Center on page 723.

To configure a parking lot in Security Center:

1. From the home page, click **LPR** > **Permits**, **Permit restrictions**, or **Overtime rules**.
2. Select the permit, permit restriction, or overtime rule you want to configure, then click **Parking lot**.

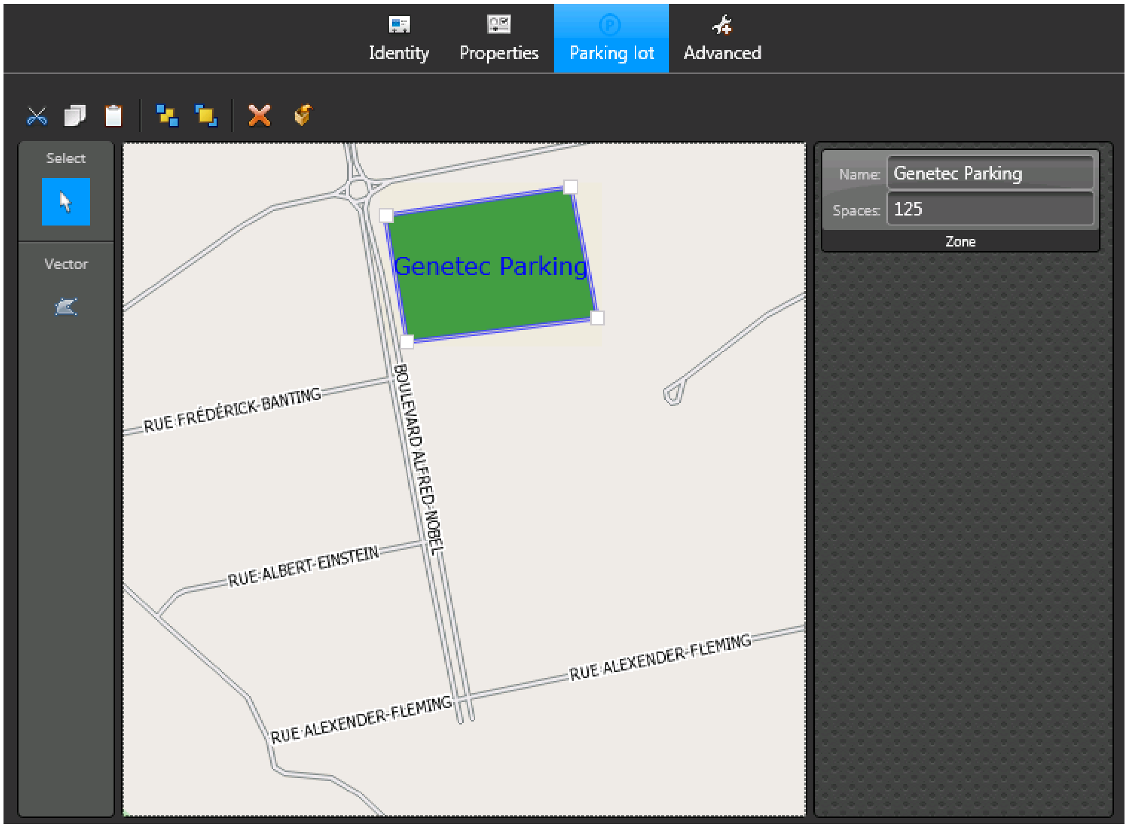
   The map appears.
3. Zoom in to the area of the map where your parking lot is located.
4. Click the **Vector** button, and place the cursor on the map.

   The cursor changes to crosshairs.
5. On the map, click to create the first corner of the polygon, then move the crosshairs to the next corner.
6. Click again to mark the second corner of the polygon. Continue this process until you return to the initial position, then click on the starting corner to close the polygon.

   A parking lot will appear with the name **New zone 1**.
7. Click on the **New zone 1** parking lot, and in the dialog that appears enter a new **Name** and the number of **Spaces** in the parking lot.

   This name will appear in Patroller along with the *Permit*, *Overtime rule* or *Parking restriction* name, to display an enforcement zone.

   TIP: Choose a name that describes where the parking lot is. This makes it easier to select the parking zone in Patroller when multiple zones are available.



Name: Genetec Parking
Spaces: 125

8 Click **Apply**.

The parking lot appears as a filled polygon with a thick blue border on the map. The name of the parking lot is written in the center.

9 (Optional) To resize a parking lot, select it in the map and use the handles to drag it to the desired size.

TIP: To select a parking lot, you can click directly on the parking lot, or click the Select button and then select the lot.

10 (Optional) To edit a parking lot, select the lot and use the buttons located at the top left of the map:

- **Cut** ✂: Cut the selected parking lot from the current entity and paste it into another. For example, you may want to cut the parking lot from a permit entity and paste it into the map when creating a parking lot for an overtime rule.
- **Copy** ❐: Copy the selected parking lot from the current entity and paste it into another. For example, you may want to use the same parking lot dimensions that were created for a permit parking lot in an overtime rule parking lot.
- **Paste** 📋: Paste the selected parking lot into another entity.
- **Send to Back** ⧉: Send the selected parking lot to the background.
- **Bring to Front** ⧉: Send the selected parking lot to the background.
- **Remove** ✕: Delete the parking lot.

Importing KML files in Security Center

The **Parking lot** tab in Config Tool enables you to import Keyhole Markup Language (KML) files so you can easily create parking lots in Security Center.

Before you begin

Create a KML file for your map. This can be done using Google Earth.

What you should know

- If the KML file you want to import is not supported or not valid, you will receive an error message.
- If you want update a KML lot in Security Center by reimporting an updated KML file, delete the original KML lot first so you don't get a duplicate.

To import a KML file:

1. From the home page, click **LPR** > **Permits**, **Permit restrictions**, or **Overtime rules**.
2. Select the permit, permit restriction, or overtime rule you want to configure, then click **Parking lot**.

   The map appears.
3. Click **Import KML** (📦) and navigate to the folder that contains your KML file.
4. Select the KML file and click **Open**.

   The parking lot appears in your map as a filled polygon with a thick blue border on the map. The name of the parking lot is written in the center.
5. Select the parking lot in the map. In the dialog box that appears, enter the number of **Spaces** the parking lot contains.
6. Click **Apply**.

Configuring advanced permit settings

The **Advanced** tab is where you configure the advanced properties of the permit such as the color and download frequency. These properties are not required for all permits, but allow you to customize certain permits for specific scenarios.

Before you begin

Create the permit.

To configure advanced permit settings:

1. From the home page, click **LPR** > **Permits**, and select the permit you want to configure.
2. Click the **Advanced** tab.
3. Beside **Color**, click the colored block and use the **Select color** dialog box to assign a new color to the permit.

   The map symbol that marks the location of the permit hit in Security Desk and Patroller will appear in that color, as well as the Permit Hit and Review Hits screen in Patroller.
4. Turn on **Disable periodic transfer** if you only want permit changes to be downloaded to Patroller when the user logs on to the application. This option requires a wireless connection between Patroller and Security Center.

   Turn on **Enable transfer modification** if you want to transfer permit modifications to Patroller as soon as they occur. For example, you can use this option on a permit to force Patroller to query for changes more frequently than the periodic transfer period (which applies to all permits). This option requires a continuous wireless connection between Patroller and Security Center.

43

AutoVu™ Mobile License Plate Inventory systems

This section includes the following topics:

Mobile License Plate Inventory

Mobile License Plate Inventory is the Patroller software installation that is configured for collecting license plates and other vehicle information for creating and maintaining a license plate inventory for a large parking area or parking garage.

The inventory can be used to report the following:

- The number of days a vehicle has been parked in the facility.
- The location (sector and row) of the vehicle in the facility.
- All vehicles parked in the facility.
- All vehicles that have left or entered the facility.

License plate reads can be collected in three ways:

- Automatic reading using the Patroller application and a Sharp camera (or cameras).
- Manual entry using the *Manual capture* feature of the Patroller application.
- (Optional) Manual capture using the handheld computer approved by Genetec Inc. that is running the Patroller MLPI application.

License plate inventory

The license plate inventory includes license plate reads of all vehicles parked in the parking facility. It is created from the license plate collection offload data of the patroller application and the handheld computer approved by Genetec Inc. (if applicable). The inventory can be used to monitor vehicle activity of the parking facility for a specific time period. For example, a patroller may collect license plate reads early in the morning and then do another collection in the evening to see how many vehicles have left the facility. The Security Desk *Inventory management* task is used to create the inventory from the offload data, and the Security Desk *Inventory Report* task is used to query any changes to an inventory.

For more information, see the *Inventory management* and *Inventory report* topics in the *Security Desk User Guide*.

How reads are reconciled

Most reads from the offload data of a license plate collection are automatically reconciled (validated and added) to the license plate inventory by Security Center. However, some of them may require manual reconciliation if a conflict is detected. For example, a vehicle may have the same license plate numbers as another vehicle, but be from a different state. If this is the case, the Security Desk *Inventory Management* task will display a dialog box asking you to reconcile the read (confirm the plate number and state of the vehicle).

For more information on the *Inventory Management* task, see the *Security Desk User Guide*.

About parking facilities

A parking facility is a type of entity that defines a large parking area as a number of sectors and rows for the purpose of inventory tracking.. It is used in the AutoVu™ *Mobile License Plate Inventory* (MLPI) application.

The license plate inventory is the list of vehicles present in a parking facility within a given time period.

Before AutoVu™ MLPI units (mobile Patrollers and handheld devices) can collect license plates for the inventory, you must define their collection route as a sequence of sectors and rows configured in the parking facility. The sector and row where a license plate is read represents the location of the vehicle inside the parking facility.

Security Center collects *license plate reads* from the MLPI units and creates an inventory for the current date. Using Security Desk, you can find where a vehicle is parked (sector and row) and how long it has been parked there in the current inventory. You can also compare two inventories on different dates to view the vehicle movements (vehicles that were arrived, moved, or left).

Creating parking facilities

To track the location of vehicles in an AutoVu™ Mobile License Plate Inventory system, you must create a parking facility.

To create a parking facility:

1 From the home page, click **LPR** > **Parking facilities**, then click **Parking facility** (➕).

2 In the **Identity** tab, enter the required information:

- **Name:** In Mobile License Plate Inventory, this name will appear in Patroller on the parking zone selection page.
- **(Optional) Description:** You can add a longer description for the rule. This field does not appear in Patroller.
- **(Optional) Logical ID:** Enter a Logical ID if applicable.

3 Click **Apply**.

The parking facility appears in a flat list view that displays all the facilities on your system.

After you finish

Define the parking facility for your parking scneario by creating sectors and rows.

Configuring parking facilities

After you have created a parking facility in Security Center, you must define the facility for your parking scenario by creating sectors and rows for the license plate collection route.

Before you begin

Create the parking facility.

What you should know

The parking space of a parking facility is divided into sectors (or levels in the case of a parking garage) for ease of reference. Each sector contains x number of rows, and each row contains x number of spaces. You can configure Patroller to trigger an alarm (sound or warning message) if the reads collected during your sweep of a row exceed the space count for that row.

The *route* is the license plate collection route followed by the MLPI units responsible for collecting the plates for the inventory. The route is downloaded by the Patrollers and handheld devices assigned to this parking facility.

NOTE: Only one route may be defined per parking facility, but each MLPI device can start its sweeping round at a different point in the route. The route forms a closed circuit.

To configure a parking facility:

1 From the home page, click **LPR** > **Parking facilities**, and select the facility you want to configure.

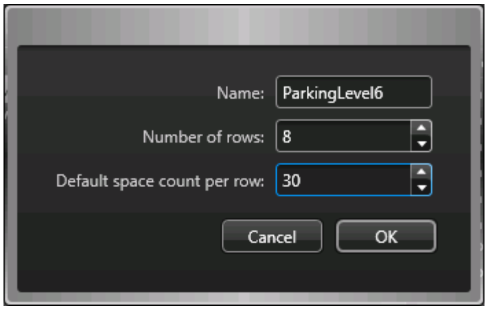
2 Click the **Properties** tab.

3 From the **LPR Manager** drop-down list, select the LPR Manager that will create and manage the license plate inventory for the selected parking facility.

Only offloads from MLPI Patrollers managed by the same LPR Manager are used to build the inventory for this parking facility. An MLPI Patroller offload can include the vehicle inventory for multiple parking facilities, but only the reads tagged for this parking facility are used to build the inventory.

4 Under **Configuration**, click **Create** (+) to add a new sector.

The parking space of a parking facility is divided into sectors (or levels in the case of a parking garage) for ease of reference. Each sector contains x number of rows.



Name: ParkingLevel6

Number of rows: 8

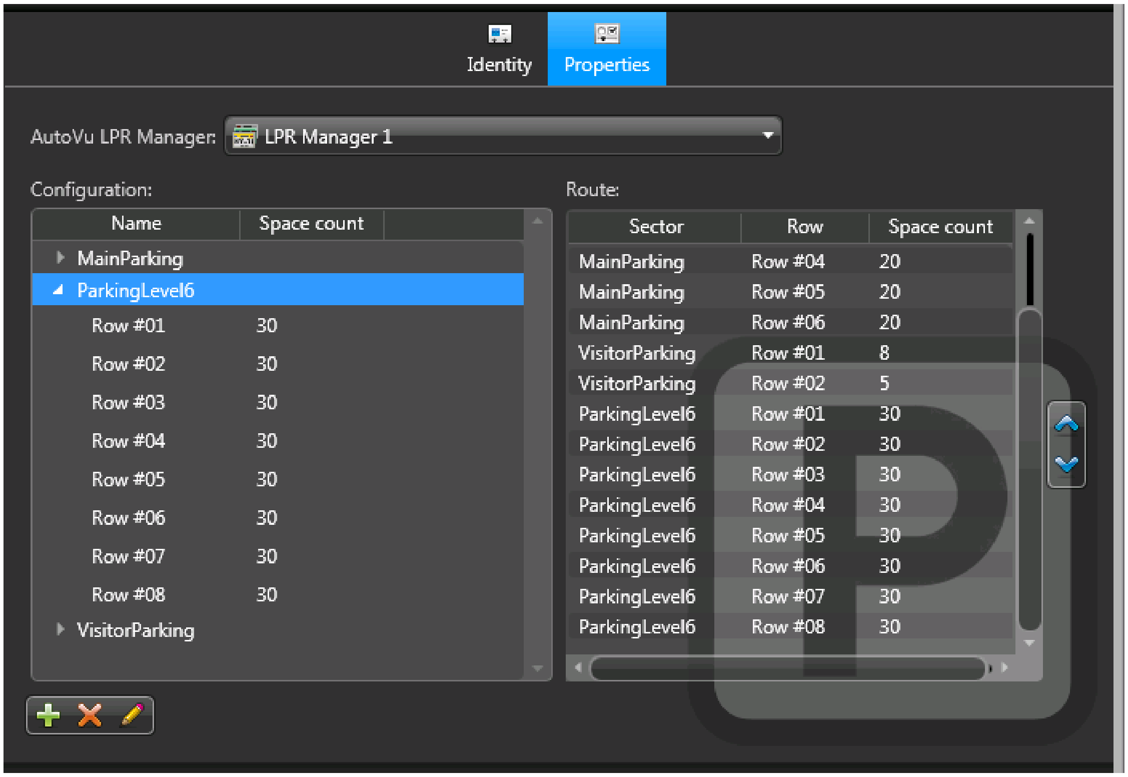
Default space count per row: 30

5 Enter the **Name** of the sector (or level if you have a parking garage).

6 Enter the **Number of rows** in the sector.

7 Click **OK**.

The sector you created appears under the **Configuration** and **Route** sections.



AutoVu LPR Manager: LPR Manager 1

Configuration:

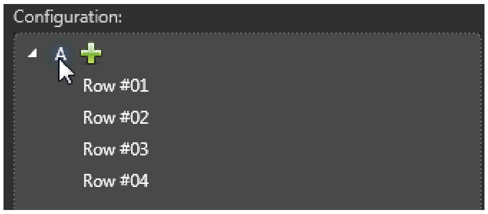
Name	Space count
▸ MainParking	
◢ ParkingLevel6	
Row #01	30
Row #02	30
Row #03	30
Row #04	30
Row #05	30
Row #06	30
Row #07	30
Row #08	30
▸ VisitorParking	

Route:

Sector	Row	Space count
MainParking	Row #04	20
MainParking	Row #05	20
MainParking	Row #06	20
VisitorParking	Row #01	8
VisitorParking	Row #02	5
ParkingLevel6	Row #01	30
ParkingLevel6	Row #02	30
ParkingLevel6	Row #03	30
ParkingLevel6	Row #04	30
ParkingLevel6	Row #05	30
ParkingLevel6	Row #06	30
ParkingLevel6	Row #07	30
ParkingLevel6	Row #08	30

8 To add rows to a sector, do the following:

a) Under **Configuration**, mouseover the sector name, and then click the **Create** (✚).



Configuration:

◢ A ✚
Row #01
Row #02
Row #03
Row #04

b) Enter the **Number of rows** to add, and then click **OK** > **Apply**.

9 (Optional) To rename a sector, do the following:

a) Under **Configuration**, click the sector name you want to rename, and then click **Edit** (✎).

b) Enter the new name, and then click **OK** > **Apply**.

10 (Optional) To delete a sector, click the sector name you want to delete under **Configuration**, and then click the **Delete** (✖) > **Apply**.

11 To change the order of sectors and rows in the route, click the up (▲)and down (▼) arrows under **Route**.

After you finish

You must set the *Read retention period* of the LPR Manager according to the period of time you want to keep your license plate inventories in the database. The default retention period is 90 days.

44

Troubleshooting LPR

This section includes the following topics:

Moving Patroller or LPR units to a different LPR Manager

If you want a different LPR Manager role to manage and control an LPR or Patroller unit, for load balancing or another purpose, you can move the unit to another LPR Manager using the *Move unit* tool. After the unit is moved, the old LPR Manager continues to manage the unit data collected before the move.

What you should know

After you move a unit in Config Tool, you need to update the unit's network settings in Patroller Config Tool and in the Sharp Portal so that the unit can communicate with its new LPR Manager. Specific unit settings (for example, unit name, logical ID, and so on) are automatically carried over to the new LPR Manager.

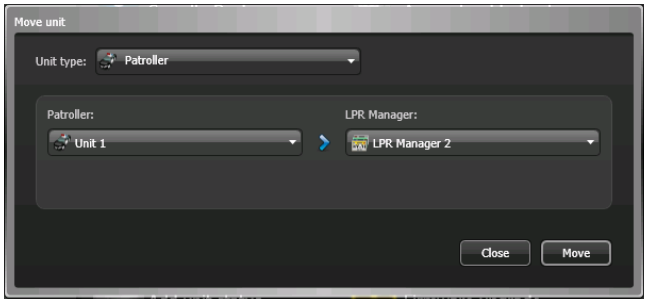
For example, if you move a Patroller unit from *LPR Manager* to *LPR Manager 2*, you must configure the Patroller unit to communicate with *LPR Manager 2* the same way you did when you originally added the unit to *LPR Manager*. This requires changing network settings in Patroller Config Tool so that they match the network settings for *LPR Manager 2* in Security Center Config Tool.

To move an LPR or Patroller unit to a different LPR Manager:

1 From the home page, click **Tools** > **Move unit**.

2 From the **Unit type** drop-down list in the **Move unit** dialog box, select the Patroller or LPR unit you want to move.

A Patroller unit is shown as an example.



3 Select the unit you want to move.

4 From the **LPR Manager** drop-down list, select the new LPR Manager to control the unit.

5 Click **Move** > **Close**.

The unit is now added to the new LPR Manager

After you finish

Make sure the unit can communicate with the new LPR Manager, as follows:

- For hotlists, permit lists, and Patroller user groups, do the following:
  1 From the home page, click **System** > **Roles**, and then select the LPR Manager that is now controlling the unit you moved.
  2 Click **Properties** > **File association**.
  3 Activate the hotlists and permit lists, and assign a Patroller user group for this LPR Manager.
- Update the network settings of Patroller units to communicate with the new LPR Manager (see the *Patroller Administrator Guide*).
- Update the network settings of LPR units to communicate with the new LPR Manager. For more information, see the *Sharp Administrator Guide*.

Part VII

Alarms and critical events

This part includes the following chapters:

- "Alarms" on page 734
- "Threat levels" on page 745
- "Zones and intrusion detection" on page 755

45

Alarms

This section includes the following topics:

About alarms

An alarm is a type of entity that describes a particular trouble situation that requires immediate attention and how it can be handled in Security Center. For example, an alarm can indicate which entities (usually cameras and doors) best describe it, who must be notified, how it must be displayed to the user, and so on.

The basic properties of an alarm are:

- **Name:** Alarm name.
- **Priority:** Priority of the alarm (1-255), based on the urgency of the situation. Higher priority alarms are displayed first in Security Desk.
- **Recipients:** Users, user groups, and analog monitor groups who are notified when the alarm occurs, and are responsible for responding to the alarm situation.
- **Broadcast mode:** How the alarm recipients are notified about the alarm.
  - **All at once:** (Default) All recipients are notified at the same time, immediately after the alarm is triggered.
  - **Sequential:** The recipients are notified individually, each after a specified delay (in seconds) calculated from the time the alarm is triggered. If the recipient is a user group, all members of the user group are notified at the same time.
- **Attached entities:** Entities that help describe the alarm situation (for example, cameras, area, doors, alarm procedure, and so on). When the alarm is received in Security Desk, the attached entities can be displayed one after another in a sequence or all at once in the *canvas*, to help you review the situation. If a composite entity is attached to the alarm, the entities that compose it are also attached to the alarm. For example, of a door entity is attached to the alarm, the cameras associated to the door are also attached to the alarm.

For information about monitoring, acknowledging, and investigating alarms in Security Desk, see the *Security Desk User Guide*.

Alarm priority

In Security Desk, alarms are displayed in the *Alarm monitoring* task and the *Monitoring* task by order of priority (this is evaluated every time a new alarm is received). The highest priority alarm is displayed in tile #1, followed by the second highest in tile #2, and so on. When two alarms have the same priority value, priority is given to the newest one.

When a new alarm is received in Security Desk with a priority level identical or higher than the current alarms displayed, it pushes the other alarms down the tile list.

When an alarm is *acknowledged* in Security Desk, it frees a tile for lower priority alarms to move up.

Video recording on alarms

When an alarm is triggered that has cameras attached to it, you can make sure that the video related to the alarm is recorded and available for future alarm investigations.

The amount of time that the video is recorded for (called the *guaranteed recording span*) is defined by two settings:

- **The alarm recording duration:** Number of seconds that the Archiver records video for after the alarm is triggered. This option (*Automatic video recording*) is set in the alarm *Advanced* tab.
- **The recording buffer:** Number of seconds that the Archiver records video for before the alarm was triggered, to make sure that whatever triggered the alarm is also recorded. This option (*Time to record before an event*) is set in the Archiver *Camera default settings* tab, or for each camera individually.

If an alarm is triggered from a camera event (for example *Object removed*), then the camera that caused the event is also attached to the alarm and starts recording.

IMPORTANT: The recordings are dependent on the archiving schedules. If recording is disabled when the alarm is triggered, no video is recorded.

Related Topics

Archiver: Camera default settings tab on page 857
Differences between threat levels and alarms on page 747

Creating alarms

For alarms to be triggered in your system, you must create an alarm entity and set up its properties.

What you should know

As a best practice, give names to alarms that best describe the situation, so it is easy to determine what happened when the alarm is triggered.

To create an alarm:

1. From the Config Tool home page, open the *Alarms* task, and click the **Alarms** view.
2. Click **Alarm** (✚).

   A new alarm entity (●) appears in the **Alarms** view.
3. Type a name for the alarm, and press **ENTER**.
4. Click the **Properties** tab.
5. In the **Priority** option, set the priority of the alarm, based on the urgency of the situation.

   Higher priority alarms are displayed first in Security Desk.
6. To add recipients for the alarm, click **Add an item** (✚) under the **Recipients** section, select the users, user groups, or analog monitor groups, and click **Add**.

   Recipients are notified when the alarm occurs, and are responsible for responding to the alarm.
7. If you chose more than one recipient, select how they are notified about the alarm from the **Broadcast mode** option:
   - **All at once:** All recipients are notified at the same time, immediately after the alarm is triggered.
   - **Sequential:** The recipients are notified individually, each after a specified delay (in seconds) calculated from the time the alarm is triggered. If the recipient is a user group, all members of the user group are notified at the same time.
8. To add entities to help describe the alarm, click **Add an item** (✚) under the **Attached entities** section, select the entities, and click **Select**.

   Attached entities help users react to the alarm situation. When the alarm is received in Security Desk, the attached entities (cameras, doors, areas, alarm procedure, and so on), are displayed in the canvas in the Alarm monitoring task.
9. From the **Video display option** drop-down list, select the video display options when the alarm is triggered.
10. To automatically rotate the attached entities inside a tile in the *Alarm monitoring* task when the alarm is triggered, switch the **Content cycling** option to **ON**, and set the number of seconds each entity is displayed for.

    NOTE:

    The order of the entities in the list is the order they are displayed in Security Desk. When the alarm is triggered by an event, the entity that caused the event is also attached to the alarm, and is displayed first.
11. Click **Apply**.
12. Click the **Advanced** tab, and configure the optional alarm settings.

After you finish

Do the following:

- Make sure the alarm recipients have the *Acknowledge alarms* and *Alarm monitoring* user privileges.

- Test the alarm you just created.

Selecting video display options for alarms

If a camera is attached to an alarm, you must configure how the video is shown when the alarm is triggered and displayed in the canvas of the Alarm monitoring task.

What you should know

The default video display option is live video. You can select live video, playback video, a series of still frames before, during, or after the alarm is triggered, or a combination of the three. The video or still frames are displayed for the number of seconds set in the **Content cycling** option in the alarm **Properties** tab.

The options you set are applied to all cameras that are attached to the alarm.

To select the video display options for an alarm:

1. Open the **Alarms** task, and click the **Alarms** view.
2. Select the alarm to configure, and click the **Properties** tab.
3. From the **Video display option** drop-down list, select one of the following:
    - **Live:** Display live video.
    - **Playback:** Display playback video.
    - **Live and playback:** Cycle between displaying live and playback video. When you unpack the tile, one tile displays live video and the other displays playback. You can also click the **Properties** icon (⚙) and configure **Picture-in-picture** so you can view the live and playback video in the same tile.
    - **Live and still frames:** Cycle between displaying live video and a series of still frames. When you unpack the tile, one tile displays live video and the other displays still frames. You can also click the **Properties** icon (⚙) and configure **Picture-in-picture** so you can view the live and still frames video in the same tile.

      NOTE: Still frames are not supported when the camera is encrypted.
    - **Still frames:** Display a series of still frames. See previous note.
4. If you select a display option that includes playback video, then select how many seconds before the alarm was triggered to start the playback.

   NOTE: To ensure that playback video is available for the length of time you set, the recording buffer for events must be an equal or larger value.
5. If you select a display option that includes still frames, click the **Properties** icon (⚙).
6. In the **Still frames** dialog box, select whether you want each still frame to be displayed for the same duration or an independent duration of time (**Same durations** or **Independent durations**).
7. If you select **Same durations**, then set the following options:
    - **Number of frames:** Select the number of still frames to display within total content cycling duration.
    - **Play:** Select how many seconds before the alarm was triggered to start the first still frame.
8. If you select **Independent durations**, do the following:

   a) Click **Add an item** (✚).

   b) In the **Relative time** option, select how many seconds before or after the alarm was triggered the still frame displays.

   c) In the **Duration** option, select how long the still frame is displayed for.

   d) Click **Add**.

   e) Add additional still frames.

   The duration of all the still frames cannot exceed the **Total duration** value.

9 If you select the **Live and Playback** or **Live and still frames** option, you can configure picture-in-picture to display both live and playback video or live and still frame video in the same tile.
   a) Click the **Properties** icon (⚙).
   b) In the **Video display configuration** dialog box, from the **Picture-in-picture** list, choose what type of video you would like to be displayed in the inset window.
   c) From the **Displayed at** list, select where you would like the inset window to be displayed.

10 Click **OK** > **Apply**.

Setting optional alarm properties

After you create an alarm and configure its basic properties, there are additional properties you can set.

To set optional properties for an alarm:

1 Open the **Alarms** task, and click the **Alarms** view.

2 Select the alarm to configure, and click the **Advanced** tab.

3 Set the following options:

- **Reactivation threshold:** The minimum time Security Center needs to wait after triggering this alarm once, before it can be triggered again. This option prevents the system from repeatedly triggering the same alarm before it is resolved.
- **Alarm procedure (URL):** Set a URL or the web page address corresponding to the *alarm procedure*, which provides alarm handling instructions to the operators. The web page is displayed when the user clicks *Show alarm procedure* (☰) in the alarm widget in Security Desk.
- **Schedule:** Define when this alarm is in operation. Outside the periods defined by this schedule, triggering this alarm has no effect.

  NOTE: You can add multiple schedules to the alarm. Schedule conflicts that cannot be resolved will be notified.
- **Automatic acknowledgment:** Turn this option on to let the system automatically acknowledge this alarm if no one acknowledges it before the specified time (in seconds). This option is recommended for low-priority alarms that serve to alert the security operator, but do not require any action. When this option is turned off, the system follows the **Auto ack alarms after** option configured at the system level in Server Admin.

  NOTE: Automatic acknowledgement does not apply to alarms that have an active condition attached. To acknowledge those alarms, you need to be logged on as an administrator and *forcibly acknowledge* them. For more information on acknowledging alarms, see the *Security Desk User Guide*.
- **Create an incident on acknowledgement:** Turn this option on to prompt the Security Desk user to report an *incident* every time they acknowledge an alarm.

  NOTE: Turning this option on turns the *automatic acknowledgement* option off.
- **Automatic video recording:** Turn this option off if you do not want to start recording video when the alarm is triggered.
- **Protect recorded video:** Turn this option on to protect the video recordings associated to this alarm for the specified number of days.

4 Click **Apply**.

Related Topics

Archiver: Camera default settings tab on page 857
Protecting video files from being deleted on page 451
Server Admin - Main server page on page 86

Testing alarms

To test if an alarm that you just created works, you can trigger it manually from Config Tool, and make sure that you receive it in Security Desk.

Before you begin

Log on to Security Desk as one of the alarm recipients.

What you should know

You can configure the *Alarm monitoring* task in Security Desk to open automatically when an alarm is triggered. For information about customizing alarm behavior, see the *Security Desk User Guide*.

To test an alarm:

1. In Config Tool, open the **Alarms** task.
2. Click the **Alarms** view, and select the alarm to test.
3. In the toolbar at the bottom of the workspace, click **Trigger alarm** (●).

   The alarm should appear in the Security Desk notification tray, and in the alarm list in the Alarm monitoring task.
4. If the Alarm monitoring task does not open automatically, double-click the alarm icon (●) in the Security Desk notification tray.
5. In the Alarm monitoring task, make sure the alarm appears in the alarm list.

After you finish

If you did not receive the alarm, then you can troubleshoot the alarm.

Troubleshooting: Alarms not received

If you do not receive an alarm in Security Desk, you can troubleshoot the cause of the issue.

To troubleshoot why an alarm is not received:

1. Make sure the user who is trying to receive the alarm is a recipient of the alarm, as follows:
   a) Open the **Alarms** task, and click the **Alarms** view.
   b) Select the alarm, and click the **Properties** tab.
   c) Make sure the user, or the user group they are a member of, is in the **Recipients** list.
2. Make sure the alarm schedule is not preventing you from triggering the alarm at this moment, as follows:
   a) Click the alarm's **Advanced** tab.
   b) Make sure the schedule listed in the **Schedule** drop-down list applies at this time.
3. Make sure the alarm recipient has the correct user privileges to receive alarms, as follows:
   a) From the Config Tool home page, open the *User management* task.
   b) Select the user to configure, and click the **Privileges** tab.
   c) Make sure the *Alarm monitoring* and *Acknowledge alarms* user privileges are set to **Allow**.
   d) Click **Apply**.

Setting up alarms using event-to-actions

You can configure alarms so that they are triggered when an event occurs, using event-to-actions.

To set up an alarm using an event-to-action:

1 Open the **System** task, and click the **General settings** view.

2 Click the **Actions** tab, and click ➕.

3 In the **Entity type** page, select an entity type, and click **Next**.

The *source entity* is the entity that the event is attached to.

4 In the **Source** page, select the source entity and click **Next**.

5 In the **Event** page, select an event type.

Only events related to the selected entity type are listed.

6 Select a schedule, and click **Next**.

The schedule determines when the event will trigger the action. For example, you might want to trigger an alarm only if a window is opened during the weekend. By default, *Always* is selected.

7 In the **Action** page, select **Trigger alarm**.

8 From the **Alarm** drop-down list, select an alarm to trigger.

9 (Optional) From the **Acknowledgement condition** drop-down list, select an event that must be triggered before the alarm can be acknowledged.

This option is only available for some event types.

10 To require a user to acknowledge the alarm after the acknowledgement condition is cleared, select the **User acknowledgement required** option.

If you clear this option, the alarm is automatically acknowledged when the acknowledgement condition is cleared.

11 Click **Next** > **Create** > **Close**.

Related Topics

Event types on page 908

Creating event-to-actions on page 177

Event types that can require acknowledgement conditions

Some event-to-actions can be configured so that a second event must be triggered before the alarm that was triggered can be acknowledged. The second event is the *acknowledgement condition*.

For example, you can configure a *Signal lost* event to trigger an alarm, and specify that the alarm can only be acknowledged after the *Signal recovered* event is generated.

The following table lists the event types that allow you to select an acknowledgement condition that must be cleared before the alarm can be acknowledged.

Source event type	Entity type	Acknowledgement condition
AC fail	Access control unit, Intrusion detection unit	AC fail input normal
Application lost	Roles	Application online

Source event type	Entity type	Acknowledgement condition
Asset offline	Asset	Asset online
Asset online	Asset	Asset offline
Battery fail	Access control unit, Intrusion detection unit	Battery fail input normal
Door forced open	Door	Door closed
Door opened	Door	Door closed
Door open too long	Door	Door closed
Hardware tamper	Access control unit, Intrusion detection unit, Zone (hardware)	Input normal
Intrusion detection area alarm activated	Intrusion detection area	• Disarmed (not ready) • Disarmed (ready to arm) • Master armed • Perimeter armed
Intrusion detection area input bypass activated	Intrusion detection area	Input bypass deactivated
Manual station activated	Door	Manual station reverted to normal state
Signal lost	Camera	Signal recovered
Unit lost	Access control unit, Intrusion detection unit, LPR unit, Video unit	Unit online
Zone armed / Zone disarmed[1]	Zone	• Zone state normal • Zone state active

[1] Events that are associated with the normal, active, and trouble states of a zone can also be configured with an acknowledgement condition.

Triggering alarms manually

To test an alarm that you just created, or if something critical occurs and you want to activate an alarm, you can trigger the alarm manually.

Before you begin

- The alarm must be configured in Config Tool.
- If you want to trigger alarms from the *Monitoring* task, you must enable Alarm monitoring.

To trigger an alarm manually:

- Do one of the following:
  - In the Config Tool **Alarms** task, select an alarm, and then click **Trigger alarm** (🔴) in the toolbar at the bottom of the workspace.
  - In the Security Desk notification tray, click **Hot actions (📢)** > **Manual action** . Click **Trigger alarm** (🔴), select an alarm, and then click **OK**.
  - In the Security Desk **Alarm monitoring** task or *Monitoring* task, click **Trigger alarm** (▶), select an alarm, and click**Trigger alarm**.

All pre-configured alarm recipients receive the alarm if they are logged on to Security Desk.

46

Threat levels

This section includes the following topics:

About threat levels

A *threat* is a potentially dangerous situation, such as a fire or a shooting, that requires immediate response from the system and the security personnel.

Each threat level is characterized by a name and a color, and is associated with two lists of actions that dictate the behavior of the system. One list is executed when the threat level is set, and the other list is executed when the threat is cleared. You can choose from any Security Center actions to define the threat level, plus some additional actions that are unique to threat levels, such as denying certain cardholders access to areas in your system or forcing certain users to log off from the system.

Threat levels are set by Security Desk users who have the *Set threat level* privilege when a dangerous situation occurs. Operators can set a threat level on an area or on the entire system (includes all areas).

Unlock schedules during an active threat level

Areas are configured with a security clearance level ranging from 0 to 7 (0 = highest security, 7 = lowest). A security clearance of 7 is the default value, usually meaning that the area does not require a special clearance. Unlock schedules for areas configured with a security clearance level different than seven are bypassed for the duration of the threat. Once the threat level is cleared, the unlock schedules for these areas resume.

Setting a threat level has no effect on the following:

- *Manual Override unlock schedule* commands from Security Desk
- *Manual Unlock* commands for specific doors from the Security Desk Door widget
- *Temporarily override unlock schedule* Event-to-Action
- REX activation, meaning the REX activation will still unlock the door
- HW Zone IO linking

Limitations of threat levels

The following limitations apply when using the threat level feature:

- Threat levels work independently of partitions. Therefore, a threat level set at the system level by the users of one partition might affect the entities belonging to another partition, if the actions have a generic scope (applied to *All entities*).
- Threat levels cannot be applied to federated areas.

Threat level actions

Normally, actions are applied to a specific entity. However, the actions that you configure for a *threat level* can be applied to a specific entity, or to all entities of the entity type related to that action.

For example, the action *Start recording* normally applies to one camera. However, when you are configuring a threat level, you can select *All entities* so that all the cameras start recording when the threat level is set.

NOTE: If you select a specific entity for your action, the action will be applied to the selected entity regardless whether the entity is found under the area where the threat level is set or not.

Actions exclusive to threat levels

The following actions are unique to threat level configuration.

Action name	Target entity	Description
Set minimum security clearance	area (Location)	Sets the minimum security clearance level required from cardholders to access the area on top of the restrictions imposed by the access rules. Additional parameter: • **Security clearance:** The minimum security clearance level required for the selected area. (0=highest level, 7=lowest level or no special clearance required). The *security clearance* option is only visible to administrative users. This action only works with door controllers that support this feature. The range of supported values might vary, depending on the access control hardware.
Set minimum user level	N/A	Logs out users with a lower user level than the one you specify when a threat level is set, and prevents them from logging back on. Additional parameter: • **User level:** The minimum user level (1=highest level, 254=lowest level) required to log on to the system, or to stay logged on to the system. This action is only executed when the threat level is set at the system level. If the user setting the threat level has a user level below the required minimum, that user is logged off the system the moment the threat level is set.
Set reader mode	area, door (Location)	Sets the reader mode for accessing doors. Additional parameter: • **Reader mode:** Select whether access is granted using *Card and PIN*, or *Card or PIN*, for the selected areas. This action only works with door controllers and readers that support this feature.

Differences between threat levels and alarms

There are key differences between threat levels and alarms, such as why they are triggered, how they are activated, and so on.

The following table highlights the differences between threat levels and alarms.

Characteristics	Alarm	Threat level
Purpose	Deals with localized events, such as a forced entry or an object being left unattended in a public area.	Deals with widespread events affecting an whole area or the entire system, such as a fire or a shooting.
Configuration privileges	• Config Tool • Add/delete alarms • Modify alarms	Only administrative users can configure threat levels.

Characteristics	Alarm	Threat level
Activation	Typically triggered by an event-to-action. Can also be triggered by a manual action.	Typically set manually by a Security Desk operator. Can also be set by an event-to-action.
System response on activation	Recording starts automatically on cameras associated to the alarm.	The threat level activation action list is automatically executed.
Notification method	The alarm icon turns red in the Security Desk notification tray. Depending on your Security Desk configuration, the *Alarm monitoring* task might be brought to the foreground.	The threat level icon turns red in the Security Desk notification tray. When a threat level is set at the system level, the background of Security Desk turns to the color of the threat level.
Recipients	Security Desk users configured as alarm recipients.	All Security Desk users.
Event ranking	Alarms are ranked according to their priority level (1=highest, 255=lowest). Higher priority alarms are displayed first. When the priority level is the same, the most recent is displayed first.	Threat levels are independent of each other. Only one threat level can be set on an area at any given time. The last threat level set overrides the previous one.
Deactivation	A Security Desk user (alarm recipient) must acknowledge the alarm. Alarms can also be automatically acknowledged by the system after a specified delay or when the acknowledgment condition is met.	A Security Desk user must manually clear the threat level or set a different threat level. A threat level can also be automatically cleared using an event-to-action (*Set threat level* to *None*).
System response on deactivation	The acknowledged alarm is removed from all active alarm list (*Alarm monitoring* task in Security Desk).	The threat level deactivation action list is automatically executed.
Related events	• *Alarm triggered* • *Alarm being investigated* • *Alarm condition cleared* • *Alarm acknowledged* • *Alarm acknowledged (alternate)* • *Alarm forcibly acknowledged*	• Threat level set • Threat level cleared

Characteristics	Alarm	Threat level
Operator privileges	• Security Desk (Application) • Alarm monitoring (Task) • Alarm report (Task) • Trigger alarms (Action) • Snooze alarms (Action) • Forward alarms (Action) • Acknowledge alarms (Action) **NOTE:** Only administrative users can forcibly acknowledge alarms.	• Security Desk (Application) • *Set threat level* (Action) The same privilege is used for both setting and clearing threat levels. To clear a threat level is to set it to *None*. **NOTE:** The threat level activation and deactivation actions are carried out by the system, independently of the operator's privileges.
Exclusive actions	None.	• Set minimum security clearance • Set minimum user level • Set reader mode

Related Topics
About alarms on page 735
Threat level actions on page 746

Defining threat levels

To help your security personnel quickly respond to a threatening situation, you can define threat levels.

What you should know

Only administrative users can define threat levels.

CAUTION: The system does not automatically revert to the state it was in before the threat level was set. You must explicitly define the actions that are triggered when the threat is cleared.

To define a threat level:

1. Open the **System** task, click the **General settings** view, and click the **Threat levels** page.
2. At the bottom of the threat level list, click **Add an item** (➕).
3. In the **Threat level configuration** dialog box, enter the **Name**, **Description**, **Logical ID** (optional), and **Color**of the threat level.

   TIP: Choose a distinctive color for each threat level, so that when the threat level is set at the system level and the Security Desk background turns that color, the users can easily identify the threat.

4. Configure the threat level **Activation actions**.

   These actions are executed by the system when the threat level is set, independently of the privileges and permissions of the user who set the threat level.

5. Configure the threat level **Deactivation actions**.

   These actions are executed by the system when the threat level is cleared or overwritten by another one, independently of the privileges and permissions of the user who cleared the threat level.

6. Click **OK**.

   A new threat level (🚨) appears in the threat level list.

7. Click **Apply**.

After you finish

For all users who need to set threat levels, make sure that they are part of the *public partition*, and make sure that they are assigned the *Set threat level* user privilege.

- To view which threat levels and security clearance are set on each area, use the *System status* task.
- To find out when threat levels were set and cleared, and who did it, use the Activity trails task.

Related Topics

Threat level actions on page 746
Monitoring the status of your Security Center system on page 263
Investigating user related activity on the system on page 266

Threat level scenario: Fire

A scenario for creating threat levels is in case of a fire.

If a fire breaks out, some actions that you want the system to respond with are the following:

- Sound the fire alarm.

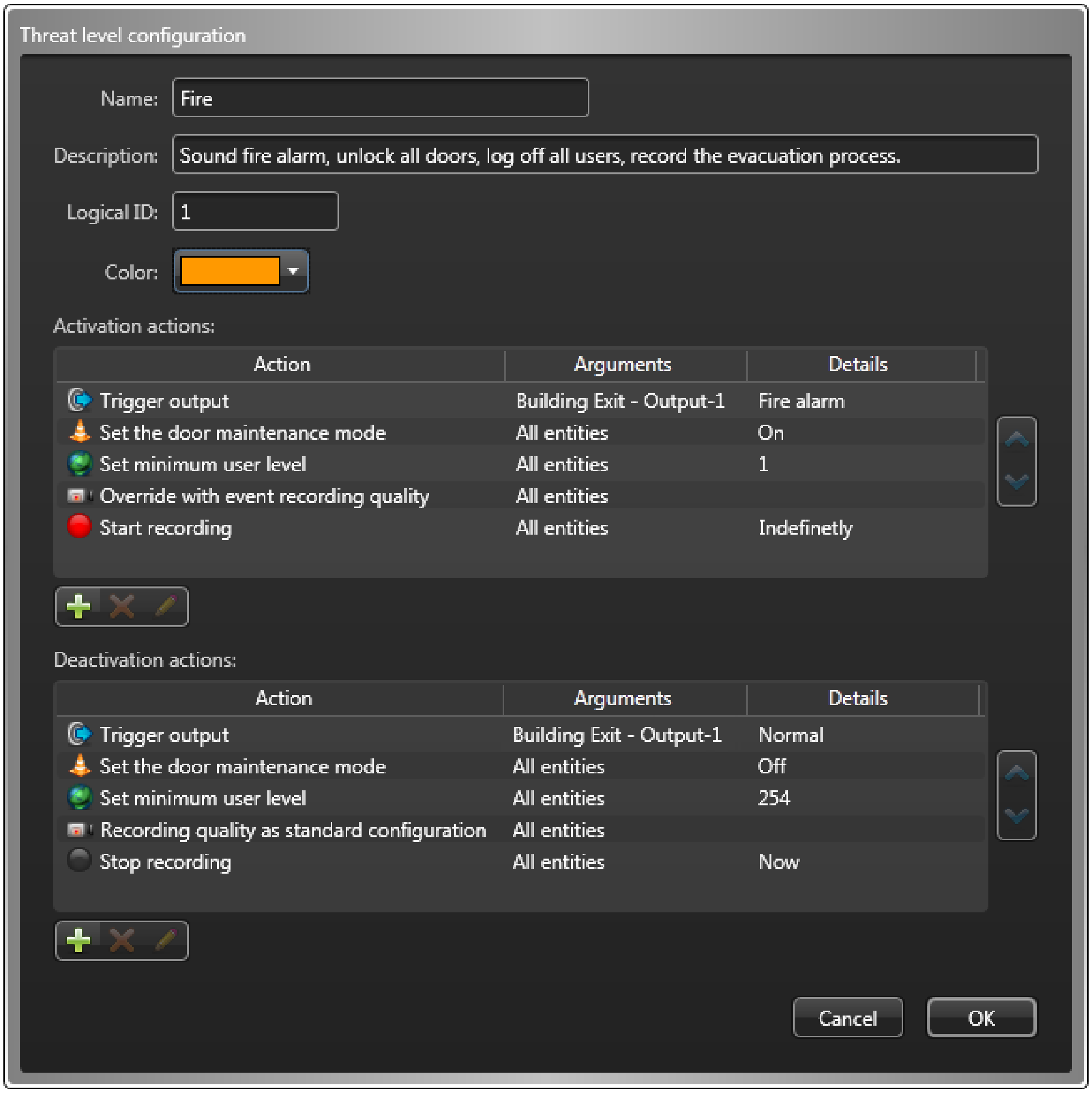
  NOTE: For the sake of illustration only. Not a recommended practice.

- Unlock all doors to let people evacuate.

  NOTE: For the sake of illustration only. Not a recommended practice.

- Log off all low priority users to free up your resources (especially network bandwidth), for high priority users to manage the current threat.
- Record the entire evacuation process at high video quality for as long as it lasts.

A threat level for responding to a fire could be configured as follows:



Name: Fire

Description: Sound fire alarm, unlock all doors, log off all users, record the evacuation process.

Logical ID: 1

Color: 🟧

Activation actions:

Action	Arguments	Details
Trigger output	Building Exit - Output-1	Fire alarm
Set the door maintenance mode	All entities	On
Set minimum user level	All entities	1
Override with event recording quality	All entities	
Start recording	All entities	Indefinetly

Deactivation actions:

Action	Arguments	Details
Trigger output	Building Exit - Output-1	Normal
Set the door maintenance mode	All entities	Off
Set minimum user level	All entities	254
Recording quality as standard configuration	All entities	
Stop recording	All entities	Now

When an operator sets this threat level, the following actions are executed by the system:

- **Trigger output:** Sounds the fire alarm by sending the *Fire alarm* output behavior to the output relay *Building Exit - Output-1*, assuming that this is where the alarm bell is connected.
- **Set the door maintenance mode:** Sets all doors within the area where the threat level is set to maintenance mode, effectively unlocking all of them for an indefinite period of time. This is better than using the *Unlock door explicitly* action which only unlocks the doors for a few seconds.
- **Set minimum user level:** Immediately logs off all users with a user level lower than 1, basically every one that is not an administrator, encouraging them to leave their desk at once, as well as stopping all unnecessary activity on the network, so the administrators can have as much bandwidth as possible at their disposal to deal with the situation.

  NOTE: This action is only executed if the threat level is set at the system level. So if the fire is limited to one area, we do not want to log off everyone from the system.
- **Override with event recording quality:** Boosts the recording quality of all cameras within the area where the threat level is set to event recording quality.
- **Start recording:** Starts recording on all cameras within the area where the threat level is set for an infinite duration, or until it the *Stop recording* command is issued.

When an operator clears this threat level, the following actions are executed by the system:

- **Trigger output:** Stops the fire alarm by sending the *Normal* output behavior to the output relay *Building Exit - Output-1*.
- **Set the door maintenance mode:** Turns off the maintenance mode on all doors within the area where the threat level is set. This effectively restores all doors to their normal behavior.
- **Set minimum user level:** Resets the minimum user level to 254 (the lowest value), allowing all users to log back on.
- **Recording quality as standard configuration:** Restores the standard recording quality on all cameras within the area where the threat level is set.
- **Stop recording:** Stops recording on all cameras within the area where the threat level is set. This action will not stop the recording on cameras that are on a continuous recording schedule.

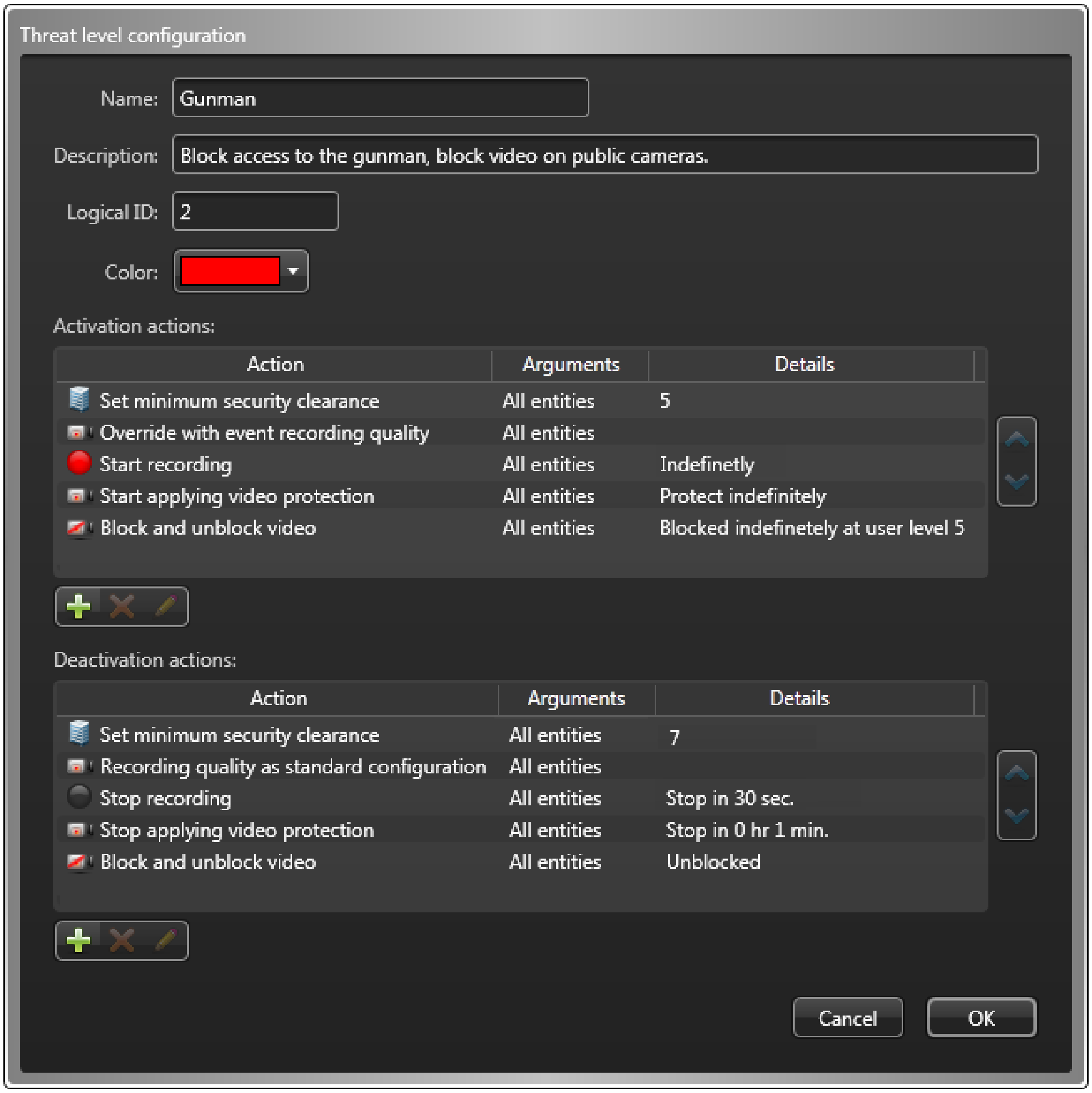
Threat level scenario: Gunman

A scenario for creating threat levels is in case of a gunman.

If a gunman or shooter is spotted, some actions that you want the system to respond with are the following:

- Block access to where the gunman/shooter is from innocent bystanders.
- Record the shooting incident in high quality video as evidence in court.
- Protect the video recordings of the whole event against accidental deletion.
- Block the sensitive video footage from the public eye in case some of the video streams are shown on public websites.

A threat level for responding to a gunman or shooter could be configured as follows:



Threat level configuration

Name: Gunman

Description: Block access to the gunman, block video on public cameras.

Logical ID: 2

Color: 🟥

Activation actions:

Action	Arguments	Details
Set minimum security clearance	All entities	5
Override with event recording quality	All entities	
Start recording	All entities	Indefinetly
Start applying video protection	All entities	Protect indefinitely
Block and unblock video	All entities	Blocked indefinetely at user level 5

Deactivation actions:

Action	Arguments	Details
Set minimum security clearance	All entities	7
Recording quality as standard configuration	All entities	
Stop recording	All entities	Stop in 30 sec.
Stop applying video protection	All entities	Stop in 0 hr 1 min.
Block and unblock video	All entities	Unblocked

When an operator sets this threat level, the following actions are executed by the system:

- **Set minimum security clearance:** Prevents the cardholders who have a security clearance lower than 5 (between 6-7) to enter the area where the gunman is, and hopefully, preventing the gunman from getting out.

NOTE: This configuration assumes that only armed security personnel have a clearance level higher than 5 (between 0-5), and that security operators continue to monitor all exits and can manually unlock doors to let the innocent people out.

- **Override with event recording quality:** Boosts the recording quality of all cameras within the area where the threat level is set to event recording quality.
- **Start recording:** Starts recording on all cameras within the area where the threat level is set for an infinite duration, or until it the *Stop recording* command is issued.
- **Start applying video protection:** Starts protecting the videos recorded from the cameras within the area where the threat level is set, from now until the *Stop applying video protection* command is issued, for an unlimited period of time.
- **Block and unblock video:** Block all users with a user level lower than 5 from viewing the video from the cameras within the area where the threat level is set, from now until the video blocking is explicitly stopped, for an unlimited period of time.

  NOTE: This configuration assumes that all security personnel have a user level higher than 5 and can continue to monitor the scene.

When an operator clears this threat level, the following actions are executed by the system:

- **Set minimum security clearance:** Restore normal access to the area to all cardholders by setting the security clearance to 99 (the lowest level).
- **Recording quality as standard configuration:** Restores the standard recording quality on all cameras within the area where the threat level is set.
- **Stop recording:** Stops recording on all cameras within the area where the threat level is set after 30 seconds. This action will not stop the recording on cameras that are on a continuous recording schedule.
- **Stop applying video protection:** Stops protecting the videos recorded from the cameras within the area where the threat level is set, after one minute.
- **Block and unblock video:** Unblock all cameras within the area where the threat level is set. The video recorded during the time when the threat level was active will remain blocked for playback to the users whose user level is lower than 5.

47

Zones and intrusion detection

This section includes the following topics:

About zones

A zone is a type of entity that monitors a set of inputs and triggers events based on their combined states. These events can be used to control output relays.

The concept of a zone is borrowed from the world of *alarm panels*, where electric inputs are associated with zones to trigger specific alarms. In Security Center, electrical inputs are associated with zones to trigger events. Using *event-to-actions*, these events can be used to not only trigger outputs, but also to trigger alarms, send emails, start camera recordings, and so on.

TIP: You can also define custom events to correspond to each of the special input combinations.

A zone can be armed (triggers activated), or disarmed (triggers deactivated) using a key switch, a software command, or on a schedule. A zone can be armed by software (using an action command or according to a schedule), or by hardware (for units that support this feature).

I/O linking

I/O linking is the control of specific output relays based on the combined result of a specific set of electric inputs. Each input can be connected to a specific monitoring device, such as a motion sensor, a smoke detector, a door or window contact, and so on.

For example, if a window shatters, the *glass break* sensor on a window connected to an input on a *unit*, can be linked to an output that triggers a buzzer.

CAUTION: On HID VertX units, some inputs, such as *AC Fail* and *Bat Fail*, must be configured for something other than their initial purpose (leave the checkboxes empty) before they can be used for I/O linking. However, other inputs, such as *Door Monitor*, can only be used for their designated purpose. If you use a specific purpose input as general purpose, your configuration will not work. Do not exceed 20 inputs per zone with HID VertX units. Exceeding this limit may lead to unit synchronization problems.

Zone states

Zone states are determined by a combination (AND/OR) of inputs associated with the zone.

The following zone states are available:

- **Normal:** When the combination of inputs yields a zero (0).
- **Active:** When the combination of inputs yields a one (1).
- **Trouble:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.

Hardware zones

A hardware zone is a zone entity in which the I/O linking is executed by a single access control unit. A hardware zone works independently of the Access Manager, and consequently, cannot be armed or disarmed from Security Desk.

Hardware zones are recommended when quick responses and offline operations are crucial for your security system. The *access control unit* controlling the zone must not be operated in *server mode*. Once the unit is configured in Security Center, it must be able to act on its own without being connected to, or controlled by Security Center.

Hardware zones can be armed using a key switch (input), or on schedules.

Virtual zones

A virtual zone is a zone entity where the I/O linking is done by software. The input and output devices can belong to different units of different types. A virtual zone is controlled by the Zone Manager and only works when all the units are online. It can be armed and disarmed from Security Desk.

Virtual zones are recommended when flexibility is required, and when access control units are not available.

I/O zones

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

I/O zones are recommended when quick responses, offline operation, and I/O linking across multiple units are required.

Differences between the types of zone

The following table lists the differences between a hardware zone, a virtual zone, and an I/O zone, and can help you decide which type of zone you need to create.

Characteristics	Hardware zone	Virtual zone	I/O zone
Recommended use	Hardware zones are recommended when quick responses and offline operations are crucial for your security system.	Virtual zones are recommended when flexibility is required, and when access control units are not available.	I/O zones are recommended when quick responses, offline operation, and I/O linking across multiple units are required.
Role	Access Manager	Zone Manager	Access Manager
Required unit type	HID or Synergis™ unit	Any type of unit with inputs and outputs[1]	Synergis™ units[2]
Unit operation mode	Online and Offline	Online	Online and Offline
I/O linking execution	Access control unit	Zone Manager	Master unit[3]
I/O linking (inputs)	All inputs must be from the same unit	Can combine inputs from any unit of any type	Can combine inputs from any unit
Logical operator (inputs)	**OR**/AND	**OR**/AND	OR
I/O linking (outputs)	All outputs must be from the same unit as the inputs	Can trigger outputs on any unit of any type	Can trigger outputs on any unit
I/O linking configuration	Zone configuration + event-to-actions	Zone configuration + event-to-actions	Zone configuration alone

Characteristics	Hardware zone	Virtual zone	I/O zone
Peer-to-peer	No	No	Yes[4]
Arm/disarm from Security Desk	No	Yes	Yes[5]
Arm/disarm using actions	No	Yes	Yes[5]
Arm/disarm using key switch	Yes[6]	No	No
Arm/disarm on schedule	Yes[7]	Yes[8]	Yes[9]
Arming delay	**OFF**/ON (mm:ss)	**OFF**/ON (mm:ss)	No
Entry delay	**OFF**/ON (mm:ss)	**OFF**/ON (mm:ss)	No
Maintenance mode	No	No	Yes

[1] Using zones to monitor the inputs of intrusion detection units is not recommended.

[2] Requires Security Center 5.5 and later, and Synergis™ Softwire 10.2 and later.

[3] The master unit is the Synergis™ unit that you select to do I/O linking.

[4] Up to 15 Synergis™ units can communicate directly with each other, as long as they are all under the same Access Manager.

[5] The master unit must be online.

[6] The key switch must be wired to an input on the same access control unit.

[7] Only one schedule at a time, and cannot be combined with the key switch approach.

[8] Supports multiple schedules.

[9] Supports multiple schedules, including exception schedules.

About Zone Managers

Zone Manager is a type of role that manages virtual zones and triggers events or output relays based on the inputs configured for each zone. It also logs the zone events in a database for zone activity reports.

Multiple instances of this role can be created on the system.

About output behaviors

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

Some examples of output behaviors can include controlling a parking gate, flashing a light in the warehouse, and so on.

Output behaviors are used to control output relays or access control units, video units, and zones that are not being used to control door locks. They can be triggered by automatic event-to-actions, manually through *hot actions* in Security Desk, or through *I/O linking*.

Creating hardware zones

To have a zone that can operate on its own even when the access control unit is not connected to the Access Manager, you must create a *hardware zone* in Security Center.

Before you begin

Do the following:

- Configure the Access Manager role that will manage the zone.
- Add the access control unit that will control the zone in your system.

What you should know

A *hardware zone* allows you to program the I/O linking behavior on an access control unit so it can operate on its own. Hardware zones can only be controlled by a single access control unit.

To create a hardware zone:

1 Open the **Area view** task.
2 Click **Add an entity** (➕) > **Zone**.
3 In the zone creation wizard, enter a name and description for the zone.
4 Select the area this zone is part of in **Location**, and click **Next**.
5 On the **Zone information** page, click **Hardware zone**.
6 From the dialog box, select the access control unit to control this zone and click **OK**.
7 Click **Create** > **Close**.

After you finish

Configure the hardware zone.

Related Topics
About zones on page 756

Configuring hardware zone settings

To monitor and set up I/O linking for hardware zones in Security Center, you must decide how the zone state is evaluated, which events are triggered based on the inputs associated with the zone, and when the zone is armed.

Before you begin

Do the following:

- To arm the zone on a schedule, a schedule must already be created.
- To arm the zone using a key switch, one of the inputs from the access control unit must be wired to the key switch.

What you should know

All input points and output relays configured for this zone must belong to the same access control unit that is controlling the zone.

You cannot arm or disarm a hardware zone from Security Desk, or by using a software command (event-to-actions).

To configure hardware zone settings:

1. Open the **Area view** task.
2. Select the hardware zone to configure, and click the **Properties** tab.
3. From the list, select the inputs to determine the state of the zone.
4. Turn the **Operator** switch to the desired position.
    - **AND:** Combine the input states with the logical AND operator.
    - **OR:** (Default) Combine the input states with the logical OR operator

    Example: If you select the **AND** operator, the zone is considered to be in a *Active* state when all selected inputs are in the *Active* state. If you select the **OR** operator, the zone is considered to be in a *Active* state if one of the selected inputs is in the *Active* state.
5. In the **Associated events** section, select which events to trigger when the zone state changes, from the following drop-down lists:

    These events are only triggered when the zone is armed. Select *None* if a zone state should be ignored.
    - **Normal:** When the combination of inputs yields a zero (0).
    - **Active:** When the combination of inputs yields a one (1).
    - **Trouble:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.
6. Enter in **Reactivation threshold**, how many milliseconds must pass before the event associated to the zone state can be re-triggered, and click **Apply**.
7. Click the **Arming** tab, and configure how the zone is armed.
8. In the *Arming source* section, select whether the zone is armed using a key switch, or on a schedule:
    - **Schedule:** Select a predefined schedule for arming the zone.
    - **Input point:** Select the input that is wired to the key switch.
9. (Optional) To give people more time to leave a zone they just armed, or disarm a zone they entered, turn the following options **ON**:
    - **Arming delay:** Duration (mm:ss) you want between the time the zone is armed and the time the event triggers become active.

- **Entry delay:** Duration (mm:ss) you want between the time the entry sensor is tripped and the time the events are triggered. This option allows you to disarm the zone before triggering the output relays.

10 (Optional) Select a **Countdown buzzer** to use for the duration of the arming delay, as follows:

NOTE: This option is only available when the zone is armed using a key switch.

a) From the **Countdown sounder** drop-down list, select an output relay.
b) From the **Output behavior** drop-down list, select an output behavior entity to determine the pattern of the signal to send to the buzzer.

11 Click **Apply**.

After you finish

- Test your zone by verifying that the generated events show up in the *Zone activities* report in Security Desk. For more information, see the *Security Desk User Guide*.
- For each associated event configured for this zone, create event-to-actions to trigger the desired output relays to complete the I/O linking configuration.

  NOTE: For the hardware zone to work, the output relays must be among the peripherals of the unit controlling the zone.

Related Topics
HID I/O linking considerations on page 960
Hardware zone configuration tabs on page 822

Creating virtual zones

To monitor input devices (sensors, switches, and so on) using Security Desk, and to use them to trigger events, you must create a *virtual zone* in Security Center.

Before you begin

Configure the Zone Manager role that will manage the zone.

What you should know

A virtual zone allows you to turn monitoring on/off in the various input devices (sensors, switches, and so on) on your system using Security Desk, and to use them to trigger events.

To create a virtual zone:

1. Open the **Area view** task.
2. Click **Add an entity** (➕) > **Zone**.
3. In the zone creation wizard, enter a name and description for the zone.
4. Select the area this zone is part of in **Location**, and click **Next**.
5. In the **Zone information** page, click **Virtual zone**.

   If you have multiple Zone Manager roles, you are prompted to select one.

6. Click **Create** > **Close**.

After you finish

Configure the virtual zone.

Related Topics
About zones on page 756

Configuring virtual zone settings

To monitor input devices and use them to trigger events for virtual zones in Security Center, you must decide how the zone state is evaluated, which events are triggered based on the inputs associated with the zone, and when the zone is armed.

Before you begin

To arm the zone on a schedule, a schedule must already be created.

What you should know

A virtual zone can be armed at any time by a Security Desk operator, or by the *Arm zone* action. Arming schedules is optional and is only necessary if you want the zone to be armed automatically at a certain time. An armed virtual zone can be disarmed at any time by a Security Desk user, or by the *Disarm zone* action triggered by an event.

To configure virtual zone settings:

1 Open the **Area view** task.
2 Select the virtual zone to configure, and click the **Properties** tab.
3 Under the **Inputs** list, click **Add an item** (+), select the inputs that will determine the state of the zone, and click **Select**.

   TIP: Hold **CTRL** or **SHIFT** to select multiple inputs.

4 Turn the **Operator** switch to the desired position.

   - **AND:** Combine the input states with the logical AND operator.
   - **OR:** (Default) Combine the input states with the logical OR operator

   Example: If you select the **AND** operator, the zone is considered to be in a *Active* state when all selected inputs are in the *Active* state. If you select the **OR** operator, the zone is considered to be in a *Active* state if one of the selected inputs is in the *Active* state.

5 In the **Associated events** section, select which events to trigger when the zone state changes, from the following drop-down lists:

   These events are only triggered when the zone is armed. Select *None* if a zone state should be ignored.

   - **Normal:** When the combination of inputs yields a zero (0).
   - **Active:** When the combination of inputs yields a one (1).
   - **Trouble:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.

6 Enter in **Reactivation threshold**, how many milliseconds must pass before the event associated to the zone state can be re-triggered, and click **Apply**.
7 Click the **Arming** tab, and configure how the zone is armed.
8 Under the *Arming source* section, click **Add an item** (+), select a predefined schedule for when the zone is armed, and click **Select**.
9 (Optional) To give people more time to leave a zone they just armed, or disarm a zone they entered, turn the following options **ON**:

   - **Arming delay:** Duration (mm:ss) you want between the time the zone is armed and the time the event triggers become active.
   - **Entry delay:** Duration (mm:ss) you want between the time the entry sensor is tripped and the time the events are triggered. This option allows you to disarm the zone before triggering the output relays.

10 Click **Apply**.

After you finish

- Test your zone by verifying that the generated events show up in the *Zone activities* report in Security Desk. For more information, see the *Security Desk User Guide*.
- For each associated event configured for this zone, create event-to-actions to trigger the desired output relays to complete the I/O linking configuration.

Related Topics
Virtual zone configuration tabs on page 851

Creating I/O zones

To have the inputs on one Synergis™ unit trigger output relays on other Synergis™ units (even when some, or none of them are connected to the Access Manager), you must create an *I/O zone* in Security Center.

Before you begin

Do the following:

- Configure the Access Manager role that will manage the zone.
- Add the Synergis™ units that will be linked by the zone.
- Make sure all units are running Synergis™ Softwire version 10.2 or later.

What you should know

An *I/O zone* allows you to program the I/O linking behavior on multiple Synergis™ units, with one unit designated as the master unit. All units must be managed by the same Access Manager. An I/O zone can be armed and disarmed from Security Desk as long as the master unit is online.

To create a hardware zone:

1. Open the **Area view** task.
2. Click **Add an entity** (✚) > **Zone**.
3. In the zone creation wizard, enter a name and description for the zone.
4. Select the area this zone is part of in **Location**, and click **Next**.
5. In the **Zone information** page, click **I/O zone**.
6. From the dialog box, select the Synergis™ unit that will play the role of *master unit* among its peers, and click **OK**.

   The master unit is the Synergis™ unit that you select to do I/O linking. Once your choice is made, it cannot be changed after the I/O zone is created.
7. Click **Create** > **Close**.

After you finish

Configure the I/O zone.

Related Topics
About zones on page 756

Configuring I/O zone settings

To monitor and set up I/O linking for I/O zones in Security Center, you must decide how the zone state is evaluated, which output relays are triggered based on the inputs associated with the zone, and when the zone is armed.

Before you begin

Do the following:

- To arm the zone on a schedule, a schedule must already be created.
- To trigger an output relay, an output behavior must already be created.

What you should know

All input points and output relays configured for this zone must belong to Synergis™ units that are managed by the same Access Manager.

You can configure the I/O linking from the I/O zone's **Properties** tab. You do not need to create *event-to-actions* in order to trigger output relays.

IMPORTANT: If the inputs and outputs configured for this zone do not belong to the same Synergis™ unit, you must enable the **Activate peer to peer** option on the Access Manager.

To configure I/O zone settings:

1. Open the **Area view** task.
2. Select the I/O zone to configure, and click the **Properties** tab.
3. From the **Arming schedule** drop-down list, select a predefined schedule for when the zone is armed.

   To add more predefined schedules for defining the arming schedule, click **Advanced** (⊕) and then click **Add an item** (✚).
4. (Optional) Click **Exceptions** to define periods within the arming schedule when the zone should not be armed.
5. Under the **Inputs** list, click **Add an item** (✚), and select inputs to determine the state of the zone.

   The zone is considered to be in a *Trouble* state if one of the inputs is in the Trouble state.
6. Under the **Outputs** list, click **Add an item** (✚), and select the output relays that you want to send the configured output behavior to, when the zone is armed and in the *Active* state, or when the zone is in the *Trouble* state.

   BEST PRACTICE: As much as possible, use the output relays on the master unit. This allows the I/O zone to continue to function when one or more slave units are down.
7. From the **Output behavior** drop-down list, select the output behavior to send to the output relays.
8. Select **Activate output on trouble when the zone is disarmed** if you want the output relays to be triggered when the zone is in the *Trouble* state.
9. From the **Revert to** drop-down list, select the output behavior to send to the output relays when the zone returns to the *Normal* state.
10. In the **Associated events** section, select which events to trigger when the zone state changes, from the following drop-down lists:

    These events are only triggered when the zone is armed. Select *None* if a zone state should be ignored.

    - **Normal:** When the combination of inputs yields a zero (0).
    - **Active:** When the combination of inputs yields a one (1).
    - **Trouble:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.

11 Enter in **Reactivation threshold**, how many milliseconds must pass before the event associated to the zone state can be re-triggered, and click **Apply**.

After you finish

Test your zone by verifying that the generated events show up in the *Zone activities* report in Security Desk. For more information, see the *Security Desk User Guide*.

Related Topics

I/O zone - Properties tab on page 825

Intrusion panel integration

Intrusion panels (also known as *alarm panels* or *control panels*) can be integrated to Security Center using the Intrusion Manager role, which allows you to monitor the status of each zone (or group of sensors) in real time, generate detailed activity reports, and arm/disarm zones (or partitions) defined on the intrusion panels in Security Desk.

Security Center supports Bosch, DSC PowerSeries, Honeywell Galaxy Dimension, and DMP intrusion panels. For information about integrating intrusion panels in Security Center, see the *Bosch Intrusion Panel Extention Guide*, the *Honeywell Galaxy Control Panel Integration Guide*, the *DMP Control Panel Integration Guide*, or the *DSC PowerSeries Intrusion Panel Extension Guide*.

How Intrusion panel integration works

The Intrusion Manager role receives events from the panel over an IP network or serial connection, reports them live in Security Desk, and logs them in a database for future reporting. The role also relays user commands to the panel (such as arming and disarming the intrusion detection areas), and triggers the outputs connected to the panel through event-to-actions (for example, an *Intrusion detection area master armed* event in Security Center can trigger an output on the panel).

About Intrusion Managers

Intrusion Manager is a type of role that monitors and controls *intrusion panels* (or alarm panels). It listens to the events reported by the intrusion panels, provides live reports to Security Center, and logs the events in a database for future reporting.

The Intrusion Manager also relays user commands to intrusion panels such as arming the *intrusion detection areas* (or zones), and triggering outputs connected to the panel using *event-to-actions*.

Multiple instances of this role can be created on the system.

Limitations of Intrusion Manager roles

For purposes of *failover*, the Intrusion Manager can be assigned to more than one server. However, the Intrusion Manager only supports failover when the intrusion panels are connected via IP. Failover is not supported if your intrusion panel is directly connected to your server via serial port, failover is not supported.

Creating the Intrusion Manager role

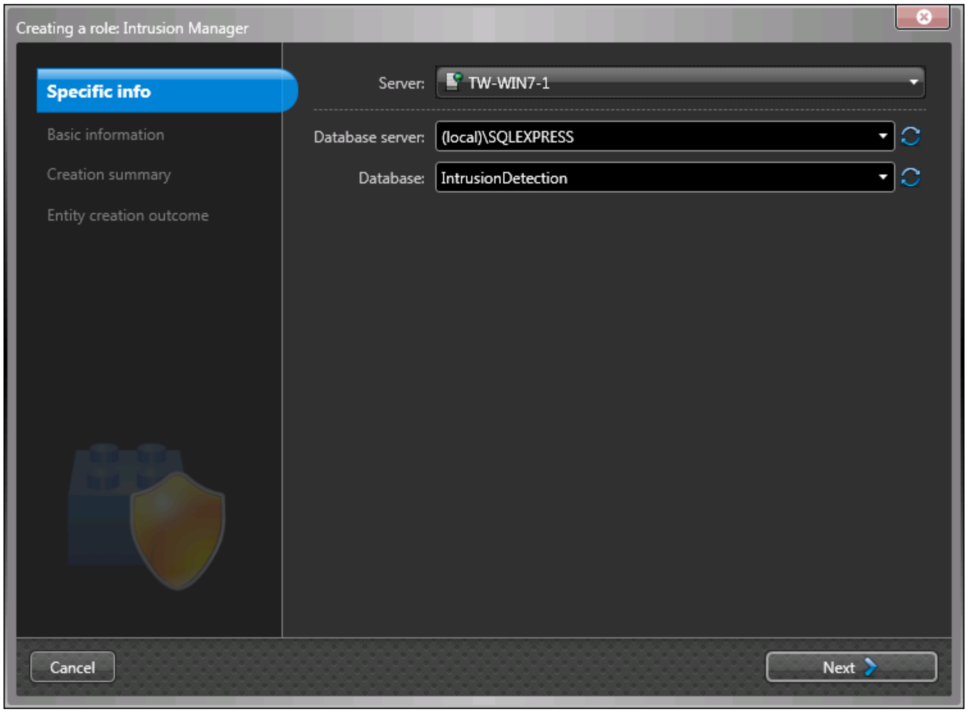
You must create an Intrusion Manager role in Config Tool to manage the panel.

To create an Intrusion Manager role:

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

2 Click **Add an entity** (➕), and then **Intrusion Manager**.

The *Creating a role: Intrusion Manager* window opens.



Creating a role: Intrusion Manager

Server: TW-WIN7-1

Database server: (local)\SQLEXPRESS

Database: IntrusionDetection

3 On the **Specific info** page, do the following:

a) From the **Server** drop-down list, select the server assigned to this role.

NOTE: If no expansion server is present, this option is not available.

b) In the **Database server** field, select or type the name of the database server.

c) In the **Database** field, select or type the name of the database (for example, **IntrusionDetection**).

d) Click **Next**.

4 On the **Basic information** page, do the following:

a) Type the **Entity name** (**Intrusion Manager**)

b) (Optional) Type an **Entity description** for the role.

c) Click **Next**.

5 On the **Creation summary** page, do the following:

a) Verify the information you entered.

b) If everything is correct, click **Create**, or click **Back** to modify your settings.

When the role is created, the following message appears: **The operation was successful**.

6 Click **Close**.

The Intrusion Manager role appears in your entity browser.

After you finish

Add the intrusion panel in Security Center.Configure the DMP extension properties.

About intrusion detection units

An intrusion detection unit is a type of entity that represents an intrusion panel (or alarm panel) that is monitored and controlled by Security Center.

An *intrusion panel* (also known as *alarm panel* or *control panel*) is a wall-mounted unit where the alarm sensors (motion sensors, smoke detectors, door sensors, and so on) and wiring of the intrusion alarms are connected and managed.

For a list of intrusion detection panels supported in Security Center, see the *Security Center Release Notes*.

To monitor and control intrusion detection areas (zones or partitions) in Security Desk, you must enroll the intrusion panel that controls them by adding an intrusion detection unit. For information about creating intrusion detection units in Security Center, see the *Bosch Intrusion Panel Extension Guide*, the *Honeywell Galaxy Control Panel Integration Guide*, the *DMP Control Panel Integration Guide*, or the *DSC PowerSeries Intrusion Panel Extension Guide*.

Limitations in monitoring intrusion panel inputs

We recommend that you use intrusion panels only for intrusion monitoring.

Intrusion panels are not designed to capture rapid consecutive changes to their input states, such as doors being opened and closed rapidly, or motion sensors that detect constant movements.

The main purpose of an input on an intrusion panel is to trigger an alarm when its state changes. When the input becomes active while its *intrusion detection area* is armed, the panel raises an alarm. Security Center uses this alarm to trigger an *Intrusion detection area alarm activated* event.

Example: DMP panels scan their inputs every 500 ms to detect state changes, but only send corresponding events every 2 seconds. Because of this behavior, it is not recommended to monitor inputs that change at a rate faster than once every 2 seconds, using these panels.

- Intrusion panels are limited in the number of events they can report; they are also limited in how fast they can transmit them. For example, DMP panels typically send one event every 2 seconds. If you are monitoring 100 inputs, and all the inputs have their state changed at the same time, it will require more than 3 minutes for Security Center to receive the last event.
- It might take a few minutes to receive the changes to the input states in Security Center.
- Some of the changes to the input states might not be reported in Security Center even though the panel raises intrusion alarms.

About intrusion detection areas

An intrusion detection area is a type of entity that corresponds to a zone or a partition (group of sensors) on an intrusion panel.

Intrusion detection areas might be created automatically by the Intrusion Manager role when the intrusion panels on which they are configured are enrolled to your system.

Intrusion detection areas are not configurable for the most part, except for the cameras assigned to them for monitoring purposes in Security Desk and the *event-to-actions*. They are automatically updated when the zones they correspond to are updated on the intrusion panels.

Users can perform the following actions on intrusion detection areas:

NOTE: You might not be able to perform some of these actions, depending on the type of intrusion panel you are using.

- **Master arm:** Master arm is arming an intrusion detection area in such a way that all sensors attributed to the area would set the alarm off if one of them is triggered. Some manufacturers call this arming mode “Away arming”.
- **Perimeter arm:** Perimeter arm is arming an intrusion detection area in such a way that only sensors attributed to the area perimeter set the alarm off if triggered. Other sensors, such as motion sensors inside the area, are ignored.
- **Disarm:** Disarm the area, by causing all sensors attributed to the selected intrusion detection area to be ignored by the intrusion panel.
- **Trigger intrusion alarm:** Trigger an intrusion alarm on the selected intrusion detection area. The alarm can also trigger an action on an input if you mapped the intrusion detection area to an output in Config Tool.
- **Silence alarm:** If there is an active alarm on the selected intrusion detection area, stop the siren on the intrusion panel from beeping. Depending on your intrusion panel and the type of alarm, clicking **Silence alarm** might also acknowledge the alarm.
- **Acknowledge alarm:** Acknowledge the intrusion alarm on the selected intrusion detection area.

Creating intrusion detection areas

If the intrusion detection areas weren't automatically created after the intrusion detection unit was enrolled, you must create them manually, so the areas can be armed, disarmed, and so on.

Before you begin

Add the intrusion detection unit to control the areas.

To create an intrusion detection area.

1 Open the **Intrusion detection** task.

2 Click **Add an entity** (✚) > **Show all** > **Intrusion detection area**.

3 In the **Basic information** page, enter a name and description for the area.

4 Select a **Partition** this area is a member of, and click **Next**.

Partitions determine which Security Center users have access to this entity. Only users that are part of the partition can view or modify the intrusion detection area.

5 From the **Intrusion detection unit** drop-down list, select the intrusion detection unit to control this area.

6 Under **Intrusion detection area unique ID**, enter the ID or name of the area as it is configured on the intrusion panel.

7 Click **Next** > **Create** > **Close**.

Related Topics

About intrusion detection areas on page 774

Moving intrusion detection units to a different Intrusion Manager

If you want a different Intrusion Manager role to manage and control an intrusion detection unit, for load balancing or another purpose, you can move the unit to another Intrusion Manager using the *Move unit* tool.

Before you begin

- The Intrusion Manager role must be on the same LAN as the intrusion detection unit it controls.
- If the unit manufacturer extension is not created automatically, you must add it.
- If the intrusion panel is physically connected to a serial port on the server hosting the original role, make sure you do the same with the server hosting the new role.

To move an intrusion detection unit to a different Intrusion Manager:

1. From the home page, click **Tools** > **Move unit**.
2. From the **Unit type** drop-down list, select **Intrusion detection unit**.
3. Select the units you want to move.
4. Under **Intrusion Manager**, select the new Intrusion Manager role to control the unit.
5. Click **Move** > **Close**.

Related Topics

Intrusion Manager configuration tabs on page 874

Part VIII

Config Tool reference

This part includes the following chapters:

- "Entity types" on page 778
- "Role types" on page 852
- "Administration tasks" on page 892
- "Events and actions" on page 907

48

Entity types

This section includes the following topics:

- "I/O zone - Properties tab" on page 825
- "Intrusion detection area - Properties tab" on page 826
- "Intrusion detection unit configuration tabs" on page 827
- "LPR unit - Properties tab" on page 828
- "Macro configuration tabs" on page 829
- "Monitor group - Monitors tab" on page 830
- "Network - Properties tab" on page 831
- "Output behavior - Properties tab" on page 832
- "Overtime rule configuration tabs" on page 833
- "Parking facility - Properties tab" on page 834
- "Partition - Properties tab" on page 835
- "Patroller - Properties tab" on page 836
- "Permit - Properties tab" on page 837
- "Permit restriction configuration tabs" on page 838
- "Schedule - Properties tab" on page 839
- "Scheduled task - Properties tab" on page 840
- "Server - Properties tab" on page 841
- "Tile plugin - Properties tab" on page 842
- "User configuration tabs" on page 843
- "User group configuration tabs" on page 845
- "Video unit - Identity tab" on page 847
- "Video unit - Properties tab" on page 848
- "Video unit - Peripherals tab" on page 849
- "Virtual zone configuration tabs" on page 851

Common configuration tabs

Some of the configuration tabs are commonly used by most Security Center entities.

Identity tab

The **Identity** tab provides descriptive information about the entity, such as its name, description, logical ID, and lets you jump to the configuration page of related entities.

- **Type:** Entity type.
- **Name:** Name for the entity Security Center. It is recommended to create a unique and descriptive name for each entity. In some cases, a default name is created, which you can change. Entity names are editable, except in the following cases:
  - **Server entities:** he entity name corresponds to the machine name and cannot be changed.
  - **Federated entities:** The entity name is defined on the original system and cannot be changed on the federation.
- **Description:** Optional information about the entity.
- **Logical ID:** Unique number assigned to the entity to easily identify them in the system (mainly for CCTV keyboard operations).
- **Relationships:**

  List of relationships between this entity and other entities on the system.

  You can use the command buttons found at the bottom of the list to manage the relationship between this entity and other entities in the system.

  - To add a new relationship, click ➕.
  - To remove a relationship, select a related entity, and click ✖.
  - To jump to a related entity's configuration page, select the entity, and click ➡.
- **Specific information:** Certain entity types, such as video units, might show additional information in this tab.

Cameras tab

The **Cameras** tab allows you to associate cameras to the entity so that when it is viewed in Security Desk, the cameras are displayed instead of the entity icon.

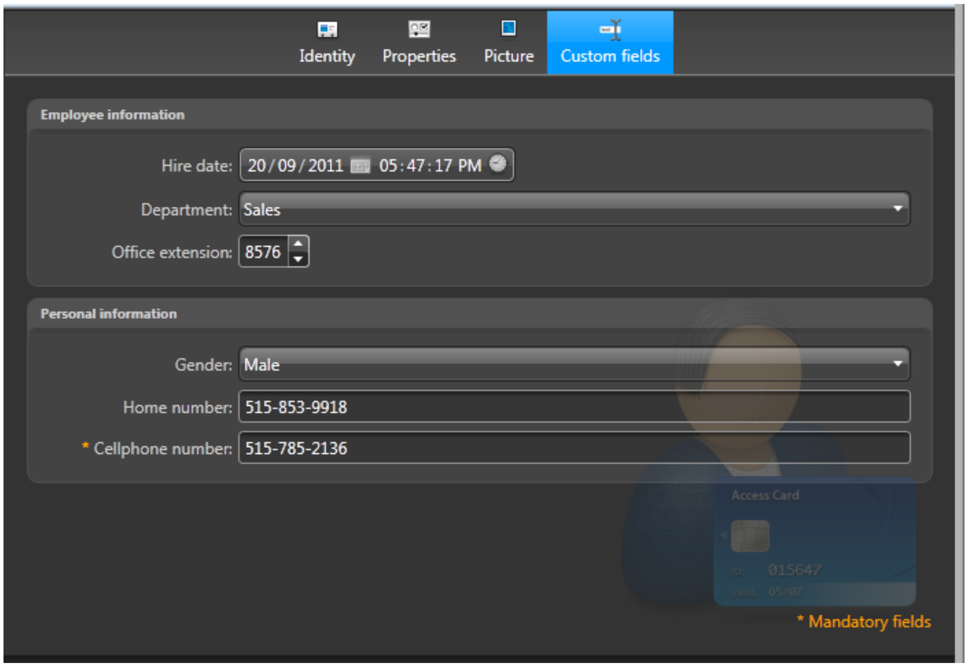
From this tab you can perform the following actions:

- To add a camera, click ➕.
- To remove the selected camera, click ✖.

Custom fields

The **Custom fields** tab lets you view and modify the custom fields defined for the entity. The sample screen shot below is that of a *cardholder* entity.

This tab only appears when custom fields are created for that type of entity.



Employee information

Hire date: 20 / 09 / 2011 05 : 47 : 17 PM

Department: Sales

Office extension: 8576

Personal information

Gender: Male

Home number: 515-853-9918

* Cellphone number: 515-785-2136

* Mandatory fields

In the above example, five custom fields have been defined for the cardholder entity, separated in two groups:

- Employee information
  - Hire date
  - Department
  - Office extension
- Personal information
  - Gender
  - Home number
  - Cellphone number (flagged as mandatory)

Location tab

The **Location** tab provides information regarding the time zone and the geographical location of the entity.

- **Time zone:** The time zone is used to display the entity events in the entity's local time zone. In Security Center, all times are stored in UTC in the *databases*, but are displayed according to the local time zone of the entities. The local time of the entity is displayed below the time zone selection.
- **Location:** The geographical location (latitude, longitude) of the entity. For video units, the location is used for the automatic calculation of the time the sun rises and sets on a given date. For fixed *LPR units* that are not equipped with a GPS receiver, the geographical location is used to plot the LPR events (*reads* and *hits*) associated to the LPR unit on the map in Security Desk.

Access control unit - HID - Identity tab

This section lists the settings found in the HID access control unit **Identity** tab, in the *Access control* task. This tab lets you view hardware-specific information, in addition to the standard entity information (name, description, logical ID, and so on).

- **Manufacturer:** Manufacturer of the access control unit.
- **Product type:** Model of the access control unit.
- **MAC address:** MAC address of the access control unit.
- **Firmware version:** Current firmware version installed on the access control unit.
- **Number of credentials:** Number of credentials stored on the unit versus the total number of credentials the unit can store, based on the available memory and the average number of bytes per credential.
- **Main memory:** Available memory on the unit.
- **Secondary memory:** Available secondary memory on the unit (when it applies).

Access control unit - HID - Properties tab

This section lists the settings found in HID access control unit **Properties** tab, in the *Access control* task. This tab lets you update the connection parameters after the HID unit has been discovered, such as the logon credentials, and the usage of certain specific inputs.

Connection settings

This section shows the connection parameters for the Access Manager to communicate with the unit. These settings are initialized when the HID unit is added to your system. Do not change these settings unless you changed them on the unit through the unit's web page or using the HID Discovery GUI after the unit was enrolled, or a representative of Genetec Inc. instructs you to do so.

- **Username/password:** Username and password used to log on to the HID unit.
- **Use translated host address:** Select this option when there is a NAT router between the unit and its Access Manager. The NAT router's IP address that is visible from the unit would be set here.
- **Static IP:** Select this option and configure the IP address, Gateway and Subnet mask manually if the HID unit uses a fixed IP address (recommended).
- **Use DHCP:** Select this option if the HID unit will be assigned its IP configuration by a DHCP server. When using the DHCP option, the DHCP server must be configured to always assign the same IP address to the unit.

General settings

This section displays the general settings of the HID unit.

- **Server mode:** This option is always greyed out because HID units do not support *server mode*.
- **Monitor AC Fail :** Select this option if the *AC fail* input is being used to monitor AC failures or for some other general purpose.
- **Monitor battery fail :** Select this option if the *Battery fail* input is being used to monitor the backup battery or for some other general purpose.

Access control unit - HID - Synchronization tab

This section lists the settings found in HID access control unit **Synchronization** tab, in the *Access control* task. This tab lets you configure the type of synchronization you want between the unit and its Access Manager.

- **Last update:** Indicates the day and time of the last successful synchronization with the unit.
- **Next update:** Day and time of the next scheduled synchronization with the unit.
- **Configuration expires on:** Indicates the day and time when the unit will no longer be capable of fully functioning independently of the Access Manager. This is due to the limited scheduling capability of the HID access control unit. You need to synchronize before the expiration date to ensure that the unit works properly on its own.

  CAUTION: HID VertX units expire after one year. Past the expiration date, the unit stops working.
- **Synchronize:** Click this button to send everything that changed since the last synchronization to the unit. This operation may cause a short service disruption if there are changes to door unlock schedules.
- **Synchronize and restart:** Click this button to send the full configuration to the unit and restart the unit. This operation will cause service disruption.

Synchronization options

You can select how frequently you want the unit synchronization to occur.

- **Automatically:** This is the recommended setting.

  Any configuration change is sent to the access control unit 15 seconds after the change is saved by the Config Tool, Web Client or Security Desk. Only configurations that affect that particular unit are sent.
- **Daily:** The unit is synchronized daily, at the specified times.
- **Every:** The unit is synchronized weekly, at the specified day and time.
- **Manual:** The unit is only synchronized when you click **Synchronize now**.

  Make sure you synchronize the unit before the configuration expires.

Access control unit - HID - Peripherals tab

This section lists the settings found in HID access control unit **Peripherals** tab, in the *Access control* task. In this tab, you can view and change the name and settings of the peripherals (readers and I/O devices) controlled by the unit.

The informations displayed on this page are:

- **Name:** Name of the interface module or peripheral. The peripherals are displayed in a hierarchical view by default.

  Click **Viewing mode** ( ) to select the *Flat view* if it is your preference.
- **Type:** Peripheral type: *In* (Input), *Out* (Output), *Reader*. Blank if it is not a peripheral.

  (Output relays only) Click **Trigger output** ( ) at the bottom of the list to send an output behavior (*Active*, *Normal*, or *Pulse*) to the selected device.
- **State:** Live peripheral state: *Active*, *Normal*, *Shunted* (inputs only), *Trouble* (inputs only), or *Unknown*.

  Use this column to test the connected interface modules and validate the wiring configuration of the I/O devices.
- **Additional info:** Settings specific to the type of peripheral.

  Double-click a peripheral, or click **Edit** ( ) at the bottom of the list to edit the settings of the selected peripheral.
- **Controlling:** Entity (door, elevator, zone) controlled by this peripheral.

  Click **Jump to** ( ) at the bottom of the list to view the configuration tabs of the entity controlled by the selected peripheral.
- **Logical ID:** (Hidden by default) Logical ID assigned to this peripheral for ease of reference in macros and SDK programs.
- **Physical name:** (Hidden by default) Static name assigned to this peripheral by the system.

TIP: Information on this page is also available to Security Desk users through the *System status* task, when monitoring peripherals.

Editable reader settings

The editable reader settings are:

- **Name:** Reader name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Shunted:** This feature is not supported by HID units.
- **Type of reader:** Select one of the following.
  - *Wiegand*
  - *Clock & Data*
  - *Wiegand (Dorado)*
  - *Clock & Data (Dorado)*

Editable input settings

The editable input settings are:

- **Name:** Input device name.

- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Shunted:** Select this option to ignore the inputs. Once shunted, the state of the input remains at *Normal*, regardless how you trigger it.
- **Debounce:** The amount of time an input can be in a changed state (for example, changed from *Active* to *Normal*) before the state change is reported. This option filters out signals that are unstable.
- **Contact type/ Presets:** Set the normal state of the input contact and its supervision mode.
  - **Not supervised / Normally closed:** The normal state of the input contact is closed, and the access control unit does not report if the input is in the trouble state.
  - **Not supervised / Normally open:** The normal state of the input contact is open, and the access control unit does not report if the input is in the trouble state.
  - **4-state supervised / Normally closed:** The normal state of the input contact is closed, and the access control unit reports when the input is in the trouble state.
  - **4-state supervised / Normally open:** The normal state of the input contact is open, and the access control unit reports when the input is in the trouble state.
- **Contact type/ Manual:** Manual settings. Allows you to set your custom range of values for *Active* and *Normal* input states.

Editable output settings

The editable reader settings are:

- **Name:** Output device name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Minimum time (Action):** If a relay is being used as part of a zone (either hardware or virtual), set a minimum number of seconds the relay stays closed when triggered by an event (for example, *Request to exit*).

Access control unit - Synergis™ – Identity tab

This section lists the settings found in the Synergis™ access control unit **Identity** tab, in the *Access control* task. This tab lets you view hardware-specific information, in addition to the standard entity information (name, description, logical ID, and so on).

- **Manufacturer:** Manufacturer of the access control unit.
- **Product type:** Model of the access control unit.
- **MAC address:** MAC address of the access control unit.
- **Discovery port:** Port used by the Access Manager to talk to this unit. It must match one of the discovery ports configured for the Genetec™ Synergis™ extension of the Access Manager.
- **Firmware version:** Current firmware version installed on the access control unit.
- **Number of credentials:** Number of credentials stored on the unit.

Access control unit - Synergis™ – Properties tab

This section lists the settings found in Synergis™ access control unit **Properties** tab, in the *Access control* task. This tab lets you update the connection parameters after the Synergis™ unit has been discovered, such as its logon credentials.

Connection settings

The connection settings are initialized when the Synergis™ unit is enrolled in your system. Do not change these settings unless you changed the unit's settings with Synergis™ Appliance Portal after the unit has been enrolled, or a representative of Genetec Inc. instructs you to do so.

- **Web address:** Web address for contacting Synergis™ Appliance Portal.
- **Username/Password:** Logon username and password.
- **Use DHCP:** Do not change this parameter unless asked by a Genetec™ Technical Assistance representative. This parameter is reset every time the Access Manager reconnects to the Synergis™ unit.
- **Ignore web proxy:** Select this option to instruct the Access Manager to ignore the Proxy Server settings on the server currently hosting the role. Clear this option to instruct the Access Manager to follow the Proxy Server settings (default=cleared).

General settings

This section allows you to configure the settings that are pushed from Security Center to the Synergis™ unit during synchronization.

- **Server mode:** Select this option if you want the Synergis™ unit to operate in *server mode* where all decisions are made by the Access Manager. Do not switch to server mode unless a representative of Genetec Inc. instructs you to do so.

Access control unit - Synergis™ – Portal tab

This section lists the settings found in the Synergis™ access control unit **Portal** tab, in the *Access control* task. This tab opens a window to the Synergis™ unit's web-based interface (Synergis™ Appliance Portal) which allows you to configure and maintain the unit.

Synergis™ Appliance Portal allows you to perform the following tasks:

- Change the security password required to log on to the Synergis™ unit.
- Configure the network settings on the Synergis™ unit so it works on your system.
- Configure the Synergis™ unit to accept connections from specific Access Managers.
- Enroll and configure the interface modules attached to the Synergis™ unit.

  NOTE: There is one exception to the rule. Mercury controllers (EP and M5-IC) must be enrolled and configured from Security Center Config Tool in the access control unit's **Peripherals** tab. For more information, see the chapter on Mercury controllers in the *Synergis™ Softwire Integration Guide*.
- Configure the access control behavior of the Synergis™ unit, for both online and offline operations.
- View the activity logs stored on the Synergis™ unit.
- Test and diagnose the interface module connections to the Synergis™ unit.
- View and export the Synergis™ unit's status and configuration.
- Upgrade the Synergis™ unit's firmware (Synergis™ Softwire).
- Restart the Synergis™ unit's hardware or software.
- Update security clearance levels assigned to Security Center areas manually on the appliance when the connection to the Access Manager is lost.

Related Topics

Access control unit - Synergis™ – Hardware tab on page 790

Access control unit - Synergis™ – Hardware tab

This section lists the settings found in the Synergis™ access control unit **Hardware** tab, in the *Access control* task. This tab only appears if your unit is running Synergis™ Softwire version 10.0 or more recent. It allows you configure the *interface modules* connected to the Synergis™ unit.

The Synergis™ unit (Synergis™ Cloud Link or Synergis™ Master Controller) supports the following third-party hardware integrations:

- Assa Abloy Aperio-enabled locks.
- Assa Abloy IP locks (both PoE and wireless).
- Axis intelligent IP controllers.
- DDS TPL and TPL-P4 RS-485 and IP controllers.
- Salto Sallis wireless locks.
- STid smart card readers.
- HID VertX interface modules (V100, V200, V300).

For more information on each of these integrations, see their related *Synergis™ Softwire Integration Guides*.

Related Topics
Access control unit - Synergis™ – Portal tab on page 789

Access control unit - Synergis™ – Synchronization tab

This section lists the settings found in the Synergis™ access control unit **Synchronization** tab, in the *Access control* task. This tab lets you manually trigger the synchronization between the unit and its Access Manager.

- **Last update:** Indicates the day and time of the last successful synchronization between the unit and its Access Manager.
- **Next update:** Does not apply. Changes affecting the Synergis™ unit are always sent automatically the moment they are saved.
- **Configuration expires on:** The synchronized data of the Synergis™ unit never expires because it understands the scheduling scheme used in Security Center.
- **Synchronize:** Click this button to send everything that changed since the last synchronization to the unit.

  This action always performs a full synchronization. A Synergis™ unit synchronization does not cause any service disruption.

Access control unit - Synergis™ - Peripherals tab

This section lists the settings found in the Synergis™ access control unit **Peripherals** tab, in the *Access control* task. This tab displays in a hierarchical view, all the *interface modules* attached to the unit, along with any downstream panels attached to them.

From the **Peripherals** tab, you can add and delete interface modules, and change the name and settings of the peripherals (readers and I/O devices) attached to the unit.

The informations displayed on this page are:

- **Name:** Name of the interface module or peripheral. The peripherals are displayed in a hierarchical view by default.

  Click **Viewing mode** () to select the *Flat view* if it is your preference.
- **Type:** Peripheral type: *In* (Input), *Out* (Output), *Reader*. Blank if it is not a peripheral.

  (Output relays only) Click **Trigger output** () at the bottom of the list to send an output behavior (*Active*, *Normal*, or *Pulse*) to the selected device.
- **State:** Live peripheral state: *Active*, *Normal*, *Shunted* (inputs and readers only), *Trouble* (inputs only), or *Unknown*.

  Use this column to test the connected interface modules and validate the wiring configuration of the I/O devices.
- **Additional info:** Settings specific to the type of peripheral.

  Double-click a peripheral, or click **Edit** () at the bottom of the list to edit the settings of the selected peripheral.
- **Controlling:** Entity (door, elevator, zone) controlled by this peripheral.

  Click **Jump to** () at the bottom of the list to view the configuration tabs of the entity controlled by the selected peripheral.
- **Logical ID:** (Hidden by default) Logical ID assigned to this peripheral for ease of reference in macros and SDK programs.
- **Physical name:** (Hidden by default) Static name assigned to this peripheral by the system.

TIP: Information on this page is also available to Security Desk users through the *System status* task, when monitoring peripherals.

Interface modules you can add and delete

You can only add and delete Mercury controllers (EP and M5-IC) attached to your Synergis™ unit from the **Peripherals** tab. For all other types of interface modules, you must add them either through the **Hardware** tab, or through the *Hardware* page of the Synergis™ Appliance Portal. For more information, see the *Synergis™ Softwire Integration Guide for Mercury Controllers*.

Editable reader settings

The editable reader settings are:

- **Name:** Reader name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Shunted:** Select this option to ignore the reads.

  This action can also be issued from Security Desk.

- **Type of reader:** Select the type corresponding to your reader. The list of available reader types depends on the type of interface module you have. Selecting the *Custom* reader type allows you to configure all the reader options manually.

Editable input settings

The editable input settings are:

- **Name:** Input device name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Shunted:** Select this option to ignore the inputs. Once shunted, the state of the input remains at *Normal*, regardless how you trigger it.
- **Debounce:** The amount of time an input can be in a changed state (for example, changed from *Active* to *Normal*) before the state change is reported. This option filters out signals that are unstable.
- **Contact type:** Set the normal state of the input contact and its supervision mode.
  - **Not supervised / Normally closed:** The normal state of the input contact is closed, and the access control unit does not report if the input is in the trouble state.
  - **Not supervised / Normally open:** The normal state of the input contact is open, and the access control unit does not report if the input is in the trouble state.
  - **4-state supervised / Normally closed:** The normal state of the input contact is closed, and the access control unit reports when the input is in the trouble state.
  - **4-state supervised / Normally open:** The normal state of the input contact is open, and the access control unit reports when the input is in the trouble state.
  - **Custom:** Allows you to set your custom range of values for *Active* and *Normal* input states. The actual values are set in the Mercury controller Advanced settings.

Editable output settings

The editable reader settings are:

- **Name:** Output device name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.

Access rule - Properties tab

This section lists the settings found in the Access rule **Properties** tab, in the *Access control* task.

In the *Properties* tab, you can link the 3 W's for an access rule: the "Who", "When" and "What". For example, "All Employees", "Office Hours", and "Access Granted".

- **Schedule:** Choose when this access rule is active.
- **When the schedule is active:** Select whether to grant or deny access from cardholders.
- **Cardholders affected by this rule:** Select the *cardholders* affected by this rule.

Alarm configuration tabs

This section lists the settings found in Alarm configuration tabs, in the *Alarm* task.

Alarm - Properties tab

In the *Properties* tab, you can define the essential alarm properties.

- **Priority:** Priority of the alarm (1-255), based on the urgency of the situation. Higher priority alarms are displayed first in Security Desk.
- **Recipients:** Users, user groups, and analog monitor groups who are notified when the alarm occurs, and are responsible for responding to the alarm situation.
- **Broadcast mode:** How the alarm recipients are notified about the alarm.
  - **All at once:** (Default) All recipients are notified at the same time, immediately after the alarm is triggered.
  - **Sequential:** The recipients are notified individually, each after a specified delay (in seconds) calculated from the time the alarm is triggered. If the recipient is a user group, all members of the user group are notified at the same time.
- **Attached entities:** Entities that help describe the alarm situation (for example, cameras, area, doors, alarm procedure, and so on). When the alarm is received in Security Desk, the attached entities can be displayed one after another in a sequence or all at once in the *canvas*, to help you review the situation. If a composite entity is attached to the alarm, the entities that compose it are also attached to the alarm. For example, of a door entity is attached to the alarm, the cameras associated to the door are also attached to the alarm.
- **Video display option:** If cameras are attached to the alarm, select whether to display live video, playback video, a series of still frames, or a combination of the three when the alarm is triggered.
  - **Live:** Display live video.
  - **Playback:** Display playback video.
  - **Live and playback:** Rotate between displaying live and playback video.
  - **Live and still frames:** Rotate between displaying live video and a series of still frames.
  - **Still frames:** Display a series of still frames.
- **Still frame durations:** Select whether you want each still frame to be displayed for the same duration or an independent duration of time.
  - **Same durations:** Display each still frame for the same duration of time.
    - **Number of frames:** Select the number of still frames to display within total content cycling duration.
    - **Play:** Select how many seconds before the alarm was triggered to start the first still frame.
  - **Independent durations:** Display each still frame for an independent duration of time.
    - **Relative time:** Select how many seconds before or after the alarm was triggered the still frame displays.
    - **Duration:** Select how long the still frame is displayed for.
- **Content cycling:** Turn this option on to automatically rotate the entities that are attached to the alarm in a display tile for an equal amount of time. The attached entities are listed in the order that they are displayed in Security Desk.

Alarm - Advanced tab

In the *Advanced settings* tab, you can configure the optional alarm properties.

- **Reactivation threshold:** The minimum time Security Center needs to wait after triggering this alarm before it can be triggered again. This option prevents the system from repeatedly triggering the same alarm before it is resolved.
- **Alarm procedure (URL):** Set a URL or the web page address corresponding to the *alarm procedure*, which provides alarm handling instructions to the operators. The web page is displayed when the user clicks *Show alarm procedure* (📋) in the alarm widget in Security Desk.
- **Schedule:** Define when this alarm is in operation. Outside the periods defined by this schedule, triggering this alarm has no effect.

  NOTE: You can add multiple schedules to the alarm. Schedule conflicts that cannot be resolved will be notified.
- **Automatic acknowledgment:** Turn this option on to let the system automatically acknowledge this alarm if no one acknowledges it before the specified time (in seconds). This option is recommended for low-priority alarms that serve to alert the security operator, but do not require any action. When this option is turned off, the system follows the **Auto ack alarms after** option configured at the system level in Server Admin.

  NOTE: Automatic acknowledgement does not apply to alarms that have an active condition attached. To acknowledge those alarms, you need to be logged on as an administrator and *forcibly acknowledge* them. For more information on acknowledging alarms, see the *Security Desk User Guide*.
- **Create an incident on acknowledgement:** Turn this option on to prompt the Security Desk user to report an *incident* every time they acknowledge an alarm.
- **Automatic video recording:** Turn this option off (default=on) if you do not want to start recording video when the alarm is triggered.
- **Protect recorded video:** Turn this option on (default=off) to protect the video recordings associated to this alarm for the specified number of days.

Analog monitor - Properties tab

This section lists the settings found in the Analog monitor **Properties** tab, in the *Video* task.

The *Properties* tab lets you configure the video stream usage (or function) and specific network settings for the analog monitor.

Video

In the *Video* section, you can configure settings that affect the quality the video.

- **Stream usage:** Select the video stream to use for cameras displayed in the analog monitor. This option is only available for decoders capable of generating multiple video streams. The stream usage options are the following:
- **Live:** Default stream used for viewing live video in Security Desk.
- **Recording:** Stream recorded by the Archiver for future investigation.
- **Remote:** Stream used for viewing video when the bandwidth is limited.
- **Low resolution:** Stream used instead of the *Live* stream when the tile used to view the stream in Security Desk is small.
- **High resolution:** Stream used instead of the *Live* stream when the tile used to view the stream in Security Desk is large.
- **Analog format:** Select NTSC (National Television System Committee) or PAL (Phase Alternating Line) analog format for the video signal. PAL format generally streams video at a lower frame rate, but at a higher resolution.
- **Display camera name:** Turn this option on if you want the camera name to be shown when it is displayed in the analog monitor in a Security Desk tile.

Network settings

In the *Network settings* section, you can configure the connection type used by the video decoder.

- **UDP port:** Port number used when the connection type is unicast *UDP*. If the encoder supports multiple video streams, this parameter is different for each stream.
- **Connection type:** Defines how communication is established between the Archiver and the unit for sending or receiving video streams. Each device on the same unit could support different connection types.
- **Best available:** Lets the Archiver select the best available connection type for the stream. The best available types rank in this order, according to availability: *Multicast*, *UDP*, and *TCP*. When the stream is requested for recording only, multicast is removed from the list, so the best available types start with UDP.
  - **Multicast:** Communication between a single sender and multiple receivers on a network. This is the preferred connection type. In this mode, multiple users in multiple locations can receive the same video transmission simultaneously from a same source, using the bandwidth only once. Most video units are capable of multicast transmissions.
  - **UDP:** Forces the stream to be sent in UDP to the Archiver. The stream must be formatted using the RTP protocol.
  - **TCP:** Forces the stream to be sent in *TCP* to the Archiver. Here, TCP is taken in the broad sense. For some types of cameras, the Archiver establishes a TCP connection to the unit and receives the stream in a proprietary protocol. For others, the stream is sent over HTTP. Typically, the stream is

not formatted according to the RTP protocol by the unit. The Archiver has to convert the stream to the RTP protocol to be archived or retransmitted to the system.

Hardware

In the *Hardware* section, you can associate other hardware devices (PTZ motor, Speaker, Microphone, and so on) to this analog monitor. When the decoder is added to the system, all hardware devices belonging to the same unit are configured by default. You can manually associate the analog monitor to other devices, according to how they are physically connected.

Area configuration tabs

This section lists the settings found in Area configuration tabs, in the *Area view* task.

Area - Identity tab

In the *Identity*tab, you configure the purpose of the area (whether or not it is used for access control), in addition to the standard entity information (name, description, logical ID, and so on).

- **Access control:** Set to **ON** to show the *Properties* and *Advanced* configuration tabs.

  NOTE: This switch is only visible when Synergis™ is enabled as feature.

Area - Properties tab

In the *Properties* tab, you define who has access to the area and through its perimeter doors.

NOTE: This tab is only visible when Synergis™ is enabled as a feature, and *Access control* is set to **ON** in the *Identity* tab of the area.

- **Access rules:** Define who has access to the area and when. Each rule can be applied to one or both sides of the doors.
  - **Access rules:** Add access rules to grant (or deny) access (entrance, exit, or both) to the area to cardholders and cardholder groups based on a schedule.
  - **Cardholders, cardholder groups:** Add cardholders and cardholder groups to define who have access to the area at all times.
    NOTE: Only grant access directly to cardholders for temporary situations or exceptions. If a group of cardholders should be allowed to access the area at all times as a regular setup, define an access rule with the *Always* schedule.
- **Doors:** Define both the *Perimeter* and *Captive* doors of the area. Perimeter doors are used to enter and exit an area, and help to control access. Captive doors are doors inside the area. By correctly setting the door sides, people counting and antipassback are properly tracked. A door's Entrance and Exit sides are relative to the area being configured.

  NOTE: Access rules assigned to the area apply to all perimeter doors of the area. If each perimeter door must be governed by its own set of rules, configure the access rules on each door.

Area - Advanced tab

In the *Advanced* tab, you define the advanced access control behaviors for the area.

NOTE: This tab is only visible when Synergis™ is enabled in your license, and *Access control* is set to **ON** in the *Identity* tab of the area. Moreover, some of these properties might not be visible, depending on your license options.

- **Antipassback:** Antipassback is the access restriction placed on a secured area that prevents the same cardholder from entering an area they have not yet exited, and vice versa.
  - **Status:** Turn the antipassback feature on or off.
  - **Schedule:** Select *Always* if you want antipassback to be applied at all times.
  - **Type:** Type of antipassback to apply.
    - **Soft:** Soft antipassback only logs the passback events in the database. It does not restrict the door from being unlocked due to a passback event.
    - **Hard:** Hard antipassback logs an entry in the database and prevents the door from being unlocked due to a passback event.

  - **Presence timeout:** Set how many minutes a cardholder’s presence in the area is remembered for the purpose of passback detection (not used for counting people). Past that period, a cardholder who never left the area can re-enter without triggering a passback event. The default value of zero (0) minutes means that a cardholder's presence never times out.
    NOTE: When global antipassback is enabled, the presence of a cardholder in an area is forgotten after seven days if no entry or exit from this area is reported for that cardholder during that period. This means that cardholders can re-enter an area that they never left, or leave an area they never entered, without triggering a passback event if no movement was registered for these cardholders on that area for seven days. This applies even if the **Presence timeout** is set to infinite (=0).
  - **Strict:** Turn this option on to generate passback events for both types of access violations: when cardholders try to re-enter an area that they never left, and when cardholders try to exit an area that they never entered. Otherwise, the default is set to **OFF** and antipassback logic is only verified on area entrances, and passback events are only generated when cardholders try to re-enter an area that they never left.
    BEST PRACTICE: If you choose to enable *strict* and *hard* antipassback on an area that is not controlled with turnstiles or similar devices that only allow one person through at a time, grant the *Forgive antipassback violation* privilege to the operators responsible for monitoring this area.
    NOTE: With strict antipassback turned off, you can have Card-In/REX-out perimeter doors, but the **Presence timeout** parameter must be configured (> 0). With strict antipassback turned on, all perimeter doors must be configured as Card-In/Card-Out, **Presence timeout** must be set to infinite (= 0), and no REX can be configured.
- **Interlock:** Security Center supports the interlocking of the perimeter doors for an area by allowing only one perimeter door to be open at one time.
  - **Status:** Turn the interlock feature on or off. When this feature is on, only one perimeter door of the area can be open at any given time. To open a door, all others must be closed.
  - **Priority:** When both the *override* and *lockdown* inputs are configured, select which one has priority when both inputs are active.
  - **Override:** Select the input that is wired to the *override* key switch or flip switch. When the switch in on, the interlock feature is disabled.
  - **Lockdown:** Select the input that is wired to the *lockdown* key switch or flip switch. When the switch is on, all perimeter doors remain locked until the switch is back to its normal position.
- **First-person-in rule:** The *first-person-in* rule is the access restriction placed on a secured area that prevents anyone from entering the area unless a supervisory cardholder is on site. The first-person-in rule can be enforced on door *unlock schedules*, *access rules*, or both.
  - **Enforce on door unlock schedules:** Set to **ON** to ignore all door unlock schedules until a supervisor is granted access to the area. The first-person-in rule has no effect on elevator unlock schedules.
  - **Enforce on access rules:** Set to **ON** to ignore access rules until a supervisor is present in the area. You specify when the first-person-in rule applies with a schedule.
  - **Supervisors:** List of cardholders who can act as area supervisors.
  - **Exemption list:** List of cardholders who continue to follow the access rules even when the first-person-in rule is in effect.
- **Visitor escort rule:** With strict antipassback turned off, you can have Card-In/REX-out perimeter doors, but an Presence timeout must be configured (> 0). With strict antipassback turned on, all perimeter doors must be configured as Card-In/Card-Out, and no REX and no timeout may be configured.

  NOTE: The actual escorts are configured in the *Visitor management* task. The maximum delay granted to the escort to present their credential after the visitor has presented theirs is configured individually for each door.

- **Enforce visitor escort rule:** Set to **ON** to require the escort to present their credential after the visitor, if the visitor has a mandatory escort assigned.

Area - Threats tab

In the *Threats* tab, you configure specific actions to be executed by the system when a threat level is activated or deactivated for this area.

NOTE: This tab is only visible when the *Threat level* license option is enabled, and at least one threat level is configured in your system.

Badge template - Badge designer tab

This section lists the settings found in the Badge template **Badge designer** tab, in the *Access control* task.

In the *Badge designer* tab, you can design and modify badge templates. In the Badge designer, there are different tools you can use to edit a template.

- **Tools:** In the *Tools* section, there are six graphical tools you can use to edit the template:
  - **Select tool:** Use to click and select an object on the template.
  - **Rectangle tool:** Use to draw a square/rectangle on the template.
  - **Ellipsis tool:** Use to draw circles/ovals on the template.
  - **Text tool:** Use to insert text on to the template.
  - **Image tool:** Use to insert a picture on to the template.
  - **Barcode tool:** Use to insert barcodes on to the template.
- **Image:** In this widget, you can choose whether the image displayed on the badge uses a cardholder picture or an image from a file, and whether the image should be stretched or not.
- **Text:** In this widget, you can add cardholder fields, as well as edit the text, the text color, and the text alignment.
- **Color and border:** In this widget, the following options are available:
  - **Fill:** Use to modify the fill color of an inserted object like a square or oval.
  - **Opacity:** Use to modify the opacity of an inserted object.
  - **Border:** Use to modify the border color of an inserted object.
  - **Border thickness:** Use to modify the thickness of the inserted object's border.
- **Size and position:** In this widget, you can choose where the text or image is located on the badge, and its width and height.
- **Properties (⚙):** Opens the *Format* dialog box, where you can select from the following card sizes and orientation.
  - CR70
  - CR80
  - CR90
  - CR100
  - Custom card size
  - Orientation. You can choose *Landscape* or *Portrait* orientation.
- **Import ():** Import a badge design that was previously exported from Config Tool as a badge template (BDG formats only).
- **Export ():** Save the current badge design to a BDG file so it can be imported to another system.
- **Cut (✂):** Delete the selected item on the badge template.
- **Copy (⧉):** Copy the selected item on the badge template.
- **Paste (📋) :** Paste the copied item onto the badge template.
- **Send to back ():** Send the selected item to the background of the badge template. This option is helpful if you want to have a background image on the badge.
- **Bring to front ():** Bring the selected item to the foreground of the badge template.

Camera - Video tab

This section lists the settings found in the Camera **Video** tab, in the *Video* task.

The *Video* tab allows you to define multiple video quality (resolution, frame rate, and so on) configurations for each video *stream* generated by your video encoder. For each stream, you can also specify its usage (or function) and specific network settings.

Video quality

In the *Video quality* section, you can configure settings that affect the quality of the video (image resolution, bit rate, frame rate, and so on). Multiple video quality configurations can be defined for the same stream on different schedules.

Video quality settings might vary from one manufacturer to another. No manufacturer supports them all.

NOTE: For any setting not covered in the list below, refer to the manufacturer's documentation.

- **Resolution:** Data format and image resolution. The available choices depend on the type of video unit you have.

  NOTE: On certain models of video units that support a large number of video feeds (4 to 12), some high resolution formats might be disabled if you enable all the video streams, because the unit cannot handle all the streams at high resolutions.
- **Quality:** Video quality depends on a combination of settings. Config Tool proposes a list of predefined configurations for you to choose from. To adjust each of them individually, select *Custom* from the *Quality* drop-down list.
- **Bit rate:** Sets the maximum bandwidth (kbps) allowed for this encoder.
- **Bit rate mode:** Certain types of video units (such as Axis) allow you to set the maximum bit rate at the unit level. In this case, the *Bit rate mode* drop-down list is available for your bit rate settings.
  - **Variable:** Variable bit rate (VBR) adjusts the bit rate according to the complexity of the images in the video. This uses a lot of bandwidth when there is a lot of activity in the image and less bandwidth when the monitored area is quiet.
  - **Constant:** Constant bit rate (CBR) allows you to set a fixed target bit rate that will consume a predictable amount of bandwidth, which will not change, whatever happens in the image. This requires you to set another parameter, the *Bit rate priority*.
- **Bit rate priority:** If you choose to maintain a constant bit rate, the encoder might not be able to keep both the frame rate and the image quality at their set values when the activity in the image increases. The *Bit rate priority* lets you configure which aspect of video quality you wish to favor when you are forced to make a compromise.
  - **Frame rate:** Maintains the frame rate at the expense of the image quality.
  - **Image quality:** Maintains the image quality at the expense of the frame rate.
  - **None:** Lowers both the frame rate and the image quality to maintain the bit rate.
- **Frame rate:** Sets the number of *frames* per second (fps). A high frame rate (10 fps or more) produces fluid video and is essential for accurate *motion detection*. However, increasing the frame rate also sends more information over the network, and therefore, requires more bandwidth.
- **Image quality:** Sets the image quality (the higher the value, the better the quality). Higher image quality requires more bandwidth, which might compromise the frame rate.

  When bandwidth is limited, you should consider the following:
  - To retain very good image quality, restrict the number of images per second (lower frame rate).
  - To transmit more images per second at a high frame rate, lower the image quality.

The encoder tries to maintain each quality setting. However, if bandwidth is limited, the encoder might reduce the frame rate in favor of the image quality.

- **Automatic settings:** Certain models of encoders (such as Bosch) let you select this option instead of setting your own value for image quality. To set the image quality manually, you have to select *Custom* in the *Quality* drop-down list.
- **Key frame interval:** A *key frame* is a frame that contains a complete image by itself as opposed to a usual frame that only holds information that changed compared to the previous frame. If your network is less reliable, you require a higher key frame rate to recover more quickly from cumulative errors in the video. Frequent key frames require a higher bandwidth. You can specify the key frame interval in seconds (1 to 20) or by frames (based on the frame rate).
- **Recording frame rate:** Record the video at a lower frame rate than the rate used for viewing video. This setting save storage space, but it does not reduce bandwidth usage. Setting the *Recording frame rate* to anything other than *All frames* locks the *Key frame interval*.
- **Profile and level:** Used only for *MPEG-4* streams, the profile determines the tools available when generating the stream (for example, interlace, or B frames), and the level limits the resource usage (for example, max bit rate).
- **Video object type:** The Video Object Type (VOT) to use for MPEG-4 streams. The available choices are governed by the choice of *Profile and Level*.
- **GOP structure:** Stands for *Group Of Picture* structure. It is possible to configure up to four types of GOP structures:
    - **I:** Stands for *Intra* frame structure. Meaning only Intra (key frame) frames are sent. This is primarily for using an external multiplexer.
    - **IP:** Stands for *Intra and Predicted* frame structure. This setting results in the lowest possible video delay.
    - **IPB:** Stands for *Intra and Predicted and Bidirectional* frame structure. This setting enables the user to have a higher quality and a higher delay.
    - **IPBB:** Stands for *Intra and Predicted and Bidirectional and Bidirectional* frame structure. This setting enables the highest quality and a highest delay.
- **GOP length:** Stands for *Group Of Picture* length. With this value, it is possible to change the *distance* (number of frames) between the *intra-frames* in the MPEG-2 video stream.
- **Streaming type:** Select between VES (video elementary stream), which sends only video information, or PRG (program stream), which sends both video and audio information.
- **Input filter mode:** Lets you select a noise filter to apply to the video signal before it is encoded. It has four settings: *None*, *Low*, *Medium*, and *High*.

  NOTE: Removing noise from the video signal also reduces the sharpness of the image. If the video signal is relatively clean, do not apply any filter (*None*). The higher the filter level, the more blurry the video image becomes. Keeping a sharp image creates more pixels to encode, which uses more bandwidth. This is why on some video units the default is set to *Medium*.
- **Bit rate control:** Lets the encoder automatically lower the *bit rate* when one of the decoders is reporting transmission errors (dropped packets). This usually happens when there is a lot of motion on the camera. The encoder drops the bit rate as low as necessary to let all decoders receive an error free transmission. When the motion subsides, the encoder gradually increases the bit rate until it reaches the configured maximum limit. The trade-off between low bit rate and transmission errors is that with a low bit rate, the image stays crisp but the video might appear choppy, while with transmission errors, the image contains noises, but the video stays fluid.
- **Compression mode:** Select between SM4, Verint's proprietary version of MPEG-4 compression, or ISO, the standard MPEG-4 compression.

Stream usage

The *Stream usage* options are only available for encoders capable of generating multiple video streams. It allows you to specify the usage (or function) of each stream.

- **Live:** Default stream used for viewing live video in Security Desk.
- **Recording:** Stream recorded by the Archiver for future investigation.
- **Remote:** Stream used for viewing video when the bandwidth is limited.
- **Low resolution:** Stream used instead of the *Live* stream when the tile used to view the stream in Security Desk is small.
- **High resolution:** Stream used instead of the *Live* stream when the tile used to view the stream in Security Desk is large.

Network settings

The *Network settings* options allow you to configure the desired connection type used by the video encoder.

- **UDP port:** Port number used when the connection type is unicast *UDP*. If the encoder supports multiple video streams, this parameter is different for each stream.
- **Connection type:** Defines how communication is established between the Archiver and the camera for sending or receiving video streams.
  - **Best available:** Lets the Archiver select the best available connection type for the stream. The best available types rank in this order, according to availability: *Multicast*, *UDP*, *TCP*, *RTSP over HTTP*, and *RTSP over TCP*.
  - **Unicast UDP:** Forces the stream to be sent in UDP to the Archiver. The stream must be formatted using the RTP protocol.
  - **Unicast TCP:** Forces the stream to be sent in *TCP* to the Archiver. Here, TCP is taken in the broad sense. For some types of cameras, the Archiver establishes a TCP connection to the unit and receives the stream in a proprietary protocol. For others, the stream is sent over HTTP. Typically, the stream is not formatted according to the RTP protocol by the unit. The Archiver has to convert the stream to the RTP protocol to be archived or retransmitted to the system.
  - **RTSP stream over HTTP:** This is a special case of TCP connection. The Archiver uses the RTSP protocol to request the stream through an HTTP tunnel. The stream is sent back through this tunnel using the RTP protocol. This connection type is used to minimize the number of ports needed to communicate with a unit. It is usually the best way to request the stream when the unit is behind a NAT or firewall, because requests sent to HTTP ports are easily redirected through them.
  - **RTSP stream over TCP:** This is another special case of TCP connection. The Archiver uses the RTSP protocol to request the stream in TCP. The request is sent to the RTSP port of the unit.
  - **Same as unit:** Special case for Panasonic units. The connection type is the same for all streams of the unit. When present, it is the only connection type supported. The real connection type must be set in the specific configuration page of the unit.
- **Multicast address:** The *multicast* address and *port number* are assigned automatically by the system when the video unit is discovered. Each video encoder is assigned a different multicast address with a fixed port number. If the encoder is capable of generating multiple video streams, then a multicast address should be assigned to each stream. This is the most efficient configuration.

Boost quality on manual recording

Temporarily boost video quality when the recording is started manually by a Security Desk user when they click the *Record* (●) button or the *Add bookmark* (🔖) button. This option is only available for the recording stream.

Boost quality on event recording

Temporarily boost video quality when the recording is triggered by a *system event* (the *Start recording* action was executed, an *alarm* was triggered, or because of a motion event). *Boost quality on event recording* settings have priority over the *Boost quality on manual recording* settings. The length of the video quality boost depends on the event type, and the camera's recording settings.

Camera - Recording tab

This section lists the settings found in the Camera **Recording** tab, in the *Video* task.

In the *Recording* tab, you can customize the recording settings on each individual camera instead of using the archiving role settings.

If the camera is associated to additional Auxiliary Archiver roles, there is one group of settings for each archiving role the camera is associated to.

- **Recording settings:** Select whether the camera uses the settings inherited from the archiving role or uses its own custom settings.
  - **Inherit from Archiver:** Use the recording settings of the archiving role.
  - **Custom settings:** Configure the recording settings for the individual camera.

You can get a description of each recording setting from the Archiver recording tab.

Camera - Motion detection tab

This section lists the settings found in the Camera **Motion detection** tab, in the *Video* task.

In the *Motion detection* tab, you can define multiple motion detection configurations for your camera. Each configuration is based on a different schedule.

- **Motion detection:** Turns motion detection ON or OFF for the time periods covered by the schedule.
- **Detection is done on:** Specifies whether motion detection is performed on the Archiver (always available), or on the video unit (not all units support this feature).
- **Sensitivity:** Controls how much difference must be detected in a *block* between two consecutive frames before it is highlighted as a *motion block*. With the sensitivity set to the maximum (100%), the slightest variation in an image block is detected as motion. Lowering the sensitivity reduces the number of motion blocks detected in the video. You can decrease the sensitivity when your equipment is prone to generate noise.
- **Auto calibrate:** Automatically set the sensitivity to determine what constitutes positive motion.
- **Consecutive frame hits:** A frame where the number of *motion blocks* reaches the *Motion on threshold* is called a *hit*. Setting this parameter higher than 1 helps avoid false motion detection hits, such as from video noise in a single frame. This setting ensures that positive motion detection is only reported when a hit is observed over a certain number of consecutive frames. When enough consecutive hits have been observed, the first hit in the series is marked as the beginning of motion.
- **Advanced settings:** When an *H.264* stream is selected as the recording stream, the *Advanced settings* button is available. Click this button to open the *H.264 advanced motion detection settings* dialog box where you can refine your motion detection settings for an H.264 stream.
- **Vector emphasis:** Sets motion detection based on the difference in motion vector values (movement) between consecutive frames.
- **Luma emphasis:** Sets motion detection based on the difference in luma values (brightness) between consecutive frames.
- **Custom:** Allows you to customize your settings using the available sliders, if the *Vector* and *Luma emphasis* presets do not provide desirable results (if you are getting too many, or too few motion events). Adjust the following slider values between 0 and 100, until you achieve desirable results. The higher the value, the more motion is detected.
  - *Luma weight*. Sets motion detection based on the difference in luma values (brightness) between consecutive frames.
  - *Chroma weight*. Sets motion detection based on the difference in chroma (color) values between consecutive frames.
  - *Vectors weight*. Sets motion detection based on the difference in vector values (movement) between consecutive frames.
  - *Macroblocks weight*. Sets motion detection based on the presence of *intra-macroblocks* in your frame. This setting is useful when you notice motion detection indicators on still frames. For example, some units generate frames completely comprised of intra-macroblocks as a new reference point. When this happens, you will see motion detection blocks covering your whole image. Setting the *Macroblocks weight* to 0 helps prevent this from happening.
- **Motion zones:** A motion zone defines *where* on the video image motion should be detected. Up to six different motion zones can be defined per configuration. For the purpose of motion detection, the video image is divided into a large number of *blocks* (1,320 for NTSC encoding standard and 1,584 for PAL). Each of these blocks can be individually turned on/off for motion detection. A block where motion detection is turned on is represented by a semi-transparent blue square overlay on the video image.

- **Motion on threshold:** Indicates the minimum number of *motion blocks* that must be detected before the motion is significant enough to be reported. Together with the *Consecutive frame hits*, positive motion detection is made.
- **Motion off threshold:** In the same way the *Motion on threshold* detects the beginning of motion, the *Motion off threshold* detects the end of motion. Motion is considered stopped when the number of motion blocks drops below the *Motion off threshold* for at least 5 seconds.
- **Test zone:** The motion zone is displayed as blue overlays. The *motion blocks* are displayed as green overlays. The number of motion blocks is updated in real time. When the number of motion blocks reaches the *Motion threshold*, it is displayed in red.
- **Test all zones:** In this mode, all *motion zones* are displayed at once, with the number of motion blocks in each displayed separately.
- **View all motion:** Test the entire video image for motion. All motion anywhere on the image is displayed as motion blocks (green overlays). The total number of motion blocks is updated in real time. Use this mode to test the sensitivity setting for this camera.
- **Events:** Select the events related to motion detection generated by the system (default or custom events).

Camera - Color tab

This section lists the settings found in the Camera **Color** tab, in the *Video* task.

In the *Color* tab, you can adjust the video attributes such as brightness, contrast, hue, and saturation, based on different schedules.

- **Brightness:** Adjust the brightness of the video image for the selected schedule.
- **Contrast:** Adjust the contrast of the video image for the selected schedule.
- **Hue:** Adjust the hue of the video image for the selected schedule.
- **Saturation:** Adjust the saturation of the video image for the selected schedule.
- **Load default:** Reset all parameters to their default values for the selected schedule.
- **Analog format:** Select NTSC (National Television System Committee) or PAL (Phase Alternating Line) analog format for the video signal. PAL format generally streams video at a lower frame rate, but at a higher resolution.

Camera - Visual tracking tab

This section lists the settings found in the Camera **Visual tracking** tab, in the *Video* task.

From the *Visual tracking* tab, you can configure the visual tracking feature.

- **Select:** Resize, reposition, and rotate the selected video overlay using your mouse.
- **Rectangle:** Draw a rectangle on the video image.
- **Ellipse:** Draw an ellipse on the video image.
- **Entities:** Display the area view from which the cameras linked to the selected overlay can be dragged from.
- **Size and position:** Resize and reposition the selected video overlay.
- **Fill:** Select the fill color of the selected overlay.
- **Border:** Select the border color of the selected overlay.
- **Opacity:** Select the opacity percentage of the selected overlay.
- **Thickness:** Select the border thickness of the selected overlay.
- **Links:** List of cameras that were dragged from the area view into the selected overlay, and that a user can jump to from that camera in Security Desk.

Camera - Hardware tab

This section lists the settings found in the Camera **Hardware** tab, in the *Video* task.

In the *Hardware* tab, you can associate other hardware devices (PTZ motors, speakers, microphones, and so on) to this camera and configure specific hardware settings. When the unit is initially added to the system, all hardware devices belonging to the same unit are configured by default. You can manually associate your camera to other devices, according to how they are physically connected.

PTZ configuration

If the PTZ motor is not integrated to your camera, you need to configure the PTZ motor separately before you can control it in Security Desk. When you turn the PTZ switch on, additional settings appear.

- **Protocol:** Protocol used by the PTZ motor.
- **Serial port:** Serial port used to control the PTZ motor. Click ✏ to set the Idle delay, Idle command, and Lock delay parameters.
- **Enhanced PTZ:** Turn this option on to enable the zoom-box, center-on-click, and enhanced zoom PTZ commands.
- **Calibrate:** Click to calibrate the PTZ.

  NOTE: Not all cameras require PTZ calibration.
- **PTZ address:** Number identifying the selected PTZ motor on the serial port. This number is important because it is possible to connect more than one PTZ motor on the same serial port. This number must correspond to the dip switch settings on the PTZ hardware.
- **Max zoom factor:** The maximum zoom factor allowed for this camera.

If you observe positioning or rotation issues when controlling a PTZ camera, you can click **Specify rotation and direction offsets** for the following additional options:

- **Pan offset:** Enter the pan offset (in degrees) needed to align the camera with the position shown in Security Center.
- **Tilt offset:** Enter the tilt offset (in degrees) needed to align the camera with the position shown in Security Center.
- **Invert rotation direction:** If the camera does not rotate in the same the direction as shown in Security Center, select this option to invert the direction of rotation.

Idle delay

The Idle delay is the amount of time a PTZ motor becomes locked for when a user does one of the following:

- Moves an idle PTZ (which generates the *PTZ activated* event). After the idle delay period, the *PTZ stopped* event is generated. If users continue to move the PTZ, then the idle delay countdown timer continuously restarts.
- Zooms a PTZ motor (which generates the *PTZ zoom by user* event). After the last zoom operation and the idle delay period ends, the *PTZ zoom by user* stopped event is generated.

Example

The idle delay is 120 seconds. If a user zooms several times, and each zoom action is less than 120 seconds apart, only one *PTZ zoom by user* event is generated. If another user performs a zoom on the same PTZ before the idle delay expires, the *PTZ zoom by user* event is generated again, logged to the second user, and the countdown timer is restarted. The *PTZ zoom by user stopped*event is only generated after the Idle delay expires, and is logged to the second user.

Idle command

When the PTZ becomes idle (after the idle delay expires and the *PTZ stopped*or *PTZ zoom by user stopped* event is generated), this option determines the next action of the PTZ.

- **None:** The PTZ remains idle until a user starts controlling it.
- **Preset:** The PTZ moves to a preset position when it becomes idle.
- **Pattern:** The PTZ motor starts a PTZ pattern when it becomes idle.

Lock delay

The *Lock delay* is the amount of time a PTZ motor becomes locked for when a user clicks the Lock PTZ button (🔒) in the PTZ widget. After the lock delay period, the PTZ automatically unlocks.

Speaker and microphone

Even if the unit your camera belongs to does not support audio, you can still link your camera with audio devices (speaker and microphone) found on other units.

Camera tampering

Select this option to let Security Center process *Camera tampering* events issued by the unit. This setting is only available if the video unit is capable of detecting camera tampering.

- **Minimum duration:** Typically, any dysfunction that prevents the scene from being viewed properly (partial or complete obstruction of the camera view, sudden change of the field of view, or loss of focus) can be seen as an attempt to tamper with the camera. You can control how sensitive the unit is to these changes, by specifying how long the dysfunction must last before the unit generates a *Camera tampering* event.
- **Alarm for dark images:** Select this option for total obstructions to be considered as dysfunctions.

Audio alarm

Select this option to let Security Center process audio alarms issued by the unit as *Audio alarm* events. This setting is only available if the video unit is capable of raising audio alarms.

NOTE: The *Alarm level* sets the value used to trigger audio alarms on the unit. A unit can be configured to issue audio alarms when the sound level rises above or falls below the set value. The alarm level can be set in the range 0-100%, where 0% is the most sensitive and 100% the least sensitive.

Image rotation

Use this setting to correct the orientation of the image when the camera is mounted upside down or at a 90 degree angle. The rotation options might vary depending on the model of the camera.

Lens type

Use this setting to select the lens type for cameras with interchangeable lenses. Depending on the selected lens type, you might have additional settings to configure, such as *dewarping* a fish-eye lens.

Camera sequence - Cameras tab

This section lists the settings found in the Camera sequence **Cameras** tab, in the *Area view* task.

In the *Cameras* tab, you can add cameras that make up the camera sequence. The order of the cameras in the list is the order they are displayed in Security Desk.

Related Topics
Creating camera sequences on page 427

Cardholder configuration tabs

This section lists the settings found in Cardholder configuration tabs, in the *Access control* task.

Cardholder - Properties tab

In the *Properties* tab, you can view the cardholder's personal information and status. Additional information might be found in the *Custom fields* tab, if custom fields are created for cardholder entities.

- **First name:** Cardholder's first name. If the software language (chosen at installation) is latin-based, the *Name* field is configured as the first name followed by the last name. This order is reversed if you are using an Asian language such as Japanese or Chinese.
- **Last name:** Cardholder's last name.
- **Email address:** Cardholder's email address, used for automated actions associated to the cardholder (send an email).
- **Use extended grant time:** Grants the cardholder more time to pass through doors where the *Extended grant time* parameter is configured for a door. Use this option for cardholders with reduced mobility.
- **Bypass antipassback rules:** Exempts the cardholder from all *antipassback* restrictions.
- **Security clearance :** (Only visible to administrative users) Cardholder's security clearance level. A cardholder's security clearance level determines their access to areas when a threat level is set in Security Center. Level 0 is the highest clearance level, with the most privileges.
  - **Inherited from parent cardholder groups:** The cardholder's security clearance level is inherited from the parent cardholder groups. If the cardholder is part of multiple cardholder groups, then they inherit the highest security clearance level from the parent cardholder groups.
  - **Specific:** Set a security clearance level for the cardholder.
- **Status:** Set the their status to *Active* or *Inactive*. For their credential to work, and for them have access to any area, their status must be *Active*.
- **Activation:** Displays the date when the cardholder was activated.
- **Expiration:** Set an expiration for their profile:
  - **Never:** Never expires.
  - **Specific date:** Expires on a specific date and time.
  - **Set expiration on first use:** Expires after a specified number of days after the first use.
  - **When not used:** Expires when it has not been used for a specified number of days.

Cardholder - Picture tab

In the *Picture* tab, you can assign a picture to the cardholder.

Cardholder group - Properties tab

This section lists the settings found in the Cardholder group **Properties** tab, in the *Access control* task.

In the **Properties** tab, you can view and configure the members of this cardholder group, and configure their common properties. Additional information might be found in the **Custom fields** tab, if custom fields are created for cardholder groups.

- **Group available for visitors:** Set this to **ON** if this group will be used for visitors
- **Email address:** Email address for automated actions associated to the group (send an email).
- **Security clearance:** (Only visible to administrative users) Security clearance level for the cardholder group. A cardholder group's security clearance level determines their access to areas when a minimum security clearance level is required on areas by setting a threat level in Security Center. Level 0 is the highest clearance level, with the most privileges.
  - **Inherited from parent cardholder groups:** The cardholder group's security clearance level is inherited from their parent cardholder group. When multiple parent cardholder groups exist, the highest clearance level is inherited.
  - **Specific:** Set a specific security clearance level for the cardholder group.
- **Cardholders:** Define the cardholder group members using the ✚ and ✖ buttons. Both individual cardholders and other cardholder groups can be members.

Credential configuration tabs

This section lists the settings found in Credential configuration tabs, in the *Access control* task.

Credential - Properties tab

In the *Properties* tab, you can configure the credential information and status. Additional information might be found in the *Custom fields* tab.

- **Credential information:** This section identifies the details of the credential itself. If the credential is an access control card, the format, facility code and card number will be shown.
  - **Cardholder:** Displays the cardholder this credential is associated with. The cardholder can be changed if required.
- **Status:** Shows whether the credential status is *active* or *Inactive/Lost/Stolen/Expired*.
- **Activation:** Displays the date and time when the credential was attributed to this state.
- **Expiration:** Set an expiration for the credential:
  - **Never:** The credential never expires.
  - **Specific date:** The credential expires on a specific date and time.
  - **Set expiration on first use:** The credential expires after a specified number of days after the first use.
  - **When not used:** The credential expires when it has not been used for a specified number of days.

Credential - Badge template tab

In the *Badge template* tab, you can define the default badge template associated to this credential. You can preview what the credential will look like when printed using any specific badge template. You can also print the card credential.

Door configuration tabs

This section lists the settings found in Door configuration tabs, in the *Area view* task.

Door - Properties tab

In the *Properties* tab, you can configure the general behavior of the door. Some of the behaviors are not supported by all types of access control units. If the configured behavior is not supported by the selected access control unit, a yellow warning appears on the page, explaining why your configuration is not valid.

- **Unlocked for maintenance:** Set to *ON* if the door is unlocked, and possibly open for maintenance purposes. While the door is in maintenance mode it remains unlocked, and the *maintenance mode* icon (◆) is displayed on the door icon in maps. *Access granted*, *Access denied*, *Door forced open*, and *Door forced open too long* events are not generated while the door is in maintenance mode.
- **Standard grant time:** Amount of time the door is unlocked after an *Access granted* event is generated.
- **Extended grant time:** For cardholders with the property "extended grant time" turned on, the amount of time the door is unlocked after access is granted.
- **Standard entry time:** Amount of time the cardholder has to cross the entry sensor, in addition to the *Standard grant time*. If no entry is detected during this time, a *No entry detected* event is generated. This option is only supported when your door is configured with an entry sensor. If no entry sensor is configured, entry is assumed when the door opens. If no door sensor is configured, entry is assumed when an access is granted.

  For example, if the *Standard grant time* is 5 seconds, and the Entry time is 3 seconds, the cardholder has a total of 8 seconds to trigger the entry sensor of the door.
- **Extended entry time:** For cardholders with the property 'extended grant time' turned on, the amount of time the cardholder has to cross the entry sensor, in addition to the Extended grant time. If no entry is detected during this time, a *No entry detected* event is generated. This option is only supported when your door is configured with an entry sensor. If no entry sensor is configured, entry is assumed when the door opens. If no door sensor is configured, entry is assumed when an access is granted.

  For example, if the *Extended grant time* is 10 seconds, and the *Extended crossing time* is 10 seconds, the cardholder has a total of 20 seconds to cross the entry sensor of the door.
- **Door relock:** Specifies when to re-lock the door after an access has been granted.
  - **On close:** Relocks when the door closes.
    NOTE: This option is not supported by HID units.
  - **Delay after opening:** Relocks after the specified delay after the door has been opened.
    NOTE: For HID units, the maximum delay is 27 minutes.
- **When door is unlocked by schedule:** Select the events you want to suppress when the door is unlocked by schedule.
  - *Door open too long* events
  - *Access granted* and *Access denied* events
- **Door held:** What to do when the door is held open.
  - **Trigger event:** Set to **ON** if the *Door open too long* event must be generated after the specified duration.
  - **Reader buzzer behavior:** Set to either **Suppressed** to never sound the buzzer, or to **Suppressed when door closes** to silence the buzzer as soon as the door closes.
- **Door forced:** What to do when the door is forced.

    - **Trigger event:** Set to **ON** if the *Door forced open* event must be generated.
    - **Reader buzzer behavior:** Set to either **Suppressed** to never sound the buzzer, to **Suppressed when door closes** to stop the buzzer as soon as the door closes, or to **Suppressed on access granted** stop the buzzer when an access is granted, or when the door is manually locked.
- **Request to exit (REX):** The options in this section are generally used to decrease the number of false *Request to exit* events at a door.
    - **Time to ignore REX after granted access:** Ignore any requests to exits for this long after access has been granted.
    - **Automatically grant REX:** Set to **ON** if a REX is being used, and you want to automatically grant the request to exit.
      NOTE: Security Center does not receive Rex events if the access control unit is connected to the Access Manager. However, the Rex events are received when the unit is offline and then connects back to the Access Manager.
    - **Ignore REX events while door is open:** Do not generate REX events when door is open.
    - **Time to ignore REX after door closes:** Once the door has closed, wait this long before generating any more REX events.
- **Visitor escort rule and two-person rule:** Settings common to the visitor escort and the two-person rule restrictions.
    - **Enforce two-person rule:** Set to **ON** if two cardholders must present their credentials within a certain delay of each other in order to gain access. This rule can be enforced only on one door side or both.
    - **Maximum delay between card presentations:** Maximum delay allowed between the two card presentations to satisfy the visitor escort rule and the two-person rule restrictions.

Door - Hardware tab

In the *Hardware* tab, you can configure the physical wiring relationships between the access control unit and the door, and associate cameras to door sides.

- **Preferred unit:** Access control unit that is connected to the door.
- **Preferred interface:** Interface module that is connected to the door.
- **Door side:** Readers, REX's, entry sensors, and cameras associated with the door side, that match the physical wiring done on the controller and the door.

  The available reader settings are:

    - **PIN entry timeout:** For an HID unit, this sets the entry timeout for the first PIN digit after the card has been read, as well as the entry timeout for all subsequent PIN digits.
      For a Synergis™ unit, this only sets the entry timeout for the first PIN digit after the card has been read. The entry timeout for all subsequent PIN digits is fixed at 5 seconds.
    - **Use card and Pin:** Set to **ON** to change the reader mode to Card and PIN and select the schedule when this mode applies.
- **Additional connections:** Other physical connections associated with the controller and the door.

Door - Access rules tab

In the *Access rules* tab, you can view the access rules applied to this door.

- **Door access applies to:** Which door sides the access rules apply to.
    - **Both sides:** Apply the same access rules to both door sides.

  - **Individual sides:** Apply individual access rules to each door side.
- **Access rights for door (side):** Define who has access to this door (or door side).
  - **Access rules:** Add access rules to grant (or deny) access to the door to cardholders and cardholder groups based on a schedule. This is the recommended approach.
  - **Cardholders, cardholder groups:** Add cardholders and cardholder groups to grant them access to the area at all times. Only use this approach for temporary situations.
    NOTE: If all perimeter doors of an area share the same access rules, define those rules at the area level.

Door - Unlock schedules tab

In the *Unlock schedules* tab, you can configure scheduled periods when the door is not used for secured access, and no access rules are in effect.

- **Unlock schedules (free access):** Periods when the door is unlocked, and no access rules are in effect.
- **Exceptions to unlock schedules (controlled access):** Periods when the door is locked, and access rules apply.

Related Topics
HID I/O linking considerations on page 960

Elevator configuration tabs

This section lists the settings found in Elevator configuration tabs, in the *Area view* task.

Elevator - Floors tab

In the **Floors** tab, you can configure the physical wiring relationships between the access control unit and the elevator floors, and select cameras used to monitor this elevator in Security Desk.

- **Preferred unit:** Access control unit that manages this elevator cab's panel.
- **Elevator cab reader:** *Reader* interface that is used inside the elevator cab.

  The available reader settings are:

  - **PIN entry timeout:** For an HID unit, this sets the entry timeout for the first PIN digit after the card has been read, as well as the entry timeout for all subsequent PIN digits.
    For a Synergis™ unit, this only sets the entry timeout for the first PIN digit after the card has been read. The entry timeout for all subsequent PIN digits is fixed at 5 seconds.
  - **Use card and Pin:** Set to **ON** to change the reader mode to Card and PIN and select the schedule when this mode applies.
- **Camera:** Camera that monitors this elevator in Security Desk.
- **Floors:** Push button relays and inputs connected to the elevator floor buttons.
  - **Push button relay:** Output relays assigned to the different elevator floor buttons. Access granted events cause an output relay to close, which enables the button-push to request a certain floor.
  - **Floor tracking:** Inputs assigned to elevator floor buttons. When you assign inputs, Security Center can take note of which floor button was pushed.
  - **Cameras:** Cameras used to monitor the elevator door on each floor.

Elevator - Access tab

In the **Access** tab, you can configure the access rules applied to each of the elevator floor, and determine when access to the elevator floors is controlled and when *free access* is available.

- **Access rules:** Select access rules to determine which floor buttons are enabled, when, and for which cardholders. Different access rules can be applied to different floors, or applied to all floors.
- **Exceptions:** Determine if there are any exceptions to the access rule you set.
  - **Schedule:** Select a schedule when the exception applies.
  - **Floor:** Select which floors the exception applies to.
  - **Mode:** Select whether access to the elevator floor is *free* or *controlled* during the exception schedule.

Elevator - Advanced tab

In the **Advanced** tab, you can configure the advanced behavior of this elevator.

- **Grant time:** How long the elevator floor button is enabled after an access granted event is generated.
- **Free access when the output relay is:**
  - **Normal:** Floor access is granted when the access control unit output relay is de-energized. This means that a power loss results in free access to the floor.
  - **Active:** Floor access is granted when the access control unit output relay is energized. This mean that a power loss results in floor access being denied.

Hardware zone configuration tabs

Hardware zones are controlled by a single access control unit. They can work offline, and can be armed or disarmed using a key switch or on schedule.

Hardware zone - Properties tab

Click the **Properties** tab to configure the inputs that define this zone, and define how they are evaluated.

- **Access control unit:** Access control unit that controls the hardware zone.
- **Interface module:** Interface module where the inputs are selected from.
- **Inputs:** Inputs combined to evaluate the zone state.
- **Operator:** Logical operator used to combine the input states to evaluate the zone state.
- **Associated events:** Events representing the zone states. Select *None* if a zone state should be ignored.
  - **Normal state:** When the combination of inputs yields a zero (0).
  - **Active state:** When the combination of inputs yields a one (1).
  - **Trouble state:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.
  - **Reactivation threshold:** The time period during which the same event should not be re-triggered.

Hardware zone - Arming tab

Click the **Arming** tab to configure the arming source of your zone and its arming behavior.

- **Arming source:** Select whether the hardware zone is armed by a key switch or on a schedule.
  - **Schedule:** Select the schedule corresponding to the period when the zone is armed.
  - **Input point:** Select the input that is wired to the key switch.
- **Delays:** Optional delays that give you time to leave the premises after arming the zone, and time to disarm the zone after tripping a sensor.
  - **Arming delay:** Duration (mm:ss) you want between the time the zone is armed and the time the event triggers become active.
  - **Entry delay:** Duration (mm:ss) you want between the time the entry sensor is tripped and the time the events are triggered. This option allows you to disarm the zone before triggering the output relays.
- **Countdown buzzer:** You can assign an output relay to activate a countdown buzzer to match the arming delay.
  - **Countdown sounder:** Select the output relay.
  - **Output behavior:** Select the output behavior that defines the signal pattern for the buzzer.

Hotlist configuration tabs

This section lists the settings found in Hotlist configuration tabs, in the *LPR* task.

Hotlist - Properties tab

In the *Properties* tab, you can configure the basic properties of the hotlist (hotlist priority, hotlist path, attributes, and so on). These settings tell Security Center how to parse the hotlist file into the format required by the *Patroller* and the *LPR Manager* to identify plates read by *Sharp units*.

- **Priority. :** Hotlist priority. Zero (0) is the highest priority setting and 100 is the lowest priority setting. If a plate read matches more than one hotlist, the hotlist with the highest priority is displayed first in the list of hotlist matches.
- **Hotlist path:** Path to the hotlist source text file that contains the hotlist data, such as license plate numbers and other related vehicle information. The source text file can be located on the LPR Manager computer's local drive (for example, the C drive), or on a network drive that is accessible from the LPR Manager computer.
- **Use delimiters:** Tells Security Center that the fields in the hotlist file vary in length, and indicates the character used to separate each field in the file. By default, *Use delimiters* is set to *On*, and the delimiter specified is a *semi-colon* (;). If your hotlist file is made up of fixed length fields, set *Use delimiters* to *Off*.
- **Visible in editor:** Allow a user to edit the hotlist or permit list using the Hotlist and permit editor task.
- **Attributes:** Tells Security Center the name and order of the fields (attributes) in the source text file.

Hotlist - Advanced tab

In the *Advanced* tab, you can configure the advanced properties of the hotlist (the color, sound, download frequency, and so on). These properties are not required for all hotlists, but allow you to customize certain hotlists for specific scenarios.

- **Color. :** Assigns a color to a hotlist. When you choose a color, the map symbol that marks the location of the hotlist hit in Security Desk and Patroller, as well of the Hotlist Hit and Review Hits screen in Patroller, appears in that color.
- **Use wildcards. :** Indicates that the hotlist contains wildcards (partial license plate numbers). You can have a maximum of two wildcard characters (asterisk *) in a PlateNumber. Wildcard hotlists are used in situations where witnesses did not see, or cannot remember a complete license plate number. This allows the officer to potentially intercept vehicles associated with a crime, which otherwise would not have been detected using standard hotlists.
- **Covert:** Set the hotlist to a *covert hotlist*. When you choose this setting, Patroller users are not alerted when a hit occurs. Only users with sufficient privileges can view *covert hits* in Security Desk.
- **Email address:** Email address that receives a notification when the hotlist you're configuring generates a hit.
- **Sound file:** The sound that Patroller plays when a hotlist hit occurs. If you leave this field blank, Patroller plays its default sounds. The path (you must include the filename) indicates the file's location on the Patroller in-vehicle computer.
- **Override privacy for emails:** Bypasses any privacy settings you applied at the Directory level, and sends an email with real LPR data to the email address you specified for this particular hotlist.
- **Disable periodic transfer:** Turns off periodic transfer of hotlist modifications to the Patroller computer. When this setting is off, hotlist changes are only downloaded to Patroller when the user logs on to the application. This option requires a wireless connection between Patroller and Security Center.

- **Enable transfer on modification:** Transfer hotlist modifications to Patroller as soon as they occur. For example, you can use this option on a hotlist to force Patroller to query for changes more frequently than the periodic transfer period (which applies to all hotlists). This can be useful for Amber alerts because they can be added to a specific hotlist and sent to a Patroller almost immediately. This option requires a continuous wireless connection between Patroller and Security Center.

I/O zone - Properties tab

On the I/O zone **Properties** tab, you can configure the inputs that define this zone, and the output relays that should be triggered, along with the desired output behavior, when the zone state be armed and active.

- **Maintenance:** Switch to **ON** to set the zone in maintenance mode. While in maintenance mode, the zone is disarmed and reverts to *Normal* state. No events are generated, and no output behaviors are triggered during this time, not even the *Trouble* event.
- **Arming schedule:** Select the schedules corresponding to the periods when the zone is armed.
- **Exceptions:** Select the schedules corresponding to the periods when the zone is not armed. The exception schedules take precedence over the arming schedules.
- **Master unit:** Shows the Synergis™ unit that is selected at the creation of the zone to do I/O linking. The I/O zone stops working if the master unit is down.
- **Inputs:** Select the inputs that must be combined to evaluate the zone state. The inputs can belong to different Synergis™ units, but all units must be under the same Access Manager.

  IMPORTANT: If the inputs do not belong to the same Synergis™ unit, you must select the **Enable peer to peer** option in the Access Manager.
- **Outputs:** Select the output relays you want to send the configured output behavior to, when the zone is armed and in the *Active* state. The zone can also be configured to trigger the outputs when the zone is in the *Trouble* state, regardless whether the zone is armed or not. The output relays can belong to different Synergis™ units, as long as the units are all under the same Access Manager.

  IMPORTANT: If the output relays do not belong to the same Synergis™ unit, you must select the **Enable peer to peer** option in the Access Manager.

  BEST PRACTICE: As much as possible, use the output relays on the master unit. This allows the I/O zone to continue to function when one or more slave units are down.
- **Output behavior:** Select the output behavior to send to the output relays.
- **Activate output on trouble when the zone is disarmed:** Select this option to always trigger the events and the output relays when the zone is in the *Trouble* state, regardless whether the zone is armed or not.
- **Revert to:** Select the output behavior to send to the output relays when the zone returns to the *Normal* state.
- **Associated events:** Events representing the zone states. Select *None* if a zone state should be ignored.
  - **Normal state:** When the combination of inputs yields a zero (0).
  - **Active state:** When the combination of inputs yields a one (1).
  - **Trouble state:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.
  - **Reactivation threshold:** The time period during which the same event should not be re-triggered.

Intrusion detection area - Properties tab

This section lists the settings found in the Intrusion detection area **Properties** tab, in the*Area view* task.

In the *Properties* tab, you can view the properties of the intrusion detection area as configured on the *intrusion detection unit*.

NOTE: This page is read-only for intrusion detection areas (zones) configured on Bosch units.

- **Physical name:** Name of the intrusion detection area (sometimes called a zone or partition) as it is configured on the physical intrusion panel. Changing the entity name of the intrusion detection area does not change its physical name.
- **Intrusion detection unit:** Entity name of the intrusion detection unit (intrusion panel) where this area is configured.
- **Devices:** Name and description of the inputs that define this intrusion detection area.

Intrusion detection unit configuration tabs

This section lists the settings found in Intrusion detection unit configuration tabs, in the *Intrusion detection* task.

Intrusion detection unit - Properties tab

In the *Properties* tab, you can configure the hardware-specific options for this unit.

- **Clear logs after download is completed:** Erase the log from the intrusion panel once it is downloaded to Security Center.
- **Interface type:** The interface type cannot be changed after the entity is created. If you need to change the interface type, you need to delete the entity and re-create it.
  - **Host (IPv4 interface only):** Host name or IP address of the intrusion panel.
  - **Port:** Connection port number of the intrusion panel.
- **Automatic synchronization:** Select this option of you want the clock on the intrusion panel to be synchronized with Security Center.
- **Synchronize now:** Synchronize the intrusion panel with Security Center now.

Intrusion detection unit - Peripherals tab

In the *Peripherals* tab, you can view the peripherals (inputs pins and output relays) connected to the intrusion detection unit.

- **Name:** Name given to the I/O device in Security Center.
- **Physical name:** Physical name of the device.
- **Logical ID:** Logical ID given to the device in Security Center.
- **Description:** Description given to the device in Security Center.
- **Input type (inputs only):** Type of input, as configured on the intrusion panel.
  - **Undefined:** The input does not have a set type. If you select this option, the input is considered as a *Perimeter* input type.
  - **Perimeter:** The input monitors the perimeter of an intrusion detection area.
  - **Interior:** The input monitors inside the intrusion detection area.
- **Contact type (inputs only):** Default contact state.
  - **Normally option:** The normal contact state of the input is open.
  - **Normally closed:** The normal contact state of the input is closed.

LPR unit - Properties tab

This section lists the settings found in the LPR unit **Properties** tab, in the *LPR* task.

In the *Properties* tab, you can view hardware and software information about the Sharp unit, such as the IP address and port being used. You can also associate a specific hotlist to the Sharp, or link the LPR camera in the Sharp to an *Omnicast* camera, or the Sharp's own context camera.

- **Properties:** Displays hardware and software information about the Sharp unit:
  - **IP address:** IP address of the Sharp unit.
  - **Port:** Port used by the *LPR Manager* to communicate with the Sharp unit.
  - **Version:** AutoVu *PlateReaderServer* software version running on the unit.
  - **Type:** Unit hardware version.
  - **Serial number:** Unit factory installed serial number.
  - **Updater Service version:** Displays the Updater service version running on the Sharp.
  - **Firmware version:** Displays the firmware version running on the Sharp.
- **Network configuration (Fixed Sharps only):**
  - **IP address:** The IP address of the fixed Sharp. The LPR Manager searches for the Sharp unit at this IP address.
  - **Assignment:** How the Sharp unit was enrolled in Security Center:
    - **Passive:** The LPR Manager discovered the Sharp unit on the network using the discovery port.
    - **Active:** The Sharp was added manually in Security Center Config Tool.
  - **Port:** Port used by the *LPR Manager* to communicate with the fixed Sharp unit.
- **Devices:** Link the LPR camera to an Omnicast™ camera.
- **File association:** Select how the Sharp behaves with hotlists:
  - **Inherit from LPR Manager role:** The Sharp uses the hotlists associated with its parent LPR Manager. This is the default setting.
  - **Specific:** Associate specific hotlists with the Sharp unit. This allows you to create Event-to-actions in Security Desk that trigger on that specific hotlist. For example, if you’re using the Sharp to allow access to a parking lot, you would put the vehicle plates on a hotlist, and then associate that hotlist to the Sharp.

NOTE: To reboot a fixed Sharp, click the *Reboot* button found in the toolbar at the bottom of the Config Tool workspace. If the Reboot button is not visible, log on to the Sharp Portals’s Configuration page, and then select *Accept remote reboot requests*. For more information, see the *Sharp Administrator Guide*.

Macro configuration tabs

This section lists the settings found in Macro configuration tabs, in the *System* task.

Macro - Properties tab

In the *Properties* tab, you can write your C# code using a basic text editor.

- **Import from file:** Click this button to import the source code from a file.
- **Checking syntax:** Click this button to validate the C# code. If errors are found in the code, they are listed in a dialog box with the line and column numbers where they are found.

Marco - Default execution context tab

In the *Default execution context* tab, you can view the context variables (input parameters) defined in your macro.

Monitor group - Monitors tab

This section lists the settings found in the Monitor group **Monitors** tab, in the *Alarm* task.

In the *Monitors* tab, you can add multiple analog monitors to the monitor group. Later, when you create alarms, you can add a monitor group and its members as a recipient of the alarm.

Network - Properties tab

This section lists the settings found in the Network **Properties** tab, in the *Network view* task.

In the *Properties* tab, you can define the network characteristics and routing information.

- **Capabilities:** Data transmission capabilities for streaming live video on the network.
  - **Unicast TCP:** Unicast (one-to-one) communication using TCP protocol is the most common mode of communication. It is supported by all IP networks, but it is also the least efficient method for transmitting video.
    IMPORTANT: Using TCP connection with secure communication (RTSP over TLS) has a significant impact on the performance of live video redirection (it doubles the CPU usage).
  - **Unicast UDP:** Unicast (one-to-one) communication using UDP protocol. Because UDP is a connectionless protocol, it works better for live video transmission. When the network traffic is busy, UDP is much less likely to cause choppy video than TCP. A network that supports unicast UDP necessarily supports unicast TCP.
  - **Multicast:** Multicast is the most efficient transmission method for live video. It allows a video stream to be transmitted once over the network to be received by as many destinations as necessary. The gain could be very significant if there are many destinations. A network supporting multicast necessarily supports unicast UDP and unicast TCP.
    NOTE: Multicast requires specialized routers and switches. Make sure you confirm this with your IT department before setting the capabilities to multicast.
- **IPv4 address prefix:** *IPv4* has two display modes. Click 👁 to select the preferred display mode.
  - **Subnet display:** This mode displays the IPv4 subnet mask as four bytes.
  - **CIDR block display:** The Classless Inter-Domain Routing (CDIR) mode displays the IPv4 subnet mask as a number of bits.
- **IPv6 address prefix:** Version 6 IP address prefix for your network. Your network must support *IPv6* and you must enable the option *Use IPv6* on all your servers using Server Admin.
- **Public servers:** You only need to specify the proxy server when *Network Address Translation* (NAT) is used between your configured networks. The proxy server must be a server known to your system and must have a public port and address configured on your firewall.
- **Routes:** Lists the routes between every two networks on your system, and the route capabilities.

Related Topics
Server - Properties tab on page 841

Output behavior - Properties tab

This section lists the settings found in the Output behavior **Properties** tab, in the *System* task.

In the *Properties* tab, you can configure the output signal pattern.

- **Output type:** Choose the output type.
    - **State:** Sets the circuit's state to open or closed.
    - **Pulse:** Sets a pulse to be generated.
    - **Periodic:** Sets a cyclic output to be generated.
- **Delay:** The delay before the pulse or periodic output is generated.
- **Duration:** The duration (in milliseconds) of the pulse.
- **Infinite:** Select this option if the periodic behavior should continue until it is told to stop by another output behavior.
- **Duty cycle:** The ratio of the output signal pattern pulse width divided by the period.
- **Period:** The time for one complete cycle of the output signal pattern.

Overtime rule configuration tabs

This section lists the settings found in Overtime rule configuration tabs, in the *LPR* task.

Overtime rule - Properties tab

In the *Properties* tab, you can configure the parking regulations enforced by this overtime rule.

- **Color:** Assign a color to the overtime rule. When you select the overtime rule in Patroller, the plate reads on the map, and the hit screen, are displayed in this color.
- **Vehicle parking position:** This setting tells the Patroller which set of calibrated parameters to use for the optimal reading of wheel images, based on the parking position of the vehicles: Parallel or Angled (45-degree).
- **Long term overtime:** Use this option for long term parking, where vehicles can park in the same spot for over 24 hours. When Long term overtime is selected, the parking time limit is specified in days (2 to 5 days).
- **Parking enforcement:** Type of restricted parking area that applies to the time limit:
  - **Same position.:** A vehicle is parked overtime if it parks in the same spot beyond the time limit specified.
  - **District:** A vehicle is parked overtime if it is parked anywhere within a city district (a geographical area) beyond the specified time limit.
  - **Block face (2 sides):** A vehicle is parked overtime if it is parked on both sides of a road between two intersections beyond the specified time limit.
- **Regulation:** Defines parameters of the parking time limit:
  - **Time limit:** Enter how long in hours and minutes a vehicle is allowed to park.
  - **Grace period:** Add extra time beyond the *Time limit* before raising an overtime hit. For example, if you set a 10 minute time limit, and a 5 minute grace period, Patroller will raise a hit after 15 minutes.
  - **Applicable days:** Select which days to enforce the *Time limit*.
  - **Applicable hours:** Select what time of day to enforce the *Time limit*.

Overtime rule - Parking lot tab

In the *Parking lot* tab, you can the *parking zone* where this parking rule must be enforced. The Parking lot tab displays a map, on which you can add a parking lot, define the number of spaces in the lot, and then draw a polygon on top of the map to represent the physical parking lot. The number of spaces in the lot is used to calculate the percentage of parking occupancy in that area. For more information on how this information is being used in the *Zone occupancy* report, see the *Security Desk User Guide*.

NOTE: You can add multiple lots to a map.

Parking facility - Properties tab

This section lists the settings found in the Parking facility **Properties** tab, in the *LPR* task.

In the *Properties* tab, you can assign an LPR Manager to the parking facility and configure its sectors and rows for the license plate collection route.

- **AutoVu™ LPR Manager:** Select the LPR Manager responsible for creating and managing the *license plate inventory* for this parking facility. Only offloads from MLPI Patrollers managed by the same LPR Manager are used to build the inventory for this parking facility.
- **Configuration:** List of sectors, rows, and space count of the parking facility.
- **Route:** License plate collection route followed by the MLPI units responsible for collecting the license plates for the inventory. The route is downloaded by the Patrollers and handheld devices assigned to this parking facility.

Partition - Properties tab

This section lists the settings found in the Partition **Properties** tab, in the *User management* task.

In the *Properties* tab, you can view and manage the partition content.

- **Members:** List of members that are part of the partition.
- **Show:** Filter the members list by entity type.
- **Global partition:** Turn this option on to share the partition with other independent Security Center systems (using Global cardholder management).

  NOTE: You cannot share the *root* partition.

Patroller - Properties tab

This section lists the settings found in the Patroller **Properties** tab, in the *LPR* task.

In the *Properties* tab, you can view information about the computer hosting the Patroller entity (you cannot edit the Patroller properties). You can also configure sound management, acknowledgment buffer settings, and a hit delay for the Patroller unit.

- **Properties:** Lists the properties of the Patroller in-vehicle computer.
    - **IP address:** IP address of the Patroller computer.
    - **Version:** Version number of the Patroller application.
    - **Type:** Patroller installation type(s).
    - **Serial number.:** Serial number of the Patroller.
    - **Machine name:** Name of the Patroller computer.
    - **Updater Service version:** Displays the updater service version running on the Patroller computer.
- **File association:** Select how the Patroller behaves with hotlists and/or permit lists:
    - **Inherit from LPR Manager role:** Patroller uses the hotlists and permit lists associated with its parent LPR Manager. This is the default setting.
    - **Specific:** Associate specific hotlists or permit lists with the Patroller unit rather than the LPR Manager. If you later want to move the Patroller entity to another LPR Manager on your system, the hotlist or permit list will follow.
- **Sound management:** Configure Patroller to play a sound when reading a plate and/or generating a hit, and choose whether sounds should be played even when Patroller is minimized.
    - **Play sound on hit:** Plays a sound when Patroller generates a hit.
    - **Play sound on read:** Plays a sound when Patroller reads a plate.
    - **Play sounds even when minimized:** Play sounds even if the Patroller window is minimized.
- **Acknowledgment buffer:** Specify a buffer restriction that limits how many hits can remain unacknowledged (not accepted or rejected) before Patroller starts automatically rejecting *all* subsequent hits. You can also choose (by priority) which hotlists should comply with this restriction.
    - **Reject count:** How many unacknowledged hits are allowed.
    - **Reject priority:** When you create a hotlist entity, you can specify a priority for that hotlist. This setting tells Patroller which hotlist(s) should comply with the buffer restriction.
- **Hotlist and permit:** Specify the *Duplicate hit delay* that tells Patroller to disregard multiple hits on the same plate for the duration of the delay. For example, if you set a delay of 10 minutes, no matter how many times Patroller reads the same plate during those 10 minutes, it will generate only one hit.

Permit - Properties tab

This section lists the settings found in the Permit **Properties** tab, in the *LPR* task.

In the *Properties* tab, you can configure the parsing of the source permit data file.

- **Path:** Path to the permit source text file that contains the permit data, such as license plate numbers and other related vehicle information. The source text file can be located on the LPR Manager computer's local drive (for example, the C drive), or on a network drive that is accessible from the LPR Manager computer.
- **Use delimiters:** Tells Security Center that the fields in the permit list file vary in length, and indicates the character used to separate each field in the file. By default, *Use delimiters* is set to *On*, and the delimiter specified is a *semi-colon* (;). If your permit list file is made up of fixed length fields, set *Use delimiters* to *Off*.
- **Visible in editor:** Allow a user to edit the hotlist or permit list using the Hotlist and permit editor task.
- **Attributes:** Tells Security Center the name and order of the fields (attributes) in the source text file.

Permit restriction configuration tabs

This section lists the settings found in Permit restriction configuration tabs, in the *LPR* task.

Permit restriction - Properties tab

In the *Properties* tab, you can configure the restrictions for the individual permits that apply to the parking zone represented by the rule.

- **Color:** Color used to represent the permit restriction in Security Desk. In Patroller, permit restrictions are always green for regular permit hits, or blue for shared permit hits. A read is displayed as a triangular-shaped icon in the selected color on the map, when an permit restriction is in effect. When a read violates one of the restrictions, the icon is encircled with a red ring. It indicates a permit hit.
- **Permits:** The permits the time restriction applies to.
  - ***Everyone***: Parking is available to everyone, regardless of whether they have a permit or not. No restriction is enforced during the specified time period. This restriction is used with other restrictions as a temporary override. For example, if a university is hosting a football game, parking would be made available to everyone during the game instead of specific permit holders.
  - ***No permit***: Only vehicles without permits can park. For example, you can use this type of restriction to reserve a zone for visitors parking. A plate read that matches any of the permits downloaded to the Patroller raises a hit.
  - ***All permits***: Only vehicles with a permit can park. A plate read that does not match any of the permits downloaded to the Patroller raises a hit.
  - ***Specific permits***: Only vehicles having one or more of the specified permits can park. A plate read that does not match any of the specified permits raises a hit.
- **Days:** Days of the week when parking is allowed.
- **Hours:** Time during the day when parking is allowed.
- **Validity:** Dates when parking is allowed.

Permit restriction - Parking lot tab

In the *Parking lot* tab, you can the *parking zone* where this parking rule must be enforced. The Parking lot tab displays a map, on which you can add a parking lot, define the number of spaces in the lot, and then draw a polygon on top of the map to represent the physical parking lot. The number of spaces in the lot is used to calculate the percentage of parking occupancy in that area. For more information on how this information is being used in the *Zone occupancy* report, see the *Security Desk User Guide*.

NOTE: You can add multiple lots to a map.

Schedule - Properties tab

This section lists the settings found in the Schedule **Properties** tab, in the *System* task.

The *Properties* tab lets you configure the time constraints that define the schedule.

Date coverage

In the *Date coverage* section, you can define a date pattern or specific dates to be covered by the schedule.

- **Daily:** Defines a pattern that repeats every day.
- **Weekly:** Defines a pattern that repeats every week. Each day of the week can have a different time coverage. This option is not available for twilight schedules.
- **Ordinal:** Defines a series of patterns that repeat on a monthly or yearly basis. Each date pattern can have a different time coverage. For example, on July 1st every year, on the first Sunday of every month, or on the last Friday of October every year.
- **Specific:** Defines a list of specific dates in the future. Each date can have a different time coverage. This option is ideal for special events that occur only once.

Time coverage

In the *Time coverage* section, you can define which time periods apply during a 24-hour day.

- **All day:** Covers the entire day. This option is not available for twilight schedules.
- **Range:** Covers one or multiple discrete time periods within the day. For example, from 9 a.m. to 12 p.m. and from 1 p.m. to 5 p.m. This option is not available for twilight schedules.
- **Daytime:** Covers from sunrise to sunset. This option is only available for twilight schedules.
- **Nighttime:** Covers from sunset to sunrise. This option is only available for twilight schedules.

Scheduled task - Properties tab

This section lists the settings found in the Scheduled task **Properties** tab, in the *System* task.

In the *Properties* tab, you can configure the scheduled task's behavior.

- **Status:** Turn the scheduled task on or off.
    - **Recurrence:** Specifies how often the scheduled task occurs.
    - **Once:** Executed once at a specific date and time.
    - **Every minute:** Executed every minute.
    - **Hourly:** Executed at a specific minute of every hour.
    - **Daily:** Executed at a specific time every day.
    - **Weekly:** Executed at a specific time on selected days of the week.
    - **On startup:** Executed on system startup.
    - **Interval:** Executed at regular intervals that can be days, hours, minutes, or seconds.
- **Action:** Action to be executed on the schedule.
- **Additional parameters:** Additional information required, depending on the action type selected.

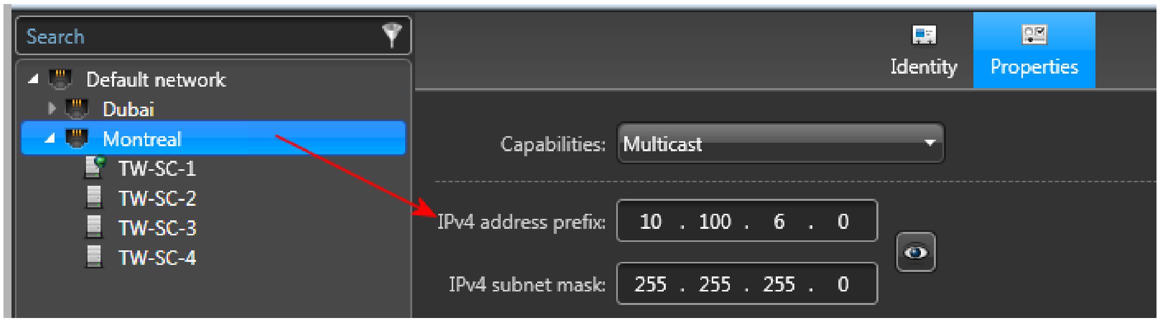
Server - Properties tab

On the server **Properties** tab, you can view the network settings configured for this server in Server Admin.

NOTE: All network settings are read-only in Config Tool. They must be configured in Server Admin, except when the server is running in backward compatibility mode (5.2 or earlier), in which case the network settings are configured inConfig Tool.

- **Public address:** Public address of this server. This setting appears only if a public address is configured in Server Admin.
  - **Port:** Port used by the Genetec Server service to listen to commands received from other Security Center servers on the public address.
  - **Proxy:** This switch is turned on if this server is configured as a proxy server for a private network protected by a firewall.
- **Private addresses:** List of *private IP addresses* used for the communication between Security Center servers. Only the private addresses enabled in Server Admin appear in this list.
  - **Port:** Port used by the Genetec Server service to listen to commands received from other Security Center servers on the private addresses.

  IMPORTANT: If the server is running in backward compatibility mode (5.2 or earlier), the first address in the private address list must match the IPv4 properties of the network entity the server belongs to in the Network view task.



Capabilities: Multicast

IPv4 address prefix: 10 . 100 . 6 . 0

IPv4 subnet mask: 255 . 255 . 255 . 0

- **Secure communication:** Use this section to view the current *identity certificate* used by the server to communicate with other Security Center servers.
  - **Issued to:** Subject of the current certificate. A *self-signed certificate* created at software installation appears in the form *GenetecServer-{MachineName}*.
  - **Issued by:** Name of the *certificate authority* that issued the certificate. The issuer and the subject are the same for self-signed certificates.
  - **Valid from/to:** Validity period of the current certificate.

  Click **View** to open the dialog box to view more information.

Related Topics

What is Transport Layer Security protocol? on page 307
Network - Properties tab on page 831
Server Admin - Overview page on page 83
Server Admin - Main server page on page 86
Server Admin - Expansion server page on page 89

Tile plugin - Properties tab

This section lists the settings found in the Tile plugin **Properties** tab, in the *Area view* task.

In the *Properties* tab, you can link the tile plugin entity to a website or a .dll file.

- **Web page:** Type a web address to link the tile plugin to.
- **Modify:** Select a .dll to link the tile plugin to.

User configuration tabs

This section lists the settings found in User configuration tabs, in the *User management* task.

User - Properties tab

In the *Properties* tab, you can configure the user's personal information and password.

- **Status:** Activate or deactivate the user profile. A user cannot log on when their profile is deactivated. Deactivating a user's profile while the user is logged on will immediately log off the user.
- **Personal information:** The personal information of a user can be imported from your company's directory service.
  - **First and last name:** First and last name of the user.
  - **Email address:** The email address of the user. Can be used to send emails, reports, or messages to the user.
- **Password settings:** All users require a password to log on to Security Center. The user must have the *Change own password* privilege for the password options to be enabled.
  - **Expires:** Turn this option on to force the user to change their password after a given number of days.
  - **Change on next logon:** Turn this option on for Patroller or Security Desk to force the user to change their password the next time they log on.
  - **Change password:** Only administrators can change the password of other users.
- **User level:** Set the *user level*. Level 1 is the highest user level, with the most privileges.
  - **Inherit from parent:** The user level can be inherited from a parent group. If the user has multiple parents, the highest user level is inherited. If the user has no parent group, the lowest user level (254) is inherited. You must set *Inherit from parent* option to *Override* in order to change this setting.
  - **Configure PTZ overrides:** Set different user level values for selected PTZ cameras. The override values allow you to give this user higher or lower priority over certain PTZ cameras.

User - Access rights tab

In the *Access rights* tab, you can view and configure the user's access rights over *partitions*. This tab only appears when user-created partitions exist in the system.

- **List of partitions:** Select a partition to grant access rights for that partition to the user. Access rights over parent and child partitions can be configured independently. Access rights inherited from parent user groups cannot be revoked.
- **Administrator:** Select this option to grant full administrative rights over all entities contained in that partition to the user, including the rights to create and delete users, user groups, and child partitions.
- **Display checked items (▽):** Click to toggle the display between showing only selected partitions and all partitions.

User - Privileges tab

In the *Privileges* tab, you can view and configure the user's privileges. The privileges of a user can be inherited inherited from parent user groups.

- **Allow:** The privilege is granted to the user.
- **Deny:** The privilege is denied to the user.

- **Undefined:** This privilege must be inherited from a parent user group. If the user is not a member of any group, or if the privilege is also undefined to the parent user group, then the privilege is denied.
- **Exceptions:** Basic privileges can be superceded at the partition level if the user is authorized to access multiple partitions. Only *Administrative*, *Task*, and *Action privileges* can be overwritten at the partition level.
- **Additional settings (⚙):** Click to view additional commands for privilege templates.
  - **Apply template:** Select one of the privilege templates to apply.
  - **Set configuration to read-only:** Set all entity configuration privileges found under the *Administrative privileges* group to *View properties*.
  - **Set configuration to read-write:** Allow the modification of all entity configurations, including *Add* and *Delete*.

User - Advanced tab

In the *Advanced* tab, you can configure the user’s advanced settings.

- **Logon settings:** Configure the user’s logon settings.
  - **User logon schedule:** Restrict the user logon according to schedules. A schedule can either be used to allow user logon or to block user logon.
  - **Logon supervisor of:** Lists the users whose logons are supervised by this current user. When a user in this list needs to log on to the system, the current user must also provide their username and password to complete the logon. A user can have more than one logon supervisor.
  - **Limit concurrent logons:** Set the maximum number of different workstations a user can log on to at the same time. This limit only applies to Security Desk. Config Tool is not restricted by this setting.
  - **Auto-lock:** Turn this option to on to lock the user out of their Security Desk workstation after a period of inactivity. To use the application again, the user must re-enter their password. This requirement can be inherited from a parent user group. You must set *Inherit from parent* to *Override* in order to change this setting.
- **Security Desk settings:** Configure the user’s Security Desk workspace.
  - **List of active tasks:** Displays the tasks found in the user’s active task list.
  - **Hot actions:** Displays the *hot actions* mapped to the PC keyboard function keys (Ctrl+F1 through Ctrl +F12) when this user is logged on to Security Center using Security Desk.
  - **Allow remote control over:** Lists the Security Desk workstations this user is allowed to control remotely using the *Remote* task in Security Desk, or a CCTV keyboard. You can specify which workstations can be controlled by user, user group, or by specific workstation.
  - **Start task cylcing on logon:** Turn this option on so that next time the user logs on from Security Desk *task cycling* starts automatically.
- **Security settings:** Configure what the user can see in the system.
  - **Limit archive viewing:** Turn this option on to restrict the user's ability to view archived video to the last *n* days. This limitation can be inherited from a parent user group. If the user has multiple parents, the most restrictive limitation is inherited. If the user has no parent group, no restriction will be imposed. You must set *Inherit from parent* to *Override* in order to change this setting.
  - **Scramble entity names:** (Only non-administrative users) Turn this option on to display the entity GUID in Security Desk and Config Tool, everywhere the entity name is supposed to be displayed for this user. This option also prevents the user from updating the entity name fields in Config Tool.
- **Default map:** The map loaded by default when the user opens the *Maps* task. If none is defined, the global default map configured at the Map Manager role level is used.

User group configuration tabs

This section lists the settings found in User group configuration tabs, in the *User management* task.

User group - Properties tab

In the *Properties* tab, you can view and configure the members of the user group.

- **Email address:** Email address that is used by all members of the group. This information can be imported from your company's directory service. The email address can be used to send emails, reports, or messages to the users.
- **User level:** Set the *user level*. Level 1 is the highest user level, with the most privileges.
  - **Inherit from parent:** The user level can be inherited from a parent group. If the user has multiple parents, the highest user level is inherited. If the user group has no parent group, the lowest user level (254) is inherited. You must set *Inherit from parent* option to *Override* in order to change this setting.
  - **Configure PTZ overrides:** Set different user level values for selected PTZ cameras. The override values allow you to give this user group higher or lower priority over certain PTZ cameras.
- **Members:** List of user group members. By default, the members inherit the privileges and partition rights of the user group.

User group - Access rights tab

In the *Access rights* tab, you can view and configure the access rights shared by the members of the user group. This tab only appears when user-created partitions exist in the system.

- **List of partitions:** Select a partition to grant access rights for that partition to the user group. Access rights over parent and child partitions can be configured independently. Access rights inherited from parent user groups cannot be revoked.
- **Administrator:** Select this option to grant full administrative rights over all entities contained in that partition to the user group, including the rights to create and delete users, user groups, and child partitions.
- **Display checked items (▼):** Click to toggle the display between showing only selected partitions and all partitions.

User group - Privileges tab

In the *Privileges* tab, you can view and configure the user group's privileges. The privileges of a user group can be inherited by the members of the group, or can be inherited from other user groups.

- **Allow:** The privilege is granted to the user group.
- **Deny:** The privilege is denied to the user group.
- **Undefined:** This privilege must be inherited from a parent user group. If the user group is not a member of any other group, or if the privilege is also undefined to the parent user group, then the privilege is denied.
- **Exceptions:** Basic privileges can be superceded at the partition level if the user group is authorized to access multiple partitions. Only *Administrative*, *Task*, and *Action privileges* can be overwritten at the partition level.
- **Additional settings (⚙):** Click to view additional commands for privilege templates.
  - **Apply template:** Select one of the privilege templates to apply.

  - **Set configuration to read-only:** Set all entity configuration privileges found under the *Administrative privileges* group to *View properties*.
  - **Set configuration to read-write:** Allow the modification of all entity configurations, including *Add* and *Delete*.

User group - Advanced tab

In the *Advanced* tab, you can configure common advanced settings for the group members.

- **Logon settings:** Configure the common logon settings for the group members.
  - **Logon supervisor of:** Lists the users whose logons are supervised by the members of this user group. When users from this list need to log on to the system, any member of this user group can help them complete their logon.
  - **Auto-lock:** Turn this option on to lock the members of this user group out of their Security Desk workstation after a period of inactivity. To use the application again, the users must reenter their password. This requirement can be inherited from a parent user group. You must set *Inherit from parent* to *Override* in order to change this setting.
- **Security Desk settings:** Configure the common Security Desk settings for the group members.
  - **Allow remote control over:** Lists the Security Desk workstations the members of this user group are allowed to control remotely using the *Remote* task inSecurity Desk, or a CCTV keyboard. You can specify which workstations can be controlled by user, user group, or by specific workstation.
- **Limit archive viewing:** Turn this option on to restrict the user group's ability to view archived video to the last *n* days. This limitation can be inherited from a parent user group. If the user group has multiple parents, the most restrictive limitation is inherited. If the user group has no parent group, no restriction will be imposed. You must set *Inherit from parent* to *Override* in order to change this setting.

Video unit - Identity tab

This section lists the settings found in the Video unit **Identity** tab, in the *Video* task.

In the *Identity* tab, you can view hardware-specific information, in addition to the standard entity information (name, description, logical ID, and so on).

- **Manufacturer:** Manufacturer of the video unit.
- **Product type:** Model of the video unit.
- **Firmware version:** Current firmware version installed on the video unit.
- **Upgrade (☢):** Upgrade the firmware on the video unit.
- **Audio:** Indicates whether the video unit supports audio.
- **SSL:** Indicates whether the video unit supports *SSL* (Secure Socket Layer protocol).

Video unit - Properties tab

This section lists the settings found in the Video unit **Properties** tab, in the *Video* task.

In the *Properties* tab, you can configure the information required by the Archiver to connect to this unit and other data transmission properties. These settings vary from one manufacturer to another. Additional options might be available, depending on the unit type.

- **IP address:** Set the IP address of the video unit.
- **Obtain network settings dynamically (DHCP):** Select this option to have the IP address assigned dynamically by your DHCP (Dynamic Host Configuration Protocol) server.

  NOTE: Do not use this option unless your DHCP server is configured to always assign the same IP address to the same device.
- **Specific settings:** Select this option to enter a fixed address. This is the IP address you entered when you initially created the video unit entity. You need to enter the following fields:
  - *Local IP*. Fixed IP address.
  - *Subnet mask*. The subnet mask tells the unit which peripherals it can communicate with directly. Anything that does not belong to the same subnet must go through the Gateway.
  - *Gateway*. IP address of the gateway. It must be on the same subnet as the unit.
- **Command port:** The port used by the Archiver to connect to the video unit. The command port is sometimes called the HTTP port by some manufacturers.
- **Discovery port:** The port used for automatic discovery. Not all manufacturers supports this feature.
- **VSIP port:** (Only for Verint units) On Verint units, both the command port and discovery port are replaced by the *VSIP port*.
- **Authentication:** Credentials used by the Archiver to connect to the video unit.
  - **Default login:** Select this option for the Archiver to use the credentials defined in the unit manufacturer’s extension.
  - **Specific:** Select this option for the Archiver to use specific credentials to connect to this unit. The fields you need to fill in depend on the unit manufacturer.
  - **Use secure communication:** Select this option to use *HTTPS* communication instead of HTTP (default).
- **Bit rate:** Use this option to limit the maximum bit rate allowed for this unit. Setting a limit to the bit rate helps prevent one unit from using up all the bandwidth available on the network.
- **Enable UPnP:** Select this option to enable the UPnP (Universal Plug and Play) protocol. Disable UPnP if you do not want the unit to be discovered by other Windows applications.
- **Enable Bonjour:** Select this option to enable the Bonjour protocol. Disable Bonjour if you are not using zero-configuration networking.
- **Enable link-local address:** Select this option to enable the use of link-local address.
- **Event stream connection type:** Select the connection type (HTTP or TCP) used for sending events. The use of TCP is recommended. Select HTTP if there is a firewall between the Archiver and the unit.
- **Camera applications:** (Axis only) List of ACAP applications installed on the unit. Select the ones you want to enable.

  NOTE: To enable AXIS Video Motion Detection, you must do it from the Camera’s **Motion detection** tab, and select **Use camera application motion detection**.

Video unit - Peripherals tab

This section lists the settings found in the Video unit **Peripherals** tab, in the *Video* task.

In the *Peripherals* tab, you can view all the peripheral devices (inputs/outputs, audio encoders/decoders) found on the unit that are not explicitly shown as entities, such as the *video encoders* or *video decoders*.

- **Peripheral State (LED):**
  - Green (🟢): Active peripheral.
  - Red (🔴): Peripheral disabled by user.
  - Yellow (🟡): Peripheral activation in progress.
    NOTE: If the LED stays yellow, it indicates that the peripheral is either not supported or has problems, in which case it is recommended to disable it.
- **Name:** Logical name. It is the same as the physical name by default.
- **Logical ID:** Logical identifier.
- **Description:** Description of the device.

You can also modify the selected peripheral devices.

- **Edit the item (✏):** Change the settings of the selected peripheral device.
- **Enable/Disable selected items (🟢/🔴):** Enable or disable the selected peripheral devices.

Output relay settings

The setting specific to output relays is as follows:

- **Default mode:** Default state of the output relay.
  - **Normally option:** The normal contact state of the output is open.
  - **Normally closed:** The normal contact state of the output is closed.

Speaker settings

The settings specific to speakers (*audio decoder* devices) are as follows:

- **Volume:** Desired volume level (0 to mute, 100 equals maximum volume).
- **UPD port:** Port number used when the connection type is unicast UDP.
- **Connection type:** Connection type that is used between the unit and the Archiver for this audio decoder.

Microphone settings

The settings specific to microphones (*audio encoder* devices) are as follows:

- **Data format:** Audio compression format.
- **Input type:** Type of input source.
  - **Line in:** Used for pre-amplified source.
  - **Mic in:** Use this if the microphone is directly connected to the unit. In this case, the signal is amplified by the hardware.
  - **Internal:** Use microphones integrated to the unit.

- **Sensitivity:** Desired amplification level (default=68). The lower the level, the less sensitive the microphone is to ambient noise, but the recording level will also be lower.
- **UDP port:** Port number used when the connection type is unicast UDP.
- **Connection type:** Connection type that is used between the unit and the Archiver for this audio encoder.
- **Multicast address:** The *multicast* address and *port number* are assigned automatically by the system when the video unit is discovered. Each audio encoder is assigned a different multicast address with a fixed port number. This is the most efficient configuration.

Virtual zone configuration tabs

Virtual zones are controlled by the *Zone Manager* role. Virtual zones are used to combine inputs and trigger outputs that belong to different units of different types. Virtual zones can be armed and disarmed from Security Desk or using *Arm zone* and *Disarm zone* actions.

Virtual zone - Properties tab

Click the **Properties** tab to configure the inputs that define this zone, and define how they are evaluated.

- **Zone Manager:** Zone Manager role that controls the virtual zone.
- **Inputs:** Inputs combined to evaluate the zone state.
- **Operator:** Logical operator used to combine the input states to evaluate the zone state.
- **Associated events:** Events representing the zone states. Select *None* if a zone state should be ignored.
  - **Normal state:** When the combination of inputs yields a zero (0).
  - **Active state:** When the combination of inputs yields a one (1).
  - **Trouble state:** Requires to have at least one supervised input. The zone is in the *Trouble* state when at least one of the input is in the *Trouble* state. The *Trouble* state supersedes all other states.
  - **Reactivation threshold:** The time period during which the same event should not be re-triggered.

Virtual zone - Arming tab

Click the **Arming** tab to configure the arming source of your zone and its arming behavior.

- **Arming source:** Select the schedules corresponding to the periods when the zone is armed.
- **Delays:** Optional delays that give you time to leave the premises after arming the zone, and time to disarm the zone after tripping a sensor.
  - **Arming delay:** Duration (mm:ss) you want between the time the zone is armed and the time the event triggers become active.
  - **Entry delay:** Duration (mm:ss) you want between the time the entry sensor is tripped and the time the events are triggered. This option allows you to disarm the zone before triggering the output relays.

49

Role types

This section includes the following topics:

Access Manager configuration tabs

You configure the settings of the Access Manager role from the **Roles and units** view of the *Access control* task in Security Center Config Tool.

Access Manager - Properties tab

Click the **Properties** tab to configure the retention period of the access control events in the database.

- **Keep events:** Specify how long you want to keep access control events logged by the Access Manager in the database, before they are deleted.
- **Enable peer to peer:** Select this option to enable the communication between Synergis™ units managed by this Access Manager.

  BEST PRACTICE: Only enable peer to peer communication if you plan to create I/O zones that involve multiple Synergis™ units, or apply antipassback to areas controlled by multiple Synergis™ units. Leave this option off for better system security and performance.
- **Enable global antipassback:** Select this option if you need to apply antipassback to areas controlled by multiple Synergis™ units. To enable this option, you must first enable peer to peer.

  BEST PRACTICE: If all your antipassback areas are controlled by a single unit, do no enable global antipassback. Enabling global antipassback increases the communication between Synergis™ units.

Access Manager - Extensions tab

Click the **Extensions** tab to configure the manufacturer-specific connection parameters shared by access control units that are controlled by this Access Manager.

- **Genetec Synergis™:** Extension for all Synergis™ units. This extension requires at least one discovery port. For more information, see the *Synergis™ Appliance Configuration Guide*.
- **HID VertX:** Extension for all HID units, including the legacy VertX models (V1000 and V2000), the VertX EVO, and the Edge EVO controllers. For the complete list of supported controller units and firmware, see the *Security Center Release Notes*.

Access Manager - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role.
- **Database status:** Current status of the database.
- **Database server:** Server in which the role's database is located.
- **Database:** Name of the database instance.
- **Actions:** Maintenance functions you can perform on the role's database:
  - **Create a database (➕):** Create a new database.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (🔔):** Set up notifications for when the database space is running low.
  - **Backup/restore (▭):** Back up or restore the database.

Active Directory configuration tabs

You configure the settings of the Active Directory role from the **Roles** view of the *System* task in Security Center Config Tool.

Active Directory - Properties tab

Click the **Properties** tab to define the parameters for how the Active Directory role operates.

- **Connection status:** Connection status between the role and the corporate AD.
- **Status:** Shows what the role is doing. *Idle* is the normal status. If there is a problem, an error message is displayed.
- **Active Directory:** Hostname or *IP address* of the corporate AD server.
  - **Use Windows credentials:** You can use the Windows credentials used for running the *Genetec Server* service, or specify a different set of Windows usernames and passwords. In both cases, the credentials you specify must have read and write access to the specified corporate AD.
  - **Use SSL connection:** Select this option to encrypt LDAP (Lightweight Directory Access Protocol) network traffic. LDAP is the protocol used for communication between the Active Directory role and the AD. The default port used for encrypted communication is 636. If you use a different port, you need to explicitly specify it by appending the port number after the AD server name, separated by a colon (':').
  - **Use a specific domain controller:** Select this option and specify the name of your domain controller if you have one that is dedicated to Security Center.
- **Partition:** Default *partition* where the entities synchronized with the corporate AD are created if the partition is not mapped to an AD attribute.
- **Synchronized groups:** List of all AD security groups imported as user groups, cardholder groups, or both.
- **No scheduled task exists to synchronize this role. :** This warning message appears if you have not configured a scheduled task to automatically handle synchronization with the corporate AD.
- **Synchronize now. :** Synchronize with the Active Directory now. You should always synchronize after making changes to the synchronized groups.

Active Directory - Links tab

Click the **Links** tab to map AD attributes to Security Center fields.

- **Cardholder:** Map AD attributes to Security Center cardholder fields.
- **Upload pictures to Active Directory:** Select this option if you want the pictures you assign to imported cardholders from Security Center to be uploaded to the AD.
- **Maximum uploaded picture file size:** This parameter only appears if *Upload pictures to Active Directory* is selected. It servers to limit the file size of the pictures you upload from Security Center to the AD.
- **Card format:** Select the default card format to use for the imported cardholder credentials when the card format property is either not mapped to an AD attribute, or when the mapped attribute is empty.
- **Badge template:** Select a default badge template to use for the imported cardholder credentials.
- **Custom fields:** Map additional AD to Security Center custom fields.

Active Directory - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Active Directory role does not require a database.

- **Servers:** Servers hosting this role.

Active Directory Federation Services - Properties tab

In the **Properties** tab, you can configure your trust chain, and all the ADFS groups that you accept as Security Center user groups.

- **Trust chain (domains):** The trust chain defines the domain of your *root ADFS*, the ADFS server that the role is directly talking to, and the domains of remote ADFS servers that Security Center is receiving claims (*Group* and *UPN*) from, through the root ADFS.
- **Accepted user groups:** User groups corresponding to the ADFS groups that Security Center accepts. These user group names must match the name defined by the remote ADFS servers, followed by the ADFS domain name. For example: *operators@companyXYZ.com*.

Archiver: Camera default settings tab

You can use the **Camera default settings** tab to configure the default recording settings applied to all cameras that are controlled by the Archiver role.

The **Camera default settings** tab includes the following settings:

- **Video quality:** Select a **Resolution**.
  - **High:** 1270x720 and greater.
  - **Standard:** Between 320x240 and 1280x720.
  - **Low:** 320x240 and less.
  - **Default:** Manufacturer default settings.
  - **Frame rate:** You can select a value between 1 and 30 fps. Does not apply to default settings.
- **Recording:** From the **Recording modes** drop-down list, select one of the following recording modes:
  - **Continuous:** Records continuously. Recording cannot be stopped by the user (🔴🔒).
  - **On motion/Manual:** Records when triggered by an action (such as *Start recording*, *Add bookmark*, or *Trigger alarm*) through motion detection, or manually by a user. In this mode, the *Record* button in Security Desk appears grey (⚫) when the Archiver is not recording, red (🔴) when it is recording but can be stopped by the user, or red with a lock (🔴🔒) when it is recording but cannot be stopped by the user (on motion or alarm recording).
  - **Manual:** Records when triggered manually by a user. In this mode, the *Record* button in Security Desk appears grey (⚫) when the Archiver is not recording, red (🔴) when it is recording but can be stopped by the user, or red with a lock (🔴🔒) when it is recording but cannot be stopped by the user (on motion or alarm recording).
  - **Custom:** Recording is specified by a custom schedule. You can use the custom schedule that you created with the installer assistant, or click ➕ to add a new custom recording schedule that you created using the *System* task. For more information about creating schedules using the *System* task, see Creating schedules on page 169.
    CAUTION: Recording schedules of the same type (for example, two daily schedules) cannot overlap, regardless of the recording mode configured for each. When a scheduling conflict occurs, the Archiver and the video units are displayed in yellow in the entity browser and they issue entity warning messages.
  - **Off:** Recording is off (⚫🔒), even when an alarm is triggered.
  - **(Optional) Show advanced settings:** Click to configure advanced recording settings.
  - **Record audio:** Switch **ON** to record audio with your video. A microphone entity must be attached to your cameras. For more information, see Configuring camera settings on page 398.
  - **Record metadata:** Switch **ON** to record metadata with your video.
  - **Redundant Archiving:** Switch **ON** to allow primary, secondary, and tertiary servers to archive video at the same time. This setting is effective only if failover is configured. For more information, see Setting up Archiver role failover on page 162.
  - **Automatic cleanup:** Specify a retention period for recorded video (in days). Video archives older than this period are deleted.
  - **Time to record before an event:** Use the slider to set the number of seconds that are recorded before an event. This buffer is saved whenever the recording starts, ensuring that whatever prompted the recording is also captured on video.

  - **Time to record after a motion:** Use the slider to set the number of seconds that continue to be recorded after a motion event. During this time, the user cannot stop the recording.
  - **Default manual recording length:** Use the slider to select the number of minutes the recording lasts when it is started manually by a user, or when the *Start recording* action is triggered.
- **Encryption:** Switch **ON** to enable *fusion stream encryption* for all cameras managed by the selected Archiver. Only users who have one or more of the listed **Certificates** installed on their workstations can view video.

  NOTE: In order to enable **Encryption**, you must add at least one *encryption certificate* to the Archiver role. For more information, see What is fusion stream encryption? on page 346.

NOTE:

- Recording settings that are configured in the Security Center installer assistant are carried over to the **Camera default settings** tab.
- Recording settings defined on the **Recording** tab of an individual camera supersede the settings defined on the **Camera default settings** tab.

Archiver: Extensions tab

In the **Extensions** tab, you can configure the common connection parameters shared by the *video units* that are controlled by the selected Archiver. The *manufacturer extensions* are automatically created when you add a unit to the Archiver.

The *Extensions* tab includes the following settings:

- **Transaction timeout:** Time that is spent waiting for a response before re-sending a command to the unit. A unit is considered lost after three failed attempts.
- **Command port:** (Bosch only) Port used by the Archiver to send commands to the Bosch units. This field has default values that get reset every time the **Protocol** field is modified.
- **Protocol:** (Bosch only) Transport protocol used by the Archiver to send commands to the Bosch units.

  The accepted values are:

  - **RCP:** Use RCP+ over TCP (default). The command port must be set to 1756.
  - **HTTP:** Use HTTP or HTTPS (RCP+ over CGI).
    IMPORTANT: To enroll a Bosch unit using either HTTP or HTTPS, you must manually create the Bosch extension, or modify an existing one.
    - To use HTTP, set **Command port** to match the value of **HTTP browser port** configured on the Bosch unit.
    - To use HTTPS, set **Use HTTPS** to **On** under the *Default logon* group, and set **Port** to match the value of **HTTPS browser port** configured on the Bosch unit.

    NOTE: The command ports configured in the Bosch extension are default values. The values configured on the Bosch units might be different. The **Discovery port** must match the values configured on the Bosch units.
- **RSTP port:** RTSP (Real Time Streaming Protocol) port used by the Archiver to request video from the units that support this protocol.

  The RTSP port is used to listen for RTSP (Real Time Streaming Protocol) requests. When multiple archiving roles are hosted on the same server, this value must be unique for each one. The configured value cannot be the same as any value used for the Media Router role, its redirector agent, or any Auxiliary Archiver hosted on the same server.
- **VSIP port:** (Verint only) Port used for *automatic discovery*. All units that are controlled through the same Verint extension must be configured with the same *VSIP port*. All Verint extensions configured for the same Archiver must have different discovery ports.
- **Refuse basic authentication:** Use this switch to enable and disable basic authentication for a manufacturer extension. This is useful if you turned off basic authentication in the Security Center InstallShield, but need to turn it on again to use a camera that only supports basic authentication. To turn basic authentication on again, you must switch **Refuse basic authentication** to **Off**.
- **Discovery port:** Automatic discovery port. If multiple instances of the same type of extension are configured for the same Archiver, they must all use a different discovery port.

  - (ACTi) Corresponds to the *Search server port 1* in the ACTi video server settings.
  - (Bosch) All units that are controlled through the same Bosch extension must be configured with the same discovery port.

  NOTE: If you decide to change the *Discovery port* after the units are discovered, you must create a new extension with the new discovery port and delete the old one. If the units are not automatically discovered, you must add them manually.
- **Discovery reply port:** (ACTi and Interlogix) Corresponds to the *Search server port 2* in the ACTi video server settings.

- **Unicast period:** Time period in which the extension repeats its connection tests using unicast to determine whether each unit is still active in the system.
- **Multicast period:** Time period in which the extension attempts to discover new units using multicast. This option can be disabled. The IP address that follows is the standard multicast IP address used by *Omnicast*. Change the standard multicast IP address only if it is already used for something else.
- **Broadcast period:** Time period in which the extension attempts to discover new units using broadcast. This option can be disabled.
- **Default logon:** Certain types of units can be protected by a username and a password against illegal access. The logon credentials can be defined individually for each unit or for all units using the same manufacturer extension.
  - **Username:** Certain types of units (such as Axis) require a username.
  - **Password:** Certain types of units (such as Bosch) require only a password.
  - **Use HTTPS:** Select this option to use *Secure Hypertext Transfer Protocol* for added security.
    NOTE: For Bosch units, this setting only appears when **Protocol** is set to **HTTP**. When **Use HTTPS** is set to **On**, the **Port** set here supercedes the **Command port**.
- **TCP notification port:** (Panasonic and Interlogix) Port used by the Archiver role to receive notifications from the units. When an event occurs, such as *Signal lost* or *Signal recovered*, the unit initiates a *TCP* connection with the Archiver and sends the notification through this port.
- **Notification channel:** (Interlogix only) When you configure multiple Archiver roles to listen to the same units, such as in a failover list, each Archiver must be identified with a different notification channel (1 to 8). You can ignore this parameter if you are using only one Archiver. For multiple Archiver roles, you must follow these rules:
  - All Archiver roles that control the same units must be configured with the same TCP notification port.
  - All Archiver roles must use a different notification channel.
- **Bosch VRM settings:** The VRM settings are exclusive to Bosch VRM (Video Recording Manager). These settings allow you to query and play back video from Bosch cameras that are managed by a Bosch VRM. Multiple Bosch extensions can use the same VRM. If you add more than one VRM to the list, you can use the move up (▲) and move down (▼) buttons to move a VRM up or down on the list. By default, the Archiver uses the first VRM on the list for queries and archived video. If the first VRM is not available, the Archiver uses the next VRM on the list.
- **Verint specific settings:** The following settings are found only on Verint units.
  - **Show all available video streams as separate cameras:** (Verint only) Omnicast™ supports encoders that generate multiple video streams from the same video source. When these encoders are discovered, the Archiver creates a *video encoder* with multiple streaming alternatives. Select this option to represent every video stream as a separate camera.
    NOTE: This option requires a camera connection license for each stream.
  - **SSL settings:** SSL (Secure Sockets Layer) is a protocol used to protect applications that need to communicate over a network. Security Center supports SSL on all message transmissions between the Archiver and the units, except for video streams because the volume of data is too high. The purpose for using SSL in Security Center is to prevent attacks, not to stop eavesdropping. Select *Enforce SSL* only if SSL must be enforced on all units controlled by this Archiver. If this option is cleared, the Archiver will use SSL only to communicate with the units on which SSL is enabled.
- **Advanced settings:** The advanced settings are reserved for use by Genetec™ Technical Assistance Center.
- **NTP settings:** Synchronizes the time between the units that support NTP (Network Time Protocol), and the NTP server. Keeping the units' time synchronized is particularly important for units that handle video archiving. You must set the following parameters:

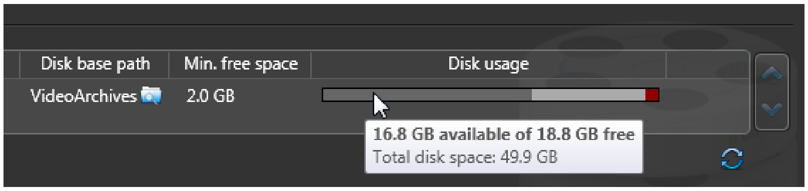
- **NTP server:** Specify the NTP server name.
- **NTP port:** Specify the NTP server port number.
- **Poll timeout:** Specify how often you want the time on the units to be checked to ensure that they are properly synchronized with the NTP server. For example, if 60 seconds is entered, the time is verified every 60 seconds.

Archiver: Resources tab

This section lists the settings found in the Archiver role **Resources** tab in the Video task.

Click the **Resources** tab to assign servers, databases, and disk storage to this Archiver role.

- **Server (⊕):** One of the servers hosting this Archiver role. You can assign a maximum of two servers to an Archiver role for failover purposes using the tabs at the bottom of the page.
  - **Network card:** Network card used to communicate with all video units.
  - **RTSP port:** Port used to listen for RTSP (Real Time Streaming Protocol) requests. When multiple archiving roles are hosted on the same server, this value must be unique for each one. The default value is 555 for the Archiver and 558 for the Auxiliary Archiver. The value configured must not duplicate any value used for the Media Router role or its redirector agent hosted on the same server.
  - **Telnet port:** Port used to listen to the *Telnet console* connection requests for debugging purposes. When you change this value, you need to deactivate and reactivate the Archiver role for the change to take effect.
- **Database status:** Current status of the database.
- **Database server:** Server in which the role's database is located.
- **Database:** Name of the database instance.
- **Actions:** Maintenance functions you can perform on the role's database:
  - **Create a database (✚):** Create a new database.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (🔔):** Set up notifications for when the database space is running low.
  - **Backup/restore (▭):** Back up or restore the database.
- **Recording:** Displays information about local drives and network drives, which can be used to store video footage. All local drives found on the host server are listed by default and grouped under *Default Disk Group*.
  - **Disk base path:** Root folder on the disk where all video files are located. The default value is *VideoArchives*.
  - **Min. free space:** Minimum free space that the Archiver must never use on the disk. The default value is 1% of total disk space capacity.
  - **Free space:** Actual free space remaining on disk.
  - **Disk usage:** Chart showing the total capacity of the disk (full chart), the minimum free space (red), the occupied disk space (dark gray), and the remaining free space for video archives (light gray). Hover over the chart with the mouse to display these values in a tooltip.



Disk base path	Min. free space	Disk usage
VideoArchives	2.0 GB	

16.8 GB available of 18.8 GB free
Total disk space: 49.9 GB

  - **Add network location (🖧):** You can only add network drives to your archive storage. All local drives on the host server are listed by default. You can exclude them from being used by the Archiver by clearing the checkbox in front of each disk.

  - **Add group:** A disk group is a logical storage unit used by the Archiver to improve the overall disk throughput. Click the **Up** and **Down** arrows to move the selected disk from one group to another.
  - **Delete (✖):** Deletes the selected disk or disk group. Each disck group must have at least one disk associated to it.
  - **Camera distribution (⚖):** Divide the cameras between the disk groups. This button appears only if you have more than one disk group defined.
  - **Refresh the drive information (🔄):** Refreshes the drive information.
- **Archive transfer:** Settings for archive transfer.
  - **Backup folder:** Location in which the backed up archives are saved as a G64x file.
  - **Delete oldest files when disks are full:** Turn on this option to delete the oldest video archives when the disk is full.
  - **Automatic cleanup:** Turn this option on to specify a retention period for the backed up video archives (in days). If you do not enable this option, the backed up video archives are not deleted by the system, and you must manually delete them.

Archiver statistics

The Statistics dialog box appears when you click the *Statistics* (◕) button. It provides information regarding the archive storage, and the rate at which it is being consumed.

- **Refresh (🔄):** Refreshes the statistics.
- **List of assigned disks:** Snapshot of the disk statistics taken from the last time a refresh occurred.
- **Protected video file statistics (◕):** View the percentage of protected video files on the selected disk.
- **Average disk usage:** Average space used per day (first line) and average space used per camera per day (second line).
- **Estimated remaining recording time:** Number of days, hours, and minutes of recording time remaining based on the average disk usage and the current load.
- **Active cameras:** Number of cameras that are currently active.
- **Archiving cameras:** Number of cameras that have archiving enabled.
- *See details*: View the *recording state* and statistics of each individual camera in the *Archiving camera details* dialog box. The statistics are taken from the last refresh of the *Statistics* dialog box. This report allows you to verify whether each encoder is currently streaming video (and audio) and whether the Archiver is currently recording the data.
- **Archiving span:** Time bracket in which video archives can be found.
- **Worst case bandwidth:** Number indicating the worst-case scenario on the total bandwidth requirement if all the cameras are at the peak of their archiving demands.

Advanced settings

The advanced settings are independent of the server hosting the Archiver role.

- **Video watermarking:** Turn on this option to protect your video archive against tampering.
- **Delete oldest files when disks are full:** Turn on this option to recycle the archive storage (the default mode). The oldest files are deleted to make space for new files when all the disks within a disk group are full.
- **Enable edge playback requests:** Turn on this option only if the Archiver controls units that are configured for *edge recording*. By default, this option is turned off to prevent sending playback requests to units that are not recording.

- **Enable thumbnail requests:** Turn on this option to show video thumbnails for the Archiver (for example, in reports).
- **Enable telnet console:** Turn on this option to enable the telnet debug console for this Archiver.
- **Protect video threshold:** This is a safety threshold that limits the amount of space that protected video files can occupy on disks. The percentage you set is the proportion of protected video that you can have of the total size of recorded videos on the disk. Protected video files are files that will not be deleted by normal archive cleanup procedures. If this threshold is exceeded, the Archiver generates the *Protected video threshold exceeded* event once every 15 minutes for as long as the condition is true, but will not delete any video file that is protected.
- **Disk load warning threshold:** The percentage of disk space that must be occupied before the *Disk load threshold exceeded* event is generated. The default value is 90%. The Archiver generates this event once every hour for as long as the condition is true.
- **Max archive transfer throughput:** The maximum bandwidth available to the Archiver for archive transfer.
- **Video files:** These two settings are used to control the size of the video files created by the Archiver:
  - **Maximum length:** Limits the length of video sequence contained in each file. The video length is the time span between the first video frame and the last video frame stored in a file. The default value is 20 minutes.
  - **Maximum size:**
    Limits the size of the video file. The default value is 500 MB.
    The Archiver starts saving the video to a new video file when either one of these conditions is met.
- **Additional settings:** These additional settings are reserved for use by the Technical Assistance personnel of Genetec Inc..

Auxiliary Archiver - Camera recording tab

You can use the **Camera recording** tab to configure the default recording settings applied to all *cameras* associated to an Auxiliary Archiver. Recording settings defined on the **Recording** tab of an individual camera supersede the settings defined on the **Camera recording** tab of the Auxiliary Archiver.

The **Camera recording** tab includes the following settings:

- **Video stream:** Select the default video stream that the Auxiliary Archiver should record for each camera. The video streams are configured for each individual camera.
- **Recording modes:** Apply different recording modes on different schedules.
  - **Continuous:** Records continuously. Recording cannot be stopped by the user (●).
  - **Custom:** Recording is specified by a custom schedule. You can use the custom schedule that was created with the installer assistant, or click ✚ to add a custom recording schedule that was created using the *System* task. For more information about creating schedules using the *System* task, see Creating schedules on page 169.
    CAUTION: Recording schedules of the same type (for example, two daily schedules) cannot overlap, regardless of the recording mode configured for each. When a scheduling conflict exists, the Archiver and the video units are displayed in yellow in the entity browser and they issue entity warning messages.
  - **Off:** Recording is off (●), even when an alarm is triggered.
- **Record audio:** Records audio along with video. A microphone entity must be attached to the camera for this option to work.

  NOTE: It is not necessary for the attached devices to belong to the same unit as the video encoder. However, for audio recording to work, you must make sure that the microphone belongs to a unit that is controlled by the same Archiver through the same Archiver extension as the unit that the video encoder belongs to.
- **Record metadata:** Records metadata (such as overlays) with your video.
- **Automatic cleanup:** Specify a retention period for recorded video (in days). Video archives older than this period are deleted.

Auxiliary Archiver - Cameras tab

This section lists the settings found in the Auxiliary Archiver role *Cameras* tab, in the Video task.

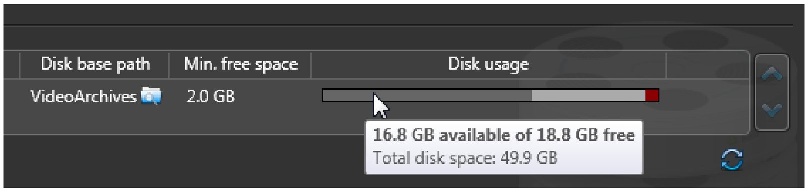
In the *Cameras* tab, you can select the *cameras* archived by this role. The Auxiliary Archiver can record any camera on your system, except those that are federated from an Omnicast™ 4.x system.

Auxiliary Archiver - Resources tab

This section lists the settings found in the Auxiliary Archiver role *Resources* tab, in the Video task.

Click the **Resources** tab to assign servers, databases, and disk storage to this Auxiliary Archiver role.

- **Server (⊕):** Server hosting this role. Failover is not supported for the Auxiliary Archiver role. You can only select one server.
  - **Network card:** Network card used to communicate with all video units.
  - **RTSP port:** Port used to listen for RTSP (Real Time Streaming Protocol) requests. When multiple archiving roles are hosted on the same server, this value must be unique for each one. The default value is 555 for the Archiver and 558 for the Auxiliary Archiver. Additionally the value configured must not duplicate any of those used for the *Media Router* role or its *redirector agent* hosted on the same server.
- **Database status:** Current status of the database.
- **Database server:** Server in which the role's database is located.
- **Database:** Name of the database instance.
- **Actions:** Maintenance functions you can perform on the role's database:
  - **Create a database (✚):** Create a new database.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (🔔):** Set up notifications for when the database space is running low.
  - **Backup/restore (▭):** Back up or restore the database.
- **Disk information:** Displays information about both local drives and network drives, which can be used to store video footage. All local drives found on the host server are listed by default and grouped under *Default Disk Group*.
  - **Disk base path:** Root folder on the disk where all video files are located. The default value is *AuxiliaryArchives*.
  - **Min. free space:** Minimum free space that the Auxiliary Archiver must leave untouched on the disk.
  - **Disk usage:** Chart showing the the total capacity of the disk (full chart), the minimum free space (red), the occupied disk space (dark grey), and the remaining free space for video archives (light grey). Hover over the chart with the mouse to display these values in a tooltip.



Disk base path	Min. free space	Disk usage
VideoArchives	2.0 GB	

16.8 GB available of 18.8 GB free
Total disk space: 49.9 GB

- **Add network location (🖧):** You can only add network drives to your archive storage. All local drives on the host server are listed by default. You can exclude them from being used by clearing the checkbox in front of each disk.
- **Add group (▣):** A disk group is a logical storage unit used by the Archiver to improve the overall disk throughput. Click the *Up* and *Down* arrows to move the selected disk from one group to another.
- **Delete (✖):** Deletes the selected disk or disk group. You cannot leave a disk group without any disk associated to it.

- **Camera distribution (⚖):** Divide the cameras between the disk groups. This button appears only if you have more than one disk group defined.
- **Refresh the drive information (🔄):** Refreshes the drive information.

Archiver statistics

The Statistics dialog box appears when you click the *Statistics* (◔) button. It provides information regarding the archive storage, and the rate at which it is being consumed.

- **Refresh (🔄):** Refreshes the statistics.
- **List of assigned disks:** Snapshot of the disk statistics taken from the last time a refresh occurred.
- **Protected video file statistics (◔):** View the percentage of protected video files on the selected disk.
- **Average disk usage:** Average space used per day (first line) and average space used per camera per day (second line).
- **Estimated remaining recording time:** Number of days, hours, and minutes of recording time remaining based on the average disk usage and the current load.
- **Active cameras:** Number of cameras that are currently active.
- **Archiving cameras:** Number of cameras that have archiving enabled.
- *See details***:** View the *recording state* and statistics of each individual camera in the *Archiving camera details* dialog box. The statistics are taken from the last refresh of the *Statistics* dialog box. This report allows you to verify whether each encoder is currently streaming video (and audio) and whether the Archiver is currently recording the data.
- **Archiving span:** Time bracket in which video archives can be found.
- **Worst case bandwidth:** Number indicating the worst-case scenario on the total bandwidth requirement if all the cameras are at the peak of their archiving demands.

Advanced settings

The advanced settings are independent of the server hosting the Archiver role.

- **Video watermarking:** Turn on this option to protect your video archive against tampering.
- **Delete oldest files when disks are full:** Turn on this option to recycle the archive storage (the default mode). The oldest files are deleted to make space for new files when all the disks within a disk group are full.
- **Enable edge playback requests:** Turn on this option only if the Archiver controls units that are configured for *edge recording*. By default, this option is turned off to prevent sending playback requests to units that are not recording.
- **Enable thumbnail requests:** Turn on this option to show video thumbnails for the Archiver (for example, in reports).
- **Enable telnet console:** Turn on this option to enable the telnet debug console for this Archiver.
- **Protect video threshold:** This is a safety threshold that limits the amount of space that protected video files can occupy on disks. The percentage you set is the proportion of protected video that you can have of the total size of recorded videos on the disk. Protected video files are files that will not be deleted by normal archive cleanup procedures. If this threshold is exceeded, the Archiver generates the *Protected video threshold exceeded* event once every 15 minutes for as long as the condition is true, but will not delete any video file that is protected.
- **Disk load warning threshold:** The percentage of disk space that must be occupied before the *Disk load threshold exceeded* event is generated. The default value is 90%. The Archiver generates this event once every hour for as long as the condition is true.

- **Max archive transfer throughput:** The maximum bandwidth available to the Archiver for archive transfer.
- **Video files:** These two settings are used to control the size of the video files created by the Archiver:
  - **Maximum length:** Limits the length of video sequence contained in each file. The video length is the time span between the first video frame and the last video frame stored in a file. The default value is 20 minutes.
  - **Maximum size:**
    Limits the size of the video file. The default value is 500 MB.
    The Archiver starts saving the video to a new video file when either one of these conditions is met.
- **Additional settings:** These additional settings are reserved for use by the Technical Assistance personnel of Genetec Inc..

Directory Manager configuration tabs

You configure the settings of the Directory Manager role from the **Roles** view of the *System* task in Security Center Config Tool.

Directory Manager - Directory servers tab

In the **Directory servers** tab, you can configure the servers assigned to Directory *failover* and *load balancing*.

- **List of Directory servers (for failover and load balancing):** List of servers assigned to Directory failover and load balancing, called the *Directory failover list*. The server identified with a different icon ( ) than the rest ( ) is the *main server*. The main server is the only Directory server that can write to the Directory database. The rest can only read from that database.
- **Advanced ( ):** Configure the server as a gateway or disaster recovery server.
- **Modify license for all servers:** Modify your Security Center license every time you make a change to the list of servers assigned to host the Directory role.

Directory Manager - Database failover tab

In the **Database failover** tab, you can configure the Directory database failover.

- **Use database failover:** Enable Directory database failover.
- **Failover mode:** Select which database failover mode to use.
- **Backup and restore:** The Directory Manager protects the Directory database by regularly backing up the master database instance (source copy). During a failover, the latest backups are restored to the backup database that's next in line.
  - **LED (●):** Indicates the database server that is currently active.
  - **Server:** Security Center *server* hosting the database instance. The server that manages the master database instance is flagged as *(Master)*.
  - **Database server:** *Database server* name. The name must be accessible from all computers. Relative names, such as `(local)\SQLSEXPRESS` cannot be used. Always explicitly write the server's DNS name (for example `TW-WIN7-SC-5`) instead of `(local)`.
  - **Database name:** Database instance name.
  - **State:** Database state. If there is a problem, an error message is displayed.
  - **Last Backup/Restore time:** Time of the last backup on the master database, or the last restore on the backup database.
  - **Folder:** Local folder on the specified server where the backup files are copied.
  - **Automatically reconnect to master database:** Select this option to force all *Directory servers* to reconnect to the master database once it is back online after a failover. This will cause a short service disruption, and all changes made to the system configuration while the master database was offline will be lost.
  - **Generate full backup every:** Specify how often (in days) a full backup is generated, and at and what time.
  - **Generate differential backup every:** Specify how often (in minutes) a differential backup should is generated. A differential backup contains the database transactions made after the previous backup (full or differential). The differential backups are deleted after the next full backup is made.
    NOTE: All backup activities are stopped when the active database is not the master database.

- **Mirroring:** Database failover is taken care of by Microsoft SQL Server and is transparent to Security Center. The *Principal* and *Mirror* instances of the Directory database are kept in synch at all times. There is no loss of data during failover.
  - **Database server:** *Database server* name. The name must be accessible from all computers. Relative names, such as `(local)\SQLSEXPRESS` cannot be used. Always explicitly write the server's DNS name (for example `TW-WIN7-SC-5`) instead of `(local)`.
  - **Database name:** Database instance name.

Global Cardholder Synchronizer configuration tabs

You configure the settings of the Global Cardholder Synchronizer role from the **Roles and units** tab of the *Access control* task in Security Center Config Tool.

Global Cardholder Synchronizer - Properties tab

Click the **Properties** tab to configure the connection parameters to the *sharing host*, the *global partitions* you want to share, and how you want to synchronize.

- **Connection status:** Indicates the current connection status between the Global Cardholder Synchronizer (GSC) role and the sharing host. The second line shows the connection activities or when the last synchronization was performed.
- **Directory:** Name of the *Directory server* on the sharing host. If anything else than the default connection port (5500) is used, you must explicitly indicate the port number after the Directory name, separated by a colon. For example: `HostServer:5888`.
- **Username and password:** Credentials used by the GCS role to connect to the sharing host. The rights and privileges of this user determine what your local system is able to see and share with the host system.
- **Global partitions:** List of global partitions found on the sharing host. Select the ones you want to share.
- **Refresh:** Click this button to view the list of global partitions found on the sharing host.
- **Synchronize:** Click this button to receive the latest updates from the sharing host. You can also synchronize the local system on schedule by setting up a scheduled task.

Global Cardholder Synchronizer - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The GCS role does not require a database.

- **Servers:** Servers hosting this role.

Health Monitor configuration tabs

You configure the settings of the Health Monitor role from the **Roles** view of the *System* task in Security Center Config Tool.

Health Monitor - Properties tab

Click the **Properties** tab to configure the health events to be monitored.

- **Client app. maintenance mode:** Turn this option on to set the client applications in maintenance mode.
- **Events to monitor:** Select which events you want the Health Monitor role to watch.

Health Monitor - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role.
- **Database status:** Current status of the database.
- **Database server:** Server in which the role’s database is located.
- **Database:** Name of the database instance.
- **Actions:** Maintenance functions you can perform on the role’s database:
  - **Create a database (➕):** Create a new database.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications ():** Set up notifications for when the database space is running low.
  - **Backup/restore ():** Back up or restore the database.

Intrusion Manager configuration tabs

You configure the settings of the Intrusion Manager role from the *Intrusion detection* task in Security Center Config Tool.

Intrusion Manager - Properties tab

Click the **Properties** tab to configure the retention period of the intrusion events in the Intrusion Manager database.

- **Keep events:** Specify how long to keep the intrusion detection events that are logged by the Intrusion Manager in the database, before they are deleted.
- **Reconnection delay:** Specify how long the *Intrusion Manager* waits before trying to reconnect to a unit that went offline.

Intrusion Manager - Extensions tab

Click the **Extensions** tab to view the intrusion unit models controlled by this Intrusion Manager role.

All supported *manufacturer extensions* are created by default when the role is created.

Intrusion Manager - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role.
- **Database status:** Current status of the database.
- **Database server:** Server in which the role’s database is located.
- **Database:** Name of the database instance.
- **Actions:** Maintenance functions you can perform on the role’s database:
  - **Create a database (✚):** Create a new database.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (●):** Set up notifications for when the database space is running low.
  - **Backup/restore (▭):** Back up or restore the database.

LPR Manager - Properties tab

In the LPR task on the *Properties* tab, you can configure the general LPR Manager role settings and optional AutoVu™ features. The availability of certain features depends on your Security Center license.

General settings

Use the *General settings* to configure the *Root folder* for the LPR Manager, the user group for the Patrollers, and how long the data from the LPR Manager is kept in the database.

- **Root folder:** Main folder on the computer hosting the LPR Manager, where all the configuration files are created, saved, and exchanged between the LPR Manager and the Patroller units it manages.
- **Optimize Root folder disk space:** (Windows Vista or later only) Enable the use of symbolic links to reduce disk utilization when the same file is replicated in multiple folders, such as when you have large hotlists and/or permit lists associated to individual Patroller units. This reduces the Root folder's overall disk space, and optimizes file transfer performance to the Patroller in-vehicle computer.

  IMPORTANT: If your root folder is on a network drive, the Genetec™ Server service must be configured to run using a domain user and not a local user.
- **User group for Patrollers:** List of users (and their passwords) who are allowed to log on to the Patrollers managed by the LPR Manager. This list is downloaded to the Patrollers.
- **Retention period:** Specify how many days of LPR-related data Security Center can query. The default is 90 days, and the maximum is 4000 days. The LPR date that is older than the values specified do not appear in Security Center queries and reports (Hit reports, Read reports, and so on).
  - **Patroller route retention period:** Number of days Patroller *route* data (GPS positions) is kept in the database.
  - **Hit retention period:** Number of days the hit data is kept in the database.
  - **Read retention period:** Number of days *license plate reads* are kept in the database. The *Read retention period* cannot exceed the *Hit retention period.* If the read retention is lower than the hit retention, only the reads that are associated with hits will be kept.
  - **Event retention period:** Number of days the LPR events (*License plate read* and *License plate hit*) are kept in the database.
  - **Hit image retention period:** Number of days the hit image data is kept in the database. The *Hit image retention period* cannot exceed the *Hit retention period* since an image is always associated to a hit.
  - **Read image retention period:** Number of days the read image data is kept in the database. The *Read image retention period* cannot exceed the *Read retention period.*

Live

The *Live* settings are used to configure how data is transferred between Security Center and Patroller.

- **Listening port:** Port used to listen for connection requests coming from fixed Sharps and Patrollers. After the connection is established, the LPR Manager can receive live updates from the *LPR units* it manages.

  NOTE: If you are using multiple LPR Managers, each LPR Manager must use a different listening port.
- **Sharp Sharp discovery port:** Port used by the LPR Manager to find fixed Sharp units on the network. The same port number must be used in the *Discovery port* setting on the Sharp.

  NOTE: When setting the discovery port, do not use port 5050 as it is reserved for the logger service.

- **Send on read (fixed Sharps only):** The Sharp images that are sent to Security Center for each plate read. These images are displayed in Security Desk when monitoring LPR events.
  - **License plate image:** Include the high resolution close-up image of the license plate along with the plate read data.
  - **Context image:** Include the wide angle context image of the vehicle along with the plate read data.
- **Channel security:** Encrypt communication between Security Center and Patroller.

  IMPORTANT: If you select this option, encryption must also be enabled in Patroller Config Tool.

  - **Encrypt communication channel:** Encrypt communication between Patroller and Security Center.
  - **Accept non encrypted messages:** Security Center will accept incoming connections from Patrollers that do not have the encryption option enabled.

File association

The *File association* settings specify which hotlists and permits are active and managed by the LPR Manager.

- **Hotlists:** A list of all the *hotlists* in Security Center. Select which hotlists you want the LPR Manager to manage.
- **Permits:** A list of all the *permits* in Security Center. Select which permits the LPR Manager manages.

Matching

The *Matching* settings are used to enable matching between hotlists and fixed Sharp units. When matching is enabled, you can configure event-to-actions in Security Desk that trigger on *Match* and *No match* events.

- **Matching:** When matching is enabled, you can configure event-to-actions in Security Desk that trigger when the Sharp reads a plate that is on a hotlist you've activated in File association.
- **Generate No match events:** Security Center generates *No match* events when a plate is not found on a specific hotlist. You can then configure event-to-actions in Security Desk based on *No match* events.

Geocoding

The *Geocoding* feature converts the raw GPS data (longitude, latitude) from Patrollers into street addresses. The street addresses are then saved along with the reads in the LPR Manager database.

NOTE: You need geocoding if your Patrollers are equipped with GPS but no maps.

- **Map type:** Displays the map type set in the Security Center license.
- **Maps and data folder:** Folder where the Benomad files are found. This folder must be on the same computer where the LPR Manager is installed.

Plate filtering

The *Plate filtering* settings determine what to do when a hotlist or permit list is modified and the LPR Manager detects that there are entries with invalid characters (non-alphanumeric characters).

- **Plate number valid characters:** The types of characters to filter on (Latin, Arabic, or Japanese).
- **Invalid plate number:** How the LPR Manager handles invalid records.
  - **Modify record:** (Default setting). Removes any non-alphanumeric characters from the plate number. For example, the plate number "ABC#%3" becomes "ABC3".
  - **Remove record:** Deletes the entire entry from the list.
- **Log filtering:** Select to log the filtering process. The plate filtering logs will be saved in the AutoVu™ root folder: *C:\Genetec\AutoVu\RootFolder*.

Email notification

The *Email notification* setting turns on email notifications for hotlist hits, and lets you customize the look and contents of the email message.

- **Email attribute name:** Used for email notification at the individual license plate level. Type the name of the hotlist attribute related to email notification. For example, if you added an “Email” attribute on the hotlist entity’s Properties tab, then type the exact same name here. The names must match exactly.
- **Email attachments:** The LPR data that is attached to the notification email, and whether to hide the license plate numbers in the message body.
  - **License plate image:** High resolution close-up images of the license plate.
  - **Context image:** A wider angle color image of the vehicle.
  - **Wheel image:** Replaces the read plate number, and the matched plate number in the email with asterisks (*).
- **Log emails:** Select this option to log hotlist hit notification emails. The email logs will be saved in the AutoVu™ root folder: *C:\Genetec\AutoVu\RootFolder*.
- **Template:** Customize the email. Do any of the following:
  - Edit the email’s subject line or message body.
  - Switch between plain text and HTML.
  - Add formatting (bold, italics, and so on).
  - Right-click in the message body for a menu of quick tags that you can use to add more information to the email.
  - Restore the default email template at any time.

XML import

The *XML import* settings are used to import data from third-party applications into the LPR Manager database. When you turn this setting on, Security Center creates an *XML import* entity, and then associates the imported data with this entity. In Security Desk, you can then filter on the *XML import* entity when running hit or read reports

NOTE: This option requires a license. Please contact your representative of Genetec Inc. for more information.

- **XML read template file:** Specify where the XML read template file is located. You'll find a default template in the Security Center installation package in *Tools\LPR\XMLTemplatesSamples\XMLImport*.

  NOTE: In most cases the default template can be used.
- **XML data folder:** Specify the folder that contains the XML data files for Security Center to import.

  NOTE: Files are deleted from this folder once they've been processed.
- **Supported XML import hashtags:** The following XML import hashtags are supported. Each hashtag must have an opening and closing XML tag (for example, to use the tag *#CONTEXT_IMAGE#* you must write <*ContextImage>#CONTEXT_IMAGE#</ContextImage*> in the XML).
  - **#PLATE_READ#:** License plate as read by the Sharp.
  - **#PLATE_STATE#:** License plate's issuing state or province, if read.
  - **#DATE_LOCAL#:** Local date of the LPR event.
  - **#DATE_UTC#:** UTC date of date of the LPR event.
  - **#TIME_UTC#:** UTC time of the LPR event.
  - **#TIME_ZONE#:** Local time zone for the LPR event.

- **#CONTEXT_IMAGE#:** Context image (Base64-encoded JPEG).
- **#PLATE_IMAGE#:** License plate image (Base64-encoded JPEG).
- **#LONGITUDE#:** Longitude of the LPR event (in decimal degrees or DMS).
- **#LATITUDE#:** Latitude of the LPR event (in decimal degrees or DMS).
- **#GUID#:** Unique identifier of the LPR event.
- **#CUSTOM_FIELDS#:** You can import other fields with this hashtag by using the key=value format. Format the key as #CUSTOM_FIELDS#{KEY}.
  NOTE: You must specify a format for DATE and TIME hashtags. For example, #DATE_LOCAL#{yyyy/MM/dd}). Click here for more information about which formats to use. If these hashtags are not included, UTC dates and times are used as a baseline for calculating the local time. If an error occurs, the time the LPR Manager role imported the data is used

XML export

The *XML export* settings are used to send LPR Manager reads and hits to third-party applications. Reads and hits are sent live as they occur.

- **XML templates folder:** Specify where the XML templates folder is located. You'll find default templates in the Security Center installation package in *Tools\LPR\XMLTemplatesSamples\XMLExport*. There are XML templates for each type of LPR event (plate reads, hotlist hits, overtime hits, permit hits, and shared permit hits).

  NOTE: In most cases the default template can be used.
- **XML export folder:** Specify the folder that contains the XML files exported by the LPR Manager.
- **Time format:** Enter the time format used in the exported files. As you set the time format the information field displays what the time format will look like in the XML file.

  To identify the units of time, use the following notation:

Notation	Description
h	Hour
m	Minute
s	Second
:	Must use a colon (:) between the hour, minute, and second units.
hh,mm,ss	Display time with leading zero. For example: 03:06:03 represents 3 hours 6 minutes 3 seconds.
h,m,s	Display without leading zero. For example: 3:6:3 represents 3 hours 6 minutes 3 seconds.
tt	Include A.M. or P.M. If using a 12-hour clock, you might want to use A.M. or P.M. notation. Unit can be preceded with or without a space. For example, HH:mm:ss tt displays 17:38:42 PM.
Lowercase h	12-hour clock.
Uppercase H	24-hour clock.

- **Date format:** Select a date format to use in the exported files. You can choose either **MM/dd/yyyy** or **yyyy-MM-dd**. For example, yyyy-MM-dd displays 2016-06-21.
- **Supported XML hashtags:** The following XML export hashtags are supported. Each hashtag must have an opening and closing XML tag (for example, to use the tag *#CONTEXT_IMAGE#* you must write *<ContextImage>#CONTEXT_IMAGE#</ContextImage>* in the XML).
    - **#ACCEPT_REASON#:** Reason hit was accepted.
    - **#ATTRIBUTES#:** Generate all Read and Hit attributes.
    - **#CAMERA_NAME#:** Name of the camera.
    - **#CONTEXT_IMAGE#:** Context image (Base64-encoded JPEG).
    - **#DATE_LOCAL#:** Local date of the LPR event.
    - **#ELAPSED_TIME#:** For an overtime hit, this tag indicates the time difference between the two plate reads (displaying the number of days is optional).
    - **#FIRST_VEHICLE#:** For a shared permit hit, this tag generates the content specified in *ReadTemplate.xml* for the first vehicle seen.
    - **#FIRST_VEHICLE_FROM_STREET#:** For an overtime hit, this tag retrieves the attribute *From street* from the first plate read.
    - **#FIRST_VEHICLE_TO_STREET#:** For an overtime hit, this tag retrieves the attribute *To street* from the first plate read.
    - **#HOTLIST_CATEGORY#:** Category field of the hotlist that generated the hit.
    - **#GUID#:** Unique identifier of the LPR event.
    - **#INVENTORY_LOCATION#:** For MLPI installations, the location of the vehicle inventory.
    - **#ISHIT#:** This tag indicates if the LPR event is a hit.
    - **#LATITUDE#:** Latitude of the LPR event (in decimal degrees).
    - **#LATITUDE#{dms}:** Latitude of the LPR event (in degrees, minutes, and seconds).
    - **#LATITUDE#{dec}:** Latitude of the LPR event (in decimal degrees).
    - **#LATITUDE_DEGREE#:** Latitude of the LPR event (degrees).
    - **#LATITUDE_DMS#:** Latitude of the LPR event (in degrees, minutes, and seconds).
    - **#LATITUDE_MINUTE#:** Latitude of the LPR event (minutes).
    - **#LATITUDE_SECOND#:** Latitude of the LPR event (seconds).
    - **#LONGITUDE#:** Longitude of the LPR event (in decimal degrees).
    - **#LONGITUDE#{dec}:** Longitude of the LPR event (in decimal degrees).
    - **#LONGITUDE#{dms}:** Latitude of the LPR event (in degrees, minutes, and seconds).
    - **#LONGITUDE_DEGREE#:** Longitude of the LPR event (degrees).
    - **#LONGITUDE_DMS#:** Longitude of the LPR event (in degrees, minutes, and seconds).
    - **#LONGITUDE_MINUTE#:** Longitude of the LPR event (minutes).
    - **#LONGITUDE_SECOND#:** Longitude of the LPR event (seconds).
    - **#MATCHED_PLATE#:** License plate against which the hit was generated.
    - **#ORIGINAL#:** For an overtime hit, this tag generates the content specified in *ReadTemplate.xml* for the first read of a given plate.
    - **#OVERVIEW_IMAGE#:** Overview image (Base64-encoded JPEG).
    - **#PATROLLER_ID#:** ID of Patroller unit.
    - **#PATROLLER_NAME#:** Name of Patroller unit.

- **#PERMIT_NAME#:** Name of the permit that generated the LPR event.
- **#PLATE_IMAGE#:** License plate image (Base64-encoded JPEG).
- **#PLATE_READ#:** License plate as read by the Sharp.
- **#PLATE_STATE#:** License plate's issuing state or province, if read.
- **#REJECT_REASON#:** Reason hit was rejected.
- **#READ#:** Embed the contents of the *ReadTemplate.xml* inside another XML template (useful for hits).
- **#RULE_COLOR#:** Color of the rule associated to the LPR event.
- **#RULE_ID#:** ID of the rule associated to the LPR event.
- **#RULE_NAME#:** Name of the rule associated to the LPR event.
- **#SECOND_VEHICLE#:** For a shared permit hit, this tag generates the content specified in *ReadTemplate.xml* for the second vehicle seen.
- **#SECOND_VEHICLE_FROM_STREET#:** For an overtime hit, this tag retrieves the attribute *From street* from the second plate read.
- **#SECOND_VEHICLE_TO_STREET#:** For an overtime hit, this tag retrieves the attribute *To street* from the second plate read.
- **#SHARP_NAME#:** Name of the Sharp that read the plate.
- **#STATE#:** License plate's issuing state or province, if read.
- **#TIME_LOCAL#:** Local time.
- **#USER_ACTION#:** User action related to the LPR event.
- **#USER_ID#:** ID of the user.
- **#USER_NAME#:** Name of the user.
- **#VEHICLE#:** Same as #READ#.

Update provider

Turn on the *Update provider* to create the required sub-folder in the LPR Root folder that will receive the update files. Also, you need to specify the *Listening port* used for Patroller and Sharp updates. The LPR Manager uses this port to update Patrollers and Sharps with new hot fixes, hit alert sounds, hotlists, firmware and so on.

- **Listening port:** Port Security Center uses to send updates to Patrollers and connected Sharp units, as well as to fixed Sharps on the network. Make sure to use the same port number in Patroller Config Tool (see the *Patroller Administrator Guide*), and in the Sharp Portal (see the *Sharp Administrator Guide*).

LPR Manager - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role.
- **Database status:** Current status of the database.
- **Database server:** Server in which the role’s database is located.
- **Database:** Name of the database instance.
- **Actions:** Maintenance functions you can perform on the role’s database:
  - **Create a database (➕):** Create a new database.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (⏰):** Set up notifications for when the database space is running low.
  - **Backup/restore (▭):** Back up or restore the database.

NOTE: When using the cloud base Azure database, the *Notifications* and *Backup/restore* options are disabled.

Map Manager configuration tabs

You configure the settings of the Map Manager role from the **Roles** view of the *System* task in Security Center Config Tool.

Map Manager - Properties tab

Click the **Properties** tab to change the default settings for this role, and configure the external resources managed by this role, such as the map providers and the KML objects.

- **Map providers:** List of third-party map providers (*GIS*) that you are licensed to use.
- **Map layers:** List of imported KML objects that can be displayed on any georeferenced map. Each KML object corresponds to a distinct map layer that the Security Desk users can choose to show or hide.
- **Cache location:** The cache is a folder where the map tiles are stored. When you create maps from images files, the role generates a set of small images, called *map tiles*, for each zoom level at which you need to view the map. The larger the map scale, the more map tiles the role needs to generate. The default folder is *C:\ProgramData\Genetec Security Center 5.5\Maps*.
- **Port:** HTTP port used by the Map Manager to communicate with client applications. (Default=8012).
- **Default map:** The system default map, also known as the *global default map*, is used when a user does not have a personalized default map configured. You can only set the global default map after you have created your first map.

Map Manager - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Map Manager role does not require a database.

- **Servers:** Servers hosting this role.

Media Gateway configuration tabs

You configure the Media Gateway role from the *Video* task in Security Center Config Tool.

Media Gateway - Properties tab

Click the **Properties** tab to configure the start multicast address and the RTSP port for the Media Gateway, and you can enable secure communication between the role and the RTSP client applications.

- **Start multicast address:** Start multicast address and port number. In multicast, all video sources are streamed to different multicast addresses while using the same port number, because multicast switches and routers use the destination IP address to make their routing decisions. Similarly, the Media Gateway assigns that same port number to all streaming cameras, starting with the specified IP address, and incrementing the IP address by 1 for every new camera it encounters.
- **Listening port:** Incoming TCP command port used by the Media Gateway.
- **User authentication:** Enables authentication between the Media Gateway and RTSP client applications.

  IMPORTANT: The cameras that an RTSP client application can view in the system depend on the user account the client uses to log on to Security Center. Assign a password to each user account added to the list, preferably a different password than the one used in Security Center.

Media Gateway - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Media Gateway role does not require a database.

- **Servers:** Servers hosting this role.

Media Router configuration tabs

You configure the settings of the Media Router role from the *Video* task in Security Center Config Tool.

Media Router - Properties tab

Click the **Properties** tab to configure the stream redirectors, the start *multicast* endpoint, and the RTSP port for the Media Router.

- **Redirectors:** Servers assigned to host *redirector agents*, which is a software module launched by the Media Router to redirect data streams from one IP endpoint to another.
  - **Server:** Server selected to host the redirector agent.
  - **Incoming UDP port range:** Range of ports used by the redirector agent to send video using *UDP*.
  - **Live capacity:** Limit the maximum number of live streams that this server (redirector) can redirect, to avoid overloading the server or the network.
  - **Playback capacity:** Limit the maximum number of playback streams that this server (redirector) can redirect, to avoid overloading the server or the network.
  - **Multicast interface:** Network adaptor used for streaming data in multicast mode.
  - **RTSP port:** Port used by the redirector agent to receive TCP commands. The same port is used to stream data using TCP.
- **Start multicast endpoint:** Start multicast address and port number. In multicast, all audio and video sources are streamed to different multicast addresses while using the same port number, because multicast switches and routers use the destination IP address to make their routing decisions. Similarly, the Media Router assigns that same port number to all streaming devices (microphones and cameras), starting with the specified IP address, and incrementing it by 1 for every new devices it encounters.

  NOTE: If you are using Windows Server 2008 or earlier, you can greatly improve your system performance if you manually assign a different port number to each streaming device.
- **RTSP port:** Incoming TCP command port used by the Media Router.
- **Use secure communication:** Encrypts all RTSP video requests. When secure communication is enabled, all video communications use RTSP over TLS. If your network is configured for Multicast or Unicast UDP, only the RTSP control channel is encrypted (no impact on performance). If your network is configured for Unicast TCP, all video-related traffic (RTSP and video data) goes through the TLS channel. This impacts the performance of live video redirection. Video playback and video export always use RTSP over TCP, therefore the video data is always encrypted. Secure communication is enabled by default on new installations, but disabled if you upgraded from a version prior to 5.5.

  IMPORTANT: When secure communication is turned on, older Security Center systems cannot federate your Security Center system.

Media Router - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role.
- **Database status:** Current status of the database.
- **Database server:** Server in which the role’s database is located.
- **Database:** Name of the database instance.
- **Actions:** Maintenance functions you can perform on the role’s database:
  - **Create a database (➕):** Create a new database.

- **Delete the database (✖):** Delete the database.
- **Database info (ℹ):** Show the database information.
- **Notifications (◎):** Set up notifications for when the database space is running low.
- **Backup/restore (▭):** Back up or restore the database.

Omnicast™ Federation™ configuration tabs

You configure the settings of the Omnicast™ Federation™ role from the **Roles** view of the *System* task in Security Center Config Tool.

Omnicast™ Federation™ - Identity tab

Click the **Identity** tab to view descriptive information about this role and jump to the configuration page of related entities.

- **Role group:** An advanced setting that is only necessary if you plan on hosting more than 40 Omnicast™ Federation™ roles on the same server..

Omnicast™ Federation™ - Properties tab

Click the **Properties** tab to configure the connection parameters to the remote Omnicast™ system, and the default video stream and events you want to receive from it.

- **Connection status:** Shows the connection status of the Federation™ role to the remote Omnicast™ system.
- **Directory:** Name of the Omnicast™ Gateway connecting you to the remote Omnicast™ system.
- **Username and password:** Credentials used by the Federation™ role to log on to the remote Omnicast™ system. The rights and privileges of that user determine what your local users can see and do on the federated remote system.
- **Version:** Version of the federated Omnicast™ system. This list only contains Omnicast™ versions that you have installed a compatibility pack for.
- **Default live stream:** Default video stream used for viewing live video from federated Omnicast™ cameras.
- **Federated events:** Select the events you want to receive from the federated Omnicast™ system. Events are necessary if you plan to monitor the federated entities in Security Desk, or to configure event-to-actions for the *federated entities*.
- **Reset connection:** Force the Federation™ role to reconnect to the remote system.

Omnicast™ Federation™ - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Omnicast™ Federation™ role does not require a database.

- **Servers:** Servers hosting this role.

Point of Sale configuration tabs

You configure the settings of the Point of Sale role from the **Roles** view of the *System* task in Security Center Config Tool.

Point of sale - Properties tab

Click the **Properties** tab to configure how this role is to get the transaction data from the external *POS system*, and how long the data should be kept in Security Center.

- **Database server:** Database server used by the external POS system.
- **Database:** Database name used by the external POS system.
- **Transaction header table:** Table name used for transaction headers.
- **Transaction details table:** Table name used for transaction details (or transaction line items).
- **Fetch transaction every:** Frequency at which the role should poll the POS database for new data.
- **Retention period:** Number of days the transaction data should be kept locally.
- **Cleanup period:** Frequency of the local database cleanup.
- **Cleanup time:** Scheduled database cleanup start time.

Point of sale - Cash registers tab

Click the **Cash registers** tab to add and configure the cash registers (or terminals) whose associated transactions should be downloaded from the external POS database.

- **Name:** Name of the cash register entity.
- **Description:** Description of the cash register entity.
- **ID:** External identifier (or primary key) used to identify the cash register in the external POS database.

Point of sale - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role.
- **Database status:** Current status of the database.
- **Database server:** Server in which the role's database is located.
- **Database:** Name of the database instance.
- **Actions:** Maintenance functions you can perform on the role's database:
    - **Create a database (➕):** Create a new database.
    - **Delete the database (✖):** Delete the database.
    - **Database info (ℹ):** Show the database information.
    - **Notifications (🔔):** Set up notifications for when the database space is running low.
    - **Backup/restore (▭):** Back up or restore the database.

Report Manager configuration tabs

You configure the settings of the Report Manager role from the **Roles** view of the *System* task in Security Center Config Tool.

Report Manager - Properties tab

Click the **Properties** tab to configure the default behavior of this role.

- **Maximum number of results for batch reports:** Sets the maximum number of results that can be returned by the *Email a report* or *Export report* actions.
- **Destination folder:** The destination folder for the reports that are saved using the *Export report* action. You can select a local drive or a network drive.

Report Manager - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Report Manager role does not require a database.

- **Servers:** Servers hosting this role.

Security Center Federation™ configuration tabs

You configure the settings of the Security Center Federation™ role from the **Roles** view of the *System* task in Security Center Config Tool.

Security Center Federation™ - Identity tab

Click the **Identity** tab to view descriptive information about this role and jump to the configuration page of related entities in addition to the general options.

- **Role group:** An advanced setting that is only necessary if you plan on hosting more than 100 Security Center Federation™ roles on the same server.

Security Center Federation™ - Properties tab

Click the **Properties** tab to configure the connection parameters to the remote Security Center system, and the default video stream and events you want to receive from it.

- **Connection status:** Shows the connection status of the Federation™ role to the remote Security Center system.
- **Server:** Name of the main server (Directory) for the remote Security Center system.
- **Username and password:** Credentials used by the Federation™ role to log on to the remote Security Center system. The rights and privileges of that user determine what your local users can see and do on the federated remote system.
- **Default live stream:** Default video stream used for viewing live video from federated Security Center cameras.
- **Federated events:** Select the events you want to receive from the federated Security Center system. Events are necessary if you plan to monitor the federated entities in Security Desk, or to configure event-to-actions for the *federated entities*.

Security Center Federation™ - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Security Center Federation™ role does not require a database.

- **Servers:** Servers hosting this role.

Web-based SDK configuration tabs

You configure the settings of the Web-based SDK role from the **Roles** view of the *System* task in Security Center Config Tool.

Web-based SDK - Properties tab

Click the **Properties** tab to configure what the external developers need to know to use the web services.

- **Port** + **Base URI:** These two parameters are used to determine the address of the web service.

  For example, with Port=4590 and Base URI=WebSdk, the web service address would be "http://<computer>:4590/WebSdk/", where <computer> is the DNS name or public IP address of the server hosting the Web-based SDK role.
- **Streaming port:** Port used to stream the events. You can configure which events to listen to.
- **Use SSL connection:** Turn this option on (default=off) to use *SSL* encryption for communications with the web service. If you are using SSL encryption, the web service address uses *https* instead of *http*.
- **SSL settings:** Settings required when you are using SSL encryption.
  - **Certificate:** Name of the certificate to use. Use the form: "CN=NameOfTheCertificate". The certificate must be registered in Windows. You can find procedures on the web on how to do just that.
  - **Bind certificate to port:** Turn this option on (default=off) to bind the certificate to the port. This operation does the same thing as you would normally do under Windows.

Web-based SDK - Resources tab

Click the **Resources** tab to configure the servers assigned to this role. The Web-based SDK role does not require a database.

- **Servers:** Servers hosting this role.

Zone Manager configuration tabs

You configure the settings of the Zone Manager role from the **Roles** view of the *System* task in Security Center Config Tool.

Zone Manager - Properties tab

Click the **Properties** tab to configure the retention period of the zone events in the database.

- **Keep events:** Specify how long to keep the zone events logged by the Zone Manager in the database, before they are deleted.

Zone Manager - Resources tab

Click the **Resources** tab to configure the servers and database assigned to this role.

- **Servers:** Servers hosting this role.
- **Database status:** Current status of the database.
- **Database server:** Server in which the role's database is located.
- **Database:** Name of the database instance.
- **Actions:** Maintenance functions you can perform on the role's database:
  - **Create a database (➕):** Create a new database.
  - **Delete the database (✖):** Delete the database.
  - **Database info (ℹ):** Show the database information.
  - **Notifications (●):** Set up notifications for when the database space is running low.
  - **Backup/restore (▭):** Back up or restore the database.

50

Administration tasks

This section lists the options in Security Center administration tasks that have a General settings view, where you can configure general or solution-specific settings for your system.

This section includes the following topics:

LPR task - General settings view

This section lists the settings found in the *General settings* view of the LPR task.

General settings - Applications page

The *Applications* page lets you configure how Security Desk displays maps in the *Monitoring* and *Route playback* tasks. You can also limit the number of logon attempts in Patroller, enforce Patroller privacy settings, and set the attributes a Patroller user must enter when enforcing a hit.

- **Map type:** Display the type of map system supported by your Security Center license.
- **Color for reads:** Click to select the color used to show *license plate reads* on maps.
- **Initial longitude/latitude:** Set the default starting location for map view in Security Desk. You can type the coordinates in the fields or click Select and zoom in on a location and click Select. A red pushpin appears to indicate the selected position.
- **Logon attempts before lockdown:** You can specify the number of unsuccessful logon attempts a Patroller can make before the account is locked out. For example, if the limit is set to 3, Patroller users have three attempts to log on to Patroller with their username and password. On the fourth attempt, their accounts will be locked and they won't be able to logon. Users with locked accounts must contact their administrators in order to have the password reset. Patroller must be connected to the Security Center server for the password to be reset.
- **Privacy:** Configure Patroller to obscure license plate numbers, or exclude plate, context, or wheel images from reads and hits so that the information is not stored in the LPR Manager database.
  - **License plate, context, or wheel images:** When switched to *On*, images are not sent to Security Center or included in offloaded data.
  - **License plate:** When switched to *On*, the plate number text string is replaced by asterisks (*) when sent to Security Center or in the offloaded data.
- **Enforced hit attributes:** Create text entry fields that Patroller users must enter text in when they *enforce* a hit. The information from the enforced hit text fields can be queried in the Security Desk hits report.

General settings - Hotlist page

The *Hotlist* page allows you to define the customized attributes, reasons, and categories that will appear in Patroller when the user adds a *New wanted* entry, or rejects or accepts a hit. The settings are downloaded to Patroller along with the selected hotlists when Patroller connects to Security Center. These settings are also available as filter options for hit reports in Security Desk.

- **New wanted attributes:** A new wanted is a hotlist item that is manually entered by the Patroller user. The new wanted attributes are attributes other than the standard ones (plate number, plate issuing state, category) that the Patroller user is asked to specify when entering a new wanted item in the Patroller.
- **New wanted categories:** List of hotlist categories that a Patroller user can pick from when entering a new wanted item. The category is the attribute that says why a license plate number is wanted in a hotlist.
- **Hit reject reasons:** List of reasons for rejecting hotlist hits. These values also become available as Reject reason filter options for generating hit reports in Security Desk.
- **Hit accept reasons:** A form that contains information Patroller users must provide when they accept a hit. The information from the hit form can be queried in the Security Desk Hit report.

- **Enable “No infraction” button:** Select this option to enable the *No infraction* button in the Patroller hit survey. This button allows the Patroller user to skip the hit survey after enforcing a hit.

General settings - Overtime rule page

The *Overtime rule* page allows you to define the custom reject reasons for overtime hits. The values defined here are downloaded to Patrollers and are available as Reject reason filter options for generating hit reports in Security Desk.

One category is pre-configured for you when you install Security Center.

General settings - Permit page

The *Permit* page allows you to define the custom reject reasons for permit hits, and to select the minimum elapsed time for shared permit violations (University Parking Enforcement only). The values defined here are downloaded to Patrollers and are available as Reject reason filter options for generating hit reports in Security Desk.

One category is pre-configured for you when you install Security Center.

- **Hit reject reasons:** List of reasons for rejecting permit hits or shared permit hits. These values also become available as Reject reason filter options for generating hits reports in Security Desk.
- **Maximum elapsed time for shared permit violation:** This parameter defines the time period used by University Parking Enforcement Patrollers to generate shared permit hits. A shared permit hit is generated when two vehicles sharing the same permit ID are parked in the same parking zone within the specified time period.

  For example, let’s say you’re using the default 120 minutes (two hours), and license plates ABC123 and XYZ456 are sharing the same parking permit. If Patroller reads plate ABC123 at 9:00 A.M., and then reads plate XYZ456 at 11:01 A.M., Patroller does **not** raise a hit because the time exceeds the 120 minutes.

General settings - Annotation fields page

The *Annotation fields* page allows you to define additional selectors to appear in Security Desk *Reads* or *Hits* report. To be valid, the selector must relate exactly to the information contained in the actual read or hit.

For example, if you configure *CarModel* and *CarColor* as an Enforced hit attribute (see), the Patroller user will be asked to enter the car’s model and color when enforcing a hit, and the information will be stored with the hit. Specifying *CarColor* as an *Annotation* field will allow the values entered by the user to be displayed in a *Hits* report.

You can also add user custom fields to annotation fields in order to associate a user’s metadata with individual reads and hits. This allows you to query and filter for the user custom fields in Security Desk *Reads* and *Hits* reports.

General setting - Updates page

The *Updates* page allows you to update Patrollers and Sharp units with hotfixes or new sound files for hit alerts. You can also update services on Sharp units, and upgrade Sharp firmware. Before you can send updates, you need to receive the updates from Genetec Inc. and place them in the *Updates* folder under the LPR *Root folder*.

- **Collapse all:** Collapses all items in the *Entity* field.
- **Expand all:** Expands all items in the *Entity* field.
- **Update all:** Update all units that are controlled by the currently-selected LPR Manager. This button updates only the units on the current tab. For example, if you’re on the *Patroller and Sharp units* tab, you’ll update all Patrollers and Sharp units on the list.

  - **Status:** Shows the status of the update. The possible statuses are:
  - **Not available:** Updater service is not supported (for example, Sharp versions 1.5 and 2.0 with less than 512 MB RAM).
  - **Entitled:** The client machine can receive the update.
  - **Synchronizing:** The client machine has started synchronizing with the server.
  - **Synchronized:** All update files have been successfully downloaded to the client machine. The client machine is waiting for the update to be applied.
  - **Installing:** Client machine has accepted the update, and has started replacing outdated files with new files.
  - **Installed:** The new updates have successfully been applied to the client machine.
  - **Uninstalling:** The update is being removed from the client machine.
  - **Uninstalled:** The update has been successfully removed from the client machine.
  - **Error:** An error occurred in the update process.
- **Drop folder:** Opens the required folder for you to copy the update file. For example, clicking the drop folder icon for a Patroller entity opens *C:\Genetec\AutoVu\RootFolder\Updates\Patroller* (default location).

  NOTE: If Security Center is running on a computer that doesn’t have access to the server computer, clicking the drop folder opens the *My Documents* folder on the local machine.
- **Patrollers and Sharp units:** Displays the Patrollers and Sharp units (fixed and mobile) that are eligible for an update.
- **Update services:** Displays the Sharp services that are eligible for an update.
- **Firmware upgrade:** Displays the Sharp units that are eligible for a firmware upgrade.

System task - General settings - Custom fields page

(Only visible to administrative users) The *Custom fields* page in the *General* view is where you define custom fields and custom data types for your system entities.

Custom fields tab

The *Custom fields* tab lists all custom fields defined in your system and allows you to add new ones.

Each custom field is characterized by the following properties:

- **Entity icon/Field name:** Custom field name and the entity type using it.
- **Data type:** Custom field data type. The default data types are:
  - **Text:** Alphanumeric text.
  - **Numeric:** Integers in the range -2147483648 to 2147483647.
  - **Decimal:** Real numbers from -1E28 to 1E28.
  - **Date:** Gregorian calendar date.
  - **Date/Time:** Gregorian calendar date and time.
  - **Boolean:** Boolean data, represented by a check box.
  - **Image:** Image file. The supported formats are: bmp, jpg, gif, and png.
  - **Entity:** Security Center entity.
- **Default value:** Preset default values are provided for certain data types. This column displays the default value that was selected when defining the custom field. The selected value appears when the field is displayed in the specific entity.
- **Mandatory:** A value must be provided with this type of field, otherwise the system will not accept your changes.
- **Value must be unique:** Indicates a key field. This option does not apply to fields using custom data types.
- **Group name/Priority:** Name the custom field is grouped under, and the field's order of appearance within the group. *No group (1)* is the default value. Custom fields that belong to no group appear first in the entity's custom field page.
- **Owner:** Name of the Global Cardholder Synchronizer role when the custom field is part of is part of a shared *global entity* definition.

Custom data types tab

The *Custom data types* tab lists all custom data types defined in your system and allows you to add new ones.

Each custom data type is characterized by the following properties:

- **Data type:** Name of the custom data type.
- **Description:** Optional data type description.
- **Values:** Enumeration of acceptable values (text strings) for this data type.
- **Owner:** Name of the Global Cardholder Synchronizer role when the custom data type is part of a shared *global entity* definition.

System task - General settings - Events page

(Only visible to administrative users) The *Events* page allows you to define event colors and custom events.

Event colors tab

The *Event colors* tab allows you to assign different colors to different *system events*.

- **Event:** Event to assign a color to.
- **Color:** Assigned color for that event in Security Desk.

Custom events tab

The *Custom events* tab allows you to view and add custom events to your system.

- **Custom event:** Name of the custom event.
- **Value:** Unique number to identify the custom event from other custom events.

System task - General settings - Actions page

The *Actions* page allows you to create *event-to-actions* for your system, and search for the ones that have already been defined by source entity (name and type), event type, and action type.

- **Entity:** Source entity, or the entity the event is attached to.
- **Event:** Name of the event that triggers the action.
- **Action:** Name of the action triggered by the event.
- **Arguments:** Additional information required for the action. For example, if the action is *Trigger alarm*, the argument is the alarm type that is triggered. Or, if the action is *Send a message*, the argument is the email recipient.
- **Details:** Additional details about the action.
- **Schedule:** Schedule when this event-to-action applies. Event occurring outside the time range covered by the schedule do not trigger any action.

System task - General settings - Logical ID page

The *Logical ID* page allows you to view and assign logical IDs to all entities defined in your system.

- **Show logical ID for:** Different groups of entity types. Logical IDs must be unique across all entities of a same group. The groups are listed in the drop-down list.
- **Hide unassigned logical IDs:** Select this option to only show entities with a logical ID assigned.
- **Name:** Name of the entity, public task, or workstation.
- **ID:** Logical ID assigned to the entity, public task, or workstation.
- **Alarm monitoring:** Assign a logical ID to the *Alarm monitoring* task in Security Desk. This allows the Security Desk user to open the Alarm monitoring task using a keyboard shortcut.

System task - General settings - User password settings page

(Only visible to administrative users) The *User password settings* page is where you can enforce a minimum complexity on all user passwords, and to configure the advanced password expiry notification period.'

- **Enforce a minimum number of:** Add minimum requirements to user passwords.
  - **Characters:** Minimum number of characters.
  - **Upper case letters:** Minimum number of upper case letters.
  - **Lower case letters:** Minimum number of lower case letters.
  - **Numerical characters:** Minimum amount of numbers.
  - **Special characters:** Minimum number of special characters.
- **Expiry notification period:** Select how many days before the password is going to expire to notify the user (0-30 days).

System task - General settings - Activity trails page

(Only visible to administrative users) The *Activity trails* page allows you to select which types of user-related activity (events triggered by users) are recorded in the database, and available for reporting in the *Activity trails* task.

System task - General settings - Audio page

(Only visible to administrative users) The *Audio* page shows all the sound bites (.wav files) available to your system that can alert you when you receive a new alarm, or that you can use with the *Play a sound* action.

- **Play:** Play the sound bite.
- **Stop:** Stop playing the sound bite.

System task - General settings - Threat levels page

(Only visible to administrative users) The *Threat levels* page lists all threat levels configured in your system, allows you to add new ones, and allows you to modify and delete existing ones.

- **Threat level:** Threat level name.
- **Description:** Threat level description.
- **Color:** Color identifying this threat level. The Security Desk background turns to this color when the threat level is set at the system level.
- **Activation actions:** Number of actions in the threat level activation list. These actions are executed by the system when the threat level is set.
- **Deactivation actions:** Number of actions in the threat level deactivation list. These actions are executed by the system when the threat level is cleared.

System task - General settings - Incident categories page

(Only visible to administrative users) The *Incident categories* page allows you to define categories that can then be selected when reporting incidents in Security Desk.

- **Add category:** The green plus sign allows you to type in categories that can serve as a logical grouping of your incidents such as theft, internal affairs, suspicious activities, etc. They will be used in Security Desk when the incident is created.
- **Remove category:** The red X allows you to delete the selected category.
- **Edit category:** The pencil allows you to modify the selected category name.

System task - General settings - Features page

(Only visible to administrative users) To simplify the user interface, the *Features* page allows you to turn off features you are not using in your system, although they are supported by your license. You can only select from features that are supported by your license. Unsupported features are not listed.

Access control task - General settings view

This section lists the settings found in the *General settings* view of the Access control task.

The *Access control – General settings* view lets you configure the general settings pertaining to access control, and to install and configure custom card formats.

- **Trigger event 'Entity is expiring soon':** Turn this option on (default=off) to have Security Center generate the *Entity is expiring soon* event *n* days before a cardholder or a credential expires, which can trigger an action to warn someone about the upcoming expiry.
- **Create incident before door state override:** Turn this option on (default=off) to prompt the Security Desk user to report an *incident* every time they lock or unlock a door manually, or override the unlock schedule assigned to the door.
- **Card request reasons:** Add reasons that users can choose from to explain why they are requesting a credential card to be printed (for example, no printer on site).
- **Maximum picture file size:** Set the maximum file size (default=20 KB) for pictures (such as a cardholder picture) stored in the Directory database to save disk space.
- **Custom card formats:** Lists the custom card formats defined in your system, and allows you to add, delete, or modify them.

51

Events and actions

This section includes the following topics:

Event types

All events in Security Center are associated with a *source entity*, which is the main focus of the event.

Security Center supports the following event types:

Event	Source entity	Description
Ability to write on a drive has been restored	Archiver or Auxiliary Archiver role	Ability to write on a drive has been restored.
Access denied: Antipassback violation	door	A cardholder requested access to an area that they have already entered, or requested access to leave an area that they were never in.
Access denied: A second cardholder is required	door	Two cardholders must present their credentials within a certain delay of each other and the delay has expired. This event only applies to doors controlled by Synergis™ units.
Access denied: Denied by access rule	door or elevator	The cardholder is denied access according to the access rule.
Access denied: Escort is required	door	In a visitor escort scenario, the escort failed to present their credential within the specified time limit.
Access denied: Escort not supported by this unit model	door	The visitor escort rule is enforced on an area, but the unit controlling its doors does not support this feature.
Access denied: Expired credential	cardholder, credential, door, or elevator	An expired credential has been used.
Access denied: First-person-in rule supervisor absent	door	The first-person-in rule has been enforced on the area, and no supervisor has arrived yet.
Access denied: Inactive cardholder	cardholder, door, or elevator	A cardholder with an inactive profile has attempted to access a door or elevator.
Access denied: Inactive credential	cardholder, credential, door, or elevator	A credential with an inactive profile has been used.
Access denied: Insufficient privileges	door or elevator	The cardholder is denied access because they do not have the required security clearance. This event only applies to doors controlled by Synergis™ units.
Access denied: Interlock	door	Access is denied because of an interlock constraint.
Access denied: Invalid PIN	door or elevator	The cardholder entered an invalid PIN.

Event	Source entity	Description
Access denied: Lost credential	cardholder, credential, door, or elevator	A credential that has been declared as lost has been used.
Access denied: No access rule assigned	door or elevator	The cardholder is denied access because they are not assigned any access rights.
Access denied: Out of schedule	door or elevator	The access rule associated with this cardholder does not apply during this date/time in the schedule.
Access denied: Stolen credential	cardholder, credential, door, or elevator	A credential that has been declared as stolen has been used.
Access denied: Unassigned credential	credential, door, or elevator	A credential has been used that has not been assigned to a cardholder has been used.
Access denied: Unknown credential	door or elevator	A credential that is unknown in the Security Center system has been used.
Access denied: Valid card, invalid PIN	door or elevator	A card and PIN are required to enter an area, and the cardholder entered an invalid PIN.
Access denied: Visitor's companion was denied	door	In a visitor escort scenario, one of the visitors or their escort has been denied access.
Access granted	cardholder, door, or elevator	Access has been granted through a door to a cardholder according to the access rules governing the door, elevator, or area. For a perimeter door of an interlock: When an authorized cardholder accesses a door of an interlock, Security Center might generate an *Access granted* event for the door even though the door does not unlock (due to another perimeter door already being open).
AC fail	access control unit or intrusion detection unit	AC (alternating current) has failed.
A door of an interlock has an unlock schedule configured	area	A door that is part of an interlock configuration has an unlock schedule configured. This invalidates the interlock.
A door of an interlock is in maintenance mode	area	A door that is part of an interlock configuration is in maintenance mode. This disables the interlock.
Alarm acknowledged	alarm	An alarm has been acknowledged by a user, or auto-acknowledged by the system.
Alarm acknowledged (alternate)	alarm	An alarm has been acknowledged by a user using the alternate mode.

Event	Source entity	Description
Alarm being investigated	alarm	An alarm with a acknowledgment condition that is still active has been put into the *under investigation* state.
Alarm condition cleared	alarm	The acknowledgment condition of an alarm has been cleared.
Alarm forcibly acknowledged	alarm	An administrative user has forced an alarm to be acknowledged.
Alarm triggered	alarm	An alarm has been triggered.
An interlock cannot be in hard antipassback mode	area	An interlock cannot be in hard antipassback mode. This is an illegal configuration.
An interlock cannot have a perimeter door with no door sensor configured	area	Interlock cannot be enforced if the system cannot tell whether a door is open or not.
An interlock cannot have only one perimeter door	area	You need at least two perimeter doors for interlock to be applied.
Antipassback disabled: Invalid settings	area	Antipassback disabled: Invalid settings.
Antipassback disabled: Not supported when unit is in server mode	area	Units have not been set to server mode. Antipassback is available according to the unit's operating mode. For more information about unit limitations, see the *Security Center Release Notes.*
Antipassback disabled: Unit is offline	area	At least one unit is in offline mode, disabling antipassback. Antipassback is available according to the unit's operating mode. Refer to the *Security Center Release Notes* for more information about unit limitations.
Antipassback violation	area or cardholder	An access request was made to enter an area with a credential that is already inside the area, or to exit an area with a credential that was never in the area.
Antipassback violation forgiven	cardholder	A security operator has granted access to a cardholder responsible for a passback violation.
Application connected	application or role	An application or a role has connected to the Directory.
Application lost	application or role	An application or a role has lost its connection to the Directory.
Archive folder path is too long	Archiver or Auxiliary Archiver role	The disk base path for video archives has exceeded the maximum length permitted by the operating system.

Event	Source entity	Description
Archiving disk changed	Archiver or Auxiliary Archiver role	The **Allotted space** on one of the disks assigned for archive storage for this Archiver has been used up, and the Archiver has switched to the next disk in line. The names of the previous disk and current disk are indicated in the **Description** field.
Archiving queue full	camera	A camera (video encoder) is streaming video faster than the Archiver is able to write the video packets to disk. A problem with the Archiver database also triggers this event. The name of the camera whose packets are lost is indicated in the **Description** field.
Archiving stopped	Archiver or Auxiliary Archiver role	Archiving has stopped because the disks allocated for archiving are full. This event always accompanies a *Disk full* event.
Asset moved	asset	An asset has been moved.
Asset offline	asset	The RFID tag of an asset has gone offline.
Asset online	asset	The RFID tag of an asset has gone online.
Audio alarm	camera	A sound has been picked up by a microphone associated to a camera.
Badge printing job cancelled	user	A user has cancelled a badge printing job.
Badge printing job completed	user	A user has completed a badge printing job.
Badge printing job queued	user	A user has queued a badge printing job.
Battery fail	access control unit or intrusion detection unit	The unit battery has failed.
Block camera started	camera	A user has blocked a video stream from other users in the system.
Block camera stopped	camera	A user has unblocked a video stream from other users in the system.
Camera not archiving	camera	The camera is on an active archiving schedule but the Archiver is not receiving the video stream.
Camera tampering	camera (video analytics)	A dysfunction has occurred, potentially due to camera tampering, resulting in a partial or complete obstruction of the camera view, a sudden change of the field of view, or a loss of focus.

Event	Source entity	Description
Cannot write on the specified location	Archiver or Auxiliary Archiver role	The Archiver cannot write to a specific drive. The path to the drive is indicated in the **Description** field.
Cannot write to any drive	Archiver or Auxiliary Archiver role	The Archiver is unable to write to any of the disk drives. This situation can arise for the following reasons: When write accesses to shared drives are revoked. When shared drives are inaccessible. When shared drives no longer exist. When this happens, archiving is stopped. The Archiver re-evaluates the drive status every 30 seconds.
Credential has expired	credential	A credential has expired.
Credential is expiring soon	credential	A credential is within *n* days of expiring. The credential expiry notification threshold is configured in the *General settings* tab of the Access control task.
Custom event	system-wide	A custom event is an event added after the initial system installation. Events defined at system installation are called system events. Custom events can be user-defined or automatically added through plugin installations. Unlike system events, custom events can be renamed and deleted.
Database lost	Archiver or Auxiliary Archiver role	The connection to the role database was lost. If this event is related to a role database, it might be because the data server is down or cannot be reached by the role server. If the event is related to the Directory database, the only action you can use is *Send an email* because all other actions require a working connection the Directory database.
Database recovered	Archiver or Auxiliary Archiver role	The connection to the role database has been recovered.
Deadbolt locked	zone	The deadbolt on a door has been locked.
Deadbolt unlocked	zone	The deadbolt on a door has been unlocked.
Direction alarm	camera (video analytics)	A direction alarm has been triggered on a camera equipped with video analytics capabilities.

Event	Source entity	Description
Disk load threshold exceeded	Archiver or Auxiliary Archiver role	The disk space allocated for archiving has exceeded its load threshold (default=80%). This is caused by under-evaluating the disk space required, or by another application that is taking more disk space than it should. If 100% of the allotted disk space is used, the Archiver starts to delete old archive files prematurely in order to free disk space for new archive files, starting with the oldest files.
Disks full	Archiver or Auxiliary Archiver role	All disks allotted for archiving are full and the Archiver is unable to free disk space by deleting existing video files. This event can occur when another application has used up all the disk space reserved for Security Center, or when the **Delete oldest files when disks full** option is not selected in the Server Admin. When this happens, archiving is stopped. The Archiver re-evaluates the disk space every 30 seconds.
Door closed	door	The door has closed. For this event to be generated, the door must be equipped with a door sensor.
Door forced open	door	The door is locked but the door sensor indicates that the door is open.
Doorknob in place	zone	The doorknob is in place and the door is closed.
Doorknob rotated	zone	The doorknob has rotated.
Door locked	door	The door has locked.
Door maintenance completed	door	The door has been taken out of maintenance mode.
Door maintenance started	door	The door has been put into maintenance mode.
Door manually unlocked	door	In Security Desk, a user has manually unlocked a door.
Door offline: Device is offline	door	One or more devices associated to this door has gone offline.
Door opened	door	The door has opened. For this event to be generated, the door must be equipped with a door sensor.
Door open too long	door	The door has been held open for too long. To enable this event, you must set the property “Trigger a ‘Door open too long’ event” in the *Properties* tab of a Door entity in Config Tool.

Event	Source entity	Description
Door unlocked	door	The door has been unlocked.
Edge storage medium failure	camera	After a unit was restarted, the video that was recorded on the edge could not be accessed.
Elevator offline: Device is offline	elevator	One or more devices associated to this elevator has gone offline.
End of camera tampering	camera (video analytics)	A dysfunction caused by camera tampering has been resolved.
Entity has expired	credential	A credential or its associated cardholder has expired (its status is now *Expired*).
Entity is expiring soon	credential	Security Center generates this event to warn you that the expiry date of an entity is approaching. The number of days of advance warning provided by this event must be set.
Entity warning	any entity	A health warning has been issued for this entity.
Entry assumed	cardholder or door	A cardholder was granted access to a door or area, and it is assumed that they entered because no entry sensor is configured.
Entry detected	cardholder or door	A cardholder was granted access to a door or area, and their entry is detected. For this event to be generated, you must configure an entry sensor on the door side where you want entry to be detected.
Face detected	camera (video analytics)	A face has been detected on a camera equipped with video analytics capabilities.
File deleted	camera	A video file associated to a camera has been deleted because the retention period has ended, or the archive storage disk was full.
Firmware upgrade failed	access control unit	A firmware upgrade on a Synergis™ unit has failed.
Firmware upgrade started	access control unit	A firmware upgrade on a Synergis™ unit has been started.
Firmware upgrade succeeded	access control unit	A firmware upgrade on a Synergis™ unit has completed successfully.
First person in	area	A cardholder has entered an empty area.
Floor accessed	elevator	An elevator floor button has been pressed.
Glass break	zone	Glass has broken.

Event	Source entity	Description
Hardware tamper	access control unit, door, elevator, or zone	The tamper input on a unit has been triggered.
Health event	Health monitor role	A health event has occurred.
Input alarm activated	input on intrusion detection unit	The input has entered an *alarm* state.
Input alarm restored	input on intrusion detection unit	The input has left an *alarm* state.
Input bypass restored	input on intrusion detection unit	The input has left a *bypassed* state.
Input bypassed	input on intrusion detection unit	The input has entered a *bypassed* state.
Input state changed: Input active	input on camera, access control unit, or intrusion detection unit	The input has entered an *active* state.
Input state changed: Input normal	input on camera, access control unit, or intrusion detection unit	The input has entered a *normal* state.
Input state changed: Input trouble	input on access control unit or intrusion detection unit	The input has entered a *trouble* state.
Interlock is not supported by the unit	area	Interlock is enabled on an area but the access control unit controlling the doors does not support this feature.
Interlock lockdown off	area	Interlock lockdown has been turned off.
Interlock lockdown on	area	Interlock lockdown has been turned on.
Interlock override off	area	Interlock override is off.
Interlock override on	area	Interlock override is on.
Intrusion detection area alarm activated	intrusion detection area	Intrusion detection area alarm activated.
Intrusion detection area arming	intrusion detection area	Intrusion detection area is being armed.
Intrusion detection area arming postponed	intrusion detection area	Intrusion detection area arming is postponed.

Event	Source entity	Description
Intrusion detection area cancelled alarm	intrusion detection area	Intrusion detection area alarm is cancelled.
Intrusion detection area cancelled postponed request	intrusion detection area	Intrusion detection area postponed request is cancelled.
Intrusion detection area disarmed	intrusion detection area	Intrusion detection area is disarmed.
Intrusion detection area disarm request	intrusion detection area	Intrusion detection area postponed request is cancelled.
Intrusion detection area duress	intrusion detection area	Intrusion detection area is disarmed with duress.
Intrusion detection area entry delay activated	intrusion detection area	Intrusion detection area entry delay activated.
Intrusion detection area forced arming	intrusion detection area	Intrusion detection area is forcefully armed.
Intrusion detection area input bypass activated	intrusion detection area	Intrusion detection area input bypass is activated.
Intrusion detection area input bypass deactivated	intrusion detection area	Intrusion detection area input bypass is deactivated.
Intrusion detection area input trouble	intrusion detection area	Intrusion detection area input trouble.
Intrusion detection area master armed	intrusion detection area	Intrusion detection area is master armed.
Intrusion detection area master arm request	intrusion detection area	Intrusion detection area master arm request is issued.
Intrusion detection area perimeter armed	intrusion detection area	Intrusion detection area is perimeter armed.
Intrusion detection area perimeter arm request	intrusion detection area	Intrusion detection area perimeter arm request is issued.
Intrusion detection area postponed arming request	intrusion detection area	Intrusion detection area arming request is postponed.
Intrusion detection unit input bypass activated	intrusion detection unit	Intrusion detection unit input bypass is activated.
Intrusion detection unit input bypass deactivated	intrusion detection unit	Intrusion detection unit input bypass is deactivated.
Intrusion detection unit input trouble	intrusion detection unit	Intrusion detection unit input trouble.

Event	Source entity	Description
Intrusion detection unit tamper	intrusion detection unit	Intrusion detection unit has been tampered with.
Invalid configuration in unit	video unit	The configuration of the unit is invalid.
Invalid custom encryption values	Archiver or Auxiliary Archiver role	This warning is issued by the Archiver on start-up and every 5 minutes if one of the custom encryption values (initial fingerprint or encryption key) specified in the Server Admin is invalid.
Last person out	area	The last cardholder has exited an area.
License plate hit	Any hit rule	A license plate read has been matched to a hotlist, an overtime rule, or a permit restriction.
License plate read	LPR unit or Patroller	A license plate has been read.
Live bookmark added	camera	A user has added a bookmark to a live video.
Lock released	zone	Event related to a zone entity.
Lock secured	zone	Event related to a zone entity.
Loitering	camera (video analytics)	Loitering activity has been detected in the camera.
Low battery	asset	The battery on the RFID tag of an asset is about to run out.
Macro aborted	macro	Execution of a macro has failed.
Macro started	macro	Execution of a macro has begun.
Manual station activated	door	Someone has pulled the door emergency release (manual pull station).
Manual station reverted to normal state	door	The door emergency release (manual pull station) has been restored to it normal operating position.
Marco completed	macro	Execution of a macro has been completed normally.
Motion	camera	There is motion detected.
Motion off	camera	This event is issued following a *Motion on* event when motion (measured in terms of number of motion blocks) has dropped below the “motion off threshold” for at least 5 seconds.
Motion on	camera	This event is issued when positive motion detection has been made.

Event	Source entity	Description
Multiple units are configured for the interlock	area	All doors that are part of an interlock configuration must be controlled by the same unit.
No entry detected	cardholder or door	A cardholder was granted access to a door or area, but no entry is detected. For this event to be generated, you must configure an entry sensor on the door side where you want entry to be detected.
No match	hotlist	A vehicle has not been matched to the hotlist associated to the Sharp unit.
No RTP packet lost in the last minute	camera	The Archiver has received all the RTP packets in the last minute.
Object condition changed	camera (video analytics)	An object has suddenly changed direction or speed, such as when a person starts running or slips.
Object crossed line	camera (video analytics)	An object has crossed a predefined tripwire.
Object detected	camera (video analytics)	An object is in the camera field of view.
Object entered	camera (video analytics)	An object has entered the camera field of view.
Object exited	camera (video analytics)	An object has exited the camera field of view.
Object following route	camera (video analytics)	An object is following a predetermined route, in a specific direction.
Object left	camera (video analytics)	An object has entered and exited the camera field of view.
Object merged	camera (video analytics)	Two separate objects in the camera field of view have merged.
Object removed	camera (video analytics)	An object has been removed from the camera field of view.
Object separated	camera (video analytics)	An object within the camera field of view has separated into two objects.
Object stopped	camera (video analytics)	A moving object has stopped.
Offload failed	Patroller	An offload from Patroller to Security Center has failed.

Event	Source entity	Description
Offload successful	Patroller	An offload from Patroller to Security Center was successful.
People counting disabled: Unit is offline	area	A unit has gone offline, thus disabling people counting.
People count reset	area	The number of people counted in an area has been reset to *0*.
Person falling	camera (video analytics)	A person falling has been detected in the camera.
Person running	camera (video analytics)	A person running has been detected in the camera.
Person sliding	camera (video analytics)	A person sliding has been detected in the camera.
Playback bookmark added	camera	A user has added a bookmark to a recorded video.
Protection threshold exceeded	Archiver or Auxiliary Archiver role	The *Protected video threshold* configured from the Archiver has been exceeded. You can monitor the percentage of disk space occupied by protected video files from the Statistics page in the Archiver's Resources tab in Config Tool.
PTZ activated	camera (PTZ)	A user started using the PTZ after it has been idle. The *Description* field indicates the user who activated the PTZ. This event is regenerated every time a different user takes control of the PTZ, even when the PTZ is still active.
PTZ locked	camera (PTZ)	A user has tried to move the PTZ while it is being locked by another user with a higher PTZ priority. The *Description* field indicates the machine, application type, and user who currently holds the lock.
PTZ stopped	camera (PTZ)	The PTZ has not been manipulated by any user after a predetermined period of time. The *Description* field indicates the user who last used the PTZ.
PTZ zoom by user	camera (PTZ)	A user started zooming the PTZ. The Description field indicates the user who performed the zoom. Subsequent *PTZ zoom by user* events are generated if another user zooms the PTZ, or if the original user zooms the PTZ after the *Idle delay* has expired.
PTZ zoom by user stopped	camera (PTZ)	The PTZ has not been zoomed by any user after a predetermined period of time. The *Description* field indicates the user who last zoomed the PTZ.

Event	Source entity	Description
Receiving RTP packets from multiple sources	camera	The Archiver is receiving more than one video stream for the same camera. **IMPORTANT**: When this rare situation arises, the Archiver cannot tell which stream is the correct one simply by looking at the source IP address because of the NAT (Network Address Translation), so an arbitrary choice is made. This can result in the wrong video stream being archived. However, the source IP address and port number of both streams are indicated in the *Description* field, and the two sources are labeled *Archived* and *Rejected*. You can find the faulty unit that is causing this conflict.
Recording started (alarm)	camera	The recording on a camera has been started as the result of an alarm being triggered.
Recording started (continuous)	camera	The recording on a camera has been started by a continuous archiving schedule.
Recording started (external)	camera	The recording on a camera has been started by the *Start recording* action. This action could have been triggered by another event or executed from a macro.
Recording started (motion)	camera	The recording on a camera has been started through motion detection.
Recording started (user)	camera	The recording on a camera has been started manually by a user.
Recording stopped (alarm)	camera	The recording on a camera has stopped because the alarm recording time has elapsed.
Recording stopped (continuous)	camera	The recording on a camera has stopped because it is no longer covered by a continuous archiving schedule.
Recording stopped (external)	camera	The recording on a camera has been stopped by the Stop recording action. This action could have been triggered by another event or executed from a macro.
Recording stopped (motion)	camera	The recording on a camera has stopped because the motion has ceased.
Recording stopped (user)	camera	The recording on a camera has been stopped manually by a user.

Event	Source entity	Description
Request to exit	door	Someone has pressed the door release button or has triggered a request to exit motion detector. The *Request to exit* event has special filtering to make this feature compatible with motion detection request to exit hardware. Set these properties in the **Config Tool** > **Door** > **Properties** tab.
Request to exit normal	door	No request to exit is being made.
RTP packets lost	camera	There are RTP packets that the Archiver never received. This could happen if the packets have been lost on the network, or if the Archiver does not have enough CPU to process all the packets received on the network card. The *Description* field indicates the number of packets lost since the last time this event was issued (no more than once every minute).
Scheduled controlled access	elevator	The schedule for controlled access to elevator floors now applies.
Scheduled free access	elevator	The schedule for free access to elevator floors now applies.
Scheduled lock	door	The door unlock schedule has expired, the lock is now re-asserted (door is locked).
Scheduled unlock	door	The door lock is unlocked due to a programmed unlock schedule.
Schedule unlock ignored: first-person-in rule supervisor absent	door	The door unlock schedule is ignored because the restriction imposed by the first-person-in rule has not yet been satisfied.
Signal lost	camera	The camera signal has been lost.
Signal recovered	camera	The camera signal has been recovered.
Synchronization completed: External system	Active Directory role	The synchronization of an external system has completed.
Synchronization error: External system	Active Directory role	The synchronization of an external system has resulted in an error.
Synchronization started: External system	Active Directory role	The synchronization of an external system has started.
Tailgating	camera (video analytics)	Two people have entered a secured area following each other very closely.
Temperature alarm	video unit	The temperature of the video unit has risen above the safety level.

Event	Source entity	Description
Threat level cleared	System, area	A threat level has been cleared on your system or on specific areas.
Threat level set	System, area	A threat level has been set on your system or on specific areas.
Transmission lost	camera	The Archiver is still connected to the camera, but it has not received any video packets for more than 5 seconds.
Transmission recovered	camera	The Archiver has started to receive video packets from the camera once again.
Undefined video analytics event	camera (video analytics)	A video analytics event has been issued, but it is not yet mapped to a Security Center event.
Unit connected	unit	The connection to a unit has been established or restored.
Unit failed to respond to edge video request	camera	Event related to a camera that is recording directly on the unit.
Unit lost	unit	The connection to a unit has been lost.
Unit synchronization failed	access control unit	The synchronization of the unit with the Access Manager has failed.
Unit synchronization started	access control unit	The synchronization of the unit with the Access Manager has started.
Unit synchronization succeeded	access control unit	The synchronization of the unit with the Access Manager has completed successfully.
Updated published	Patroller, Mobile Sharp	An update has been processed, and is ready to be deployed to Patroller.
Update failed	Patroller, Mobile Sharp	An update on Patroller or a Mobile Sharp unit has failed, or a file could not be synchronized on a Patroller computer.
Update installation completed	Patroller, Mobile Sharp	An update has completed on Patroller or a Mobile Sharp unit, and no reboot is required.
Update installation started	Patroller, Mobile Sharp	A user has started an updated on Patroller by clicking the “Update” icon.
Update uninstallation completed	Patroller, Mobile Sharp	A rollback on Patroller or a Mobile Sharp unit has completed.
Update uninstallation started	Patroller, Mobile Sharp	A user has started a rollback on Patroller by clicking the “Rollback” icon.

Event	Source entity	Description
User logged off	user	A user has logged off of a Security Center application.
User logged on	user	A user has logged on to a Security Center application.
VRM connection attempt	Archiver role	The Archiver has attempted to connect to a VRM unit.
VRM connection failure	Archiver role	The Archiver has failed to connect to a VRM unit.
Window closed	zone	A physical window has closed.
Window opened	zone	A physical window has opened.
Zone armed	zone	A zone has been armed.
Zone disarmed	zone	A zone has been disarmed.
Zone maintenance completed.	I/O zone	An I/O zone has been taken out of maintenance mode.
Zone maintenance started	I/O zone	An I/O zone has been put into maintenance mode.
Zone offline	hardware zone	A hardware zone is offline.

Action types

All *actions* in Security Center are associated with a target entity, which is the main entity affected by the action. Additional parameters are indicated in the *Description* column. All parameters must be configured for an action to be valid.

Action	Description
Add bookmark	Adds a *bookmark* to a *camera* recording. Parameters: • **Camera:** Select the camera. • **Message:** Bookmark text.
Arm intrusion detection area	Arms an *intrusion detection area*. Parameters: • **Intrusion detection area:** Select the intrusion detection area. • **Mode:** Either *Master arm* or *Perimeter arm*. • **When:** Either immediately or with a delay.
Arm zone	Arms a *virtual zone*. Parameter: • **Zone:** Select a virtual zone.
Block and unblock video	Blocks or unblocks a camera from other users in the system. Parameters: • **Block/Unblock:** Select whether the action will block or unblock the camera. • **Camera:** Select the camera. • **End:** Select how long to block the video for: • **For:** The video is blocked from users for the selected amount of time. • **Indefinitely:** The video is blocked from users until you manually unblock it. • **User level:** Select a minimum user level. All users with a level lower than the one you select are blocked from viewing video.
Cancel postpone intrusion detection area arming	Cancels the postponed arming of an *intrusion detection area*. Parameter: • **Intrusion detection area:** Select the intrusion detection area.

Action	Description
Clear tasks	Clears the task list in the specified Security Desk monitors. Parameters: • **Destination:** Select one of the following: ◦ **User:** All monitors of all Security Desk applications connected with the specified username. ◦ **Monitor:** Specific Security Desk monitor identified by a machine name and a monitor ID.
Disarm intrusion detection area	Disarms an *intrusion detection area*. Parameter: • **Intrusion detection area:** Select the intrusion detection area.
Disarm zone	Disarms a *virtual zone*. Parameter: • **Zone:** Select a virtual zone.
Display a camera on an analog monitor	Displays a camera in an analog monitor in a canvas tile. Parameters: • **Camera:** Select which camera to display in the analog monitor. The camera must be supported by the analog monitor, and use the same video format. • **Analog monitor:** Select an analog monitor to display the camera in.
Display an entity in the Security Desk	Displays a list of entities in the Security Desk *canvas* of selected *users*, in terms of one entity per tile. This action is ignored if a user does not have a *Monitoring* task open in Security Desk. Parameters: • **Recipients:** Select the users. • **Entities:** List of entities to display. Each entity is displayed in a separate tile. • **Display options:** Select one of the following: ◦ **View in a free tile:** Only use free tiles. ◦ **Force display in tiles:** Display in free tiles first. When there are no more free tiles, use the busy tiles following the tile ID sequence.
Email a report	Sends a report (based on a saved reporting task) as an email attachment to a list of *users*. Parameters: • **Report:** Select a saved public task. • **Recipients:** Select the users to the send the report to. • **Export format:** Report format, either *PDF* or *Excel*.

Action	Description
Email a snapshot	Sends a series of snapshots of a video feed as an email attachment to a list of users. Parameters: • **Camera:** Select the camera. • **Snapshots:** Select how many seconds before (maximum -300 seconds) or after (maximum 5 seconds) the defined *Recurrence time* to email the snapshot. • **Recipients:** Select the users who will receive the snapshot. An email address must be defined in the user's settings. • **Export format:** Available image formats: *PNG*, *GIF*, *JPEG*, or *Bitmap*.
Export report	Generates and saves a saved public task to a file location. Parameters: • **Report:** Select a saved public task. • **Export format:** Select the file format (CSV, Excel, or PDF). • **Orientation:** (PDF only) Select whether the PDF file should be in portrait or landscape mode. • **Overwrite existing file:** Select whether to overwrite a previously saved report in the destination folder.
Forgive antipassback violation	Forgives an *antipassback* violation for a *cardholder*, or *cardholder group*. Parameter: • **Entity:** Select a cardholder or cardholder group.
Go home	Commands the PTZ camera to go to its home position. Not all PTZ cameras support this feature. Parameter: • **Camera:** Select a PTZ camera.
Go to preset	Commands the PTZ camera to go to the specified preset position. Parameters: • **Camera:** Select a PTZ camera. • **Preset:** Preset position (number) to go to.
Import from file	Imports a file and sends the import results to a *user*. Parameters: • **Recipient:** Select a user. • **File name:** Opens the Import tool window, where you can select the file that is used to import the data.

Action	Description
Override with event recording quality	Sets the *Boost quality on event recording* to *ON* for the selection camera and applies the custom boost quality recording settings. Selecting this option overrides the general settings for event recording. The effect of this action lasts as long as it is not modified by another action, such as *Recording quality as standard configuration*, or until the Archiver restarts. Parameter: • **Camera:** Select a camera.
Override with manual recording quality	Sets the *Boost quality on manual recording* to *ON* for the selection camera and applies the custom boost quality recording settings. Selecting this option overrides the general settings for event recording. The effect of this action lasts as long as it is not modified by another action, such as *Recording quality as standard configuration*, or until the Archiver restarts. Parameter: • **Camera:** Select a camera.
Play a sound	Plays a sound bite in a user or user group's Security Desk. This action is ignored if the user is not running Security Desk. Parameters: • **User, User group:** Select a user or user group. • **Sound to play:** Sound file (.wav) to play. For the user to hear the sound bite, the same sound file must be installed on the PC where Security Desk is running. The standard alert sound files that come with the installation are located in *C:\Program files\Genetec Security Center 5.5\Audio*.
Postpone intrusion detection area arming	Postpones the intrusion detection area arming. Parameters: • **Arming mode:** Either *Master arm* or *Perimeter arm*. • **Intrusion detection area:** Select the intrusion detection area. • **Postpone for:** Set how long to postpone the arming for, in seconds. • **Arming delay:** Set the arming delay in seconds.
Reboot unit	Restarts a unit. Parameters: • **Entity:** Select a video unit or access control unit to restart.
Recording quality as standard configuration	Cancels the effect of the *Override with manual recording quality* and *Override with event recording quality* actions and restores the standard recording configuration. Parameter: • **Camera:** Select a camera.

Action	Description
Reset area people count	Resets the people counter in an *area*. Parameter: • **Area:** Select an area.
Reset external system	Forces the Omnicast™ Federation™ role to reconnect to the remote *Omnicast* system. Parameter: • **Role:** Select an Omnicast™ Federation™ role.
Run a macro	Starts the execution of a *macro*. Parameters: • **Macro:** Select a macro. • **Context:** Specific value settings for the context variables.
Run a pattern	Commands the PTZ camera to run the specified pattern. Parameters: • **Camera:** Select a PTZ camera. • **Pattern:** Pattern number to run.
Send a message	Sends a pop-up message to a user's Security Desk. This action is ignored if the user is not running Security Desk. Parameters: • **Recipients:** Select a user or user group. • **Message:** Text to be to displayed in the pop-up message. • **Has timeout:** Select how long the message is shown for.
Send an email	Sends an email to users or cardholders. The selected user must have an email address configured, and the mail server must be properly configured for Security Center, or the action is ignored. Parameters: • **Recipients:** Select a user, user group, cardholder, or cardholder group. • **Message:** The email text to be sent to the recipient.
Send task	Sends and adds a public task to aSecurity Desk application. Parameters: • **Task:** Select a saved public task to send. • **Destination:** Select one of the following: • **User:** All Security Desk connected with that user. • **Monitor:** Specific Security Desk monitor identified by a machine name and a monitor ID.

Action	Description
Set reader mode	Sets the reader mode for accessing doors. Parameters: • **Location:** Select an area, door, or elevator. • **Reader mode:** Select whether access is granted using *Card and PIN*, or *Card or PIN*, for the selected area, door, or elevator. This action only works with door controllers and readers that support this feature.
Set the door maintenance mode	Sets the *Unlocked for maintenance* status of a *door* to on or off. Parameters: • **Door:** Select a door. • **Maintenance:** Desired maintenance mode (On or Off).
Set threat level	Sets a threat level on your Security Center system, or on specific areas. Parameters: • **Area:** Select which areas to set the threat level on. Can be your entire system, or specific areas. • **Threat level:** Select which threat level to set.
Silence buzzer	Resets the Buzzer output defined for a door. This action sets the *Buzzer* option to *None* in the *Hardware* tab of a door in Config Tool. Parameter: • **Door:** Select a door.
Sound buzzer	Sets the Buzzer output defined for a door. The buzzer sound is specified under the *Buzzer* option in the *Hardware* tab of a door in Config Tool. Parameter: • **Door:** Select a door.

Action	Description
Start applying video protection	Starts protecting upcoming video recordings against deletion. The protection is applied on all *video files* needed to store the protected *video sequence*. Since no video file can be partially protected, the actual length of the protected video sequence depends on the granularity of the video files. When multiple *Start applying video protection* actions are applied on the same video file, the longest protection period is kept. Parameters: • **Camera:** Select a camera. • **Keep protected for:** Duration of the video protection. • **Specific:** Sets the protection period in number of days. • **Infinite:** The protection can only be removed manually from the *Archive storage details* task. • **Protect video for next:** Duration of the video to protect. • **Specific:** Sets the duration in minutes and hours. • **Infinite:** All future recordings are protected until the action *Stop applying video protection* is executed.
Start recording	Starts recording on the specified camera. This action is ignored if the camera is not on an active recording schedule. Recordings started by this action cannot be stopped manually by a user. Parameters: • **Camera:** Select a camera. • **Recording duration:** Sets the duration of the video recording. • **Default:** Sets the duration to follow the value defined in *Default manual recording length* configured for the camera. • **Infinite:** The recording can only be stopped by the *Stop recording* action. • **Specific:** Sets the recording duration in seconds, minutes, and hours.
Start transfer	Starts an archive transfer. Parameters: • **Transfer group:** Select a transfer group to begin the transfer for. The transfer can consist of retrieving video recordings from units, duplicating video archives from one Archiver to another Archiver, or backing up archives to a specified location.
Stop applying video protection	Stops protecting upcoming video recordings against deletion. This action does not affect the *video archives* that are already protected. Additional parameter: • **Camera:** Select a camera. • **Stop in:** Sets the video protection to stop *Now* or in a *Specific* amount of time in minutes and hours.

Action	Description
Stop recording	Stops recording on the specified camera. This action only works if the recording was started by the *Start recording* action. Parameters: • **Camera:** Select a camera. • **Stop in:** Sets the recording to stop *Now* or in a *Specific* amount of time in seconds, minutes and hours.
Stop transfer	Stops an archive transfer. Parameters: • **Transfer group:** Select a transfer group to stop the transfer for.
Synchronize role	Starts a synchronization process on the specified role (*Active Directory* or *Global Cardholder Synchronizer*). Parameter: • **Role:** Select a role that needs synchronization. • **Get image:** (Active Directory role only) Enable this option if image attributes are to be synchronized as well.
Temporarily override unlock schedules	Temporarily locks or unlocks a door for a given period of time. Parameters: • **Door:** Select a door. • **Lock mode:** Select *Unlocked* or *Locked*. • **For:** Amount of time in minutes or hours. • **From/To:** Date and time range to unlock the door.
Trigger alarm	Triggers an alarm. This action might generate additional events, depending on the alarm configuration. Parameters: • **Alarm:** Select an alarm. • **Acknowledgement condition:** Event type that must be triggered before the alarm can be acknowledged. • **User acknowledgement required:** Select whether the alarm must be manually acknowledged, or if it is automatically acknowledged by the system after the acknowledgement condition is cleared.
Trigger intrusion alarm	Triggers a physical alarm on an intrusion detection area. Parameters: • **Recipient type:** Type of alarm trigger, either the intrusion detection area or a specific alarm input. • **Intrusion detection area:** Select an intrusion detection area.

Action	Description
Trigger output	Triggers an *output behavior* on an output pin of a *unit*. For example, an action can be configured to trigger the output pin of a unit (controller or input/output module). Parameters: • **Output relay:** Select an output pin (unit). • **Output behavior:** Select the output behavior to trigger.
Unlock door explicitly	Temporarily unlocks a door for five seconds, or the *Standard grant time* configured for that door. Parameter: • **Door:** Select a door.

Appendices

Appendices

This section includes the following topics:

A

License options

This section includes the following topics:

Viewing license information

You can view information about your purchased license, such as your SMA number, license expiration date supported features, and so on, from the About page in Config Tool or from the Server Admin.

To view license information from Config Tool:

1 From the home page, click **About.**

To view license information from Server Admin:

1 Log on to your main server using Server Admin.

2 Click the **Directory** tab, scroll to the **License** section, and click **License information**.

License options in Security Center

This section describes the meaning of all Security Center license options.

Security Center license options

The generic Security Center license options are the following:

- **Macros:** Allows you to create macros in your system.
- **Threat level:** Allows you to create threat levels in Config Tool, as well as set threat levels in Security Desk.
- **Remote Security Desk:** Allows you to remotely monitor and control other Security Desk workstations and monitors, using the *Remote* task on your local Security Desk.
- **Mission Control:** Allows you to use the Mission Control features.
- **Intrusion detection:** Allows you to use intrusion detection functionality in Security Center, such as adding Intrusion Manager roles and intrusion detection units in Config Tool, and receive intrusion alarms in Security Desk.
- **Automatic email notifications:** Allows you to set up an email server for email notifications, including:
  - Receiving email notifications from the *Watchdog*.
  - Using *Send an email* and *Email a report* actions.
- **Web SDK:** Allows you to create Web-based SDK roles.
- **Asset management:** Allows you to use asset management functionality in Security Center in combination with the *RF Code* plugin, which let you define assets you can track and report in Security Desk.
- **Number of custom fields:** Maximum number of custom fields that you are allowed to define.
- **Number of federated systems:** Maximum number of federated systems allowed, counting both Omnicast™ 4.x and Security Center systems.
- **Number of Security Desk connections:** Maximum number of simultaneous Security Desk connections allowed on your system.
- **Number of ADFS integrations:** Maximum number of *Active Directory Federation Services* connections allowed on your system.
- **Number of Active Directories:** Maximum number of Active Directory domains that can be synchronized with your system.
- **Number of additional Directory servers:** Maximum number of Directory servers you can have in addition to your main server to set up a high availability system.
- **Number of intrusion detection units:** Maximum number of intrusion panels supported on your system.
- **Number of input points:** Maximum number of inputs that can be configured for *doors*, *elevators*, and *zones*. Only inputs found on dedicated I/O subpanels such as the HID V200 or the Mercury MR16IN, are counted. The integrated inputs found on controller boards are not counted.
- **Number of output relays:** Maximum number of outputs that can be configured for *doors*, *elevators*, and *zones*. Only relays found on dedicated I/O subpanels such as the HID V300 or the Mercury MR16OUT, are counted. The integrated outputs found on controller boards are not counted.
- **Number of cash registers:** Maximum number of cash registers that you can import from an external *point of sale* system.

Synergis™ license options

The *Synergis™* access control options are the following:

- **Card requests:** Allows users to request card credentials to be printed by other users on the system. Also allows you to create request reasons in Config Tool.
- **Import Tool:** Allows you to import cardholders and credentials from a flat file.
- **Antipassback:** Allows you to configure areas with *antipassback* restrictions.
- **People counting:** Allows you to use the *People counting* task in Security Desk.
- **Badge template:** Allows you to define *badge templates* in your system.
- **USB enrollment reader:** Allows you to detect and use USB readers on your system.
- **Visitors:** Allows you to use the *Visitor management* task in Security Desk.
- **Number of cardholders and visitors:** Maximum number of cardholders and visitors allowed on your system, including those imported from Active Directories.
- **Number of readers:** Maximum number of *readers* that can be configured for *doors* and *elevators* on your system.
- **Number of Access Managers:** Maximum number of *Access Manager* roles that can be created on your system.
- **Number of Global Cardholder Synchronizers:** Maximum number of *Global Cardholder Synchronizer* roles running on *sharing guest* systems that are allowed to connect to the *sharing host* at the same time. This license option is used by the *sharing host* to limit the number of connections.

Omnicast™ license options

The *Omnicast™* license options are the following:

- **Number of cameras and analog monitors:** Maximum number of *cameras* and *analog monitors* allowed on your system. Cameras and analog monitors managed locally by your system and those federated from remote systems are counted. Cameras and analog monitors are also cumulative. For example, if you use 5 cameras and 5 analog monitors simultaneously, they will count for 10 entities in the license.
- **Number of promotional cameras:** Number of video channels allowed on your system according to a commercial promotion available at the time of purchase. Video units eligible for such a promotion are using these promotional licenses first. For example, if you purchase camera connections when a promotion applies, the next eligible cameras you add to your system will use the promotional camera licenses up to the limit of *Number of promotional cameras*. When this limit is reached, the next eligible cameras added will use regular camera connections. This applies to the current *Analog Camera Promotion*.
- **Number of OVReady cameras:** Maximum number of OVReady cameras (with *video analytics* capabilities) allowed on your system.
- **Number of panoramic cameras:** Number of panoramic cameras allowed on your system.
- **Number of DVR inputs:** Number of video inputs from DVRs (digital video recorders) allowed on your system.
- **Number of Auxiliary Archivers:** Number of *Auxiliary Archiver* roles allowed on your system.
- **Number of CCTV keyboards:** Number of CCTV keyboards allowed on your system.
- **Number of standby Archiver servers:** Number of *Archiver* roles allowed to have a secondary server assigned for failover.
- **Number of standby Archiver servers per Archiver:** Number of standby servers allowed per Archiver role. This license is required to assign a tertiary server to an Archiver role for failover.
- **Audio:** Allows your system to stream audio and enables all audio features on your system.

- **Forensic search:** Enables the *Forensic search* task in Security Desk.
- **Edge recording:** Enables the capability to transfer data from edge recording units to the Archiver.
- **Camera blocking:** Allows you to block video from other users on the system.
- **Hardware acceleration:** Allows you to use the hardware acceleration feature for video decoding.
- **Number of RTSP streams:** Maximum number of video streams that can be requested simultaneously from the Media Gateway role.
- **Archiver encryption:** Allows you to encrypt video streams.

AutoVu™ license options

The *AutoVu™* LPR license options are the following:

- **Security Desk map:** Type of map engine supported in Security Desk: *Bing* or *BeNomad*.
- **Geocoder:** Type of map engine used by the LPR Manager for geocoding: *Bing* or *BeNomad*.
- **Microsoft Bing license expiration date:** Bing license expiration date.
- **XML import:** Allows you to import data from third-party applications.
- **Number of LPR Managers:** Maximum number of *LPRManager* roles allowed on your system.
- **Number of fixed Sharp analytic streams:** Maximum number of fixed Sharp units allowed on your system.
- **Number of Patrollers - Law Enforcement:** Maximum number of *Patrollers* configured for *Law Enforcement* allowed on your system.
- **Number of Patrollers - City Parking Enforcement:** Maximum number of *Patrollers* configured for *City Parking Enforcement* allowed on your system.
- **Number of Patrollers - University Parking Enforcement:** Maximum number of *Patrollers* configured for *University Parking Enforcement* allowed on your system.
- **Number of Patrollers - MLPI:** Maximum number of *Patrollers* configured for *Mobile License Plate Inventory* allowed on your system.
- **Number of Patrollers equipped with maps:** Maximum number of *Patrollers* equipped with maps allowed on your system.

Plan Manager options

The *Plan Manager* license options are the following:

- **Plan Manager Basic:** Allows you to use Plan Manager in Basic mode.
- **Plan Manager Standard:** Allows you to use Plan Manager in Standard mode.
- **Plan Manager Advanced:** Allows you to use the Advanced configuration of Plan Manager in Advanced mode.

Mobile license options

The *Security Center Mobile* license options are the following:

- **Number of mobile device servers:** Maximum number of *Mobile Servers* allowed on your system.
- **Number of mobile devices:** Maximum number of simultaneous *Mobile app* connections allowed on your system.
- **Number of Web Clients:** Maximum number of *Web Client* connections allowed on your system.

Certificate license options

The *certificate* license options. Each certificate is identified by an application/plugin name and the publisher name. The option specifies the maximum number of simultaneous connections from each type of application allowed on your system.

B

Default Security Center ports

This section includes the following topics:

Common communication ports

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

Computer	Inbound	Outbound	Port usage
Main server	TCP 5500		Directory connection requests
Client workstations (Security Desk and Config Tool)		TCP 5500	Directory connection requests
Client workstations (Config Tool)		TCP 443	Communication with GTAP for SMA validation/ sending feedback
Servers (new installation)	TCP 5500	TCP 5500	Communication with other servers
	TCP 4502	TCP 4502	Backward compatibility. For connections from servers running Security Center 5.3 and earlier.
	HTTP 80		Connection through Server Admin
Servers (upgraded from 5.3 and earlier)	TCP 4502	TCP 4502	If 4502 was the server port before the upgrade, then 4502 remains the server port after the upgrade, and 4503 is used for backward compatibility. If another port was used as server port before the upgrade, then that same port is kept as server port after the upgrade. 4502 is then used for backward compatibility, and 4503 is not necessary.
	TCP 4503	TCP 4503	
Map Manager	HTTPS 8012		Communication with client applications for map downloads.
System Availability Monitor Agent (SAMA)	TCP 4592		Connection from Security Center servers.
		TCP 443	Connection to the Health Service in the Cloud.
Genetec™ Update Service (GUS)	TCP 4595	TCP 4595	Connection from Security Center applications and communication with other GUS servers.
		TCP 443	Connection to the Internet.

AutoVu™-specific ports

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

Computer	Inbound	Outbound	Port usage
LPR Manager		UDP 5000	Fixed Sharp unit discovery
	TCP 8731		Fixed Sharp units and Patrollers
	TCP 8832		Patroller hotfix requests
	TCP 8787		Pay-by-Plate

Synergis-specific ports

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

Computer	Inbound	Outbound	Port usage
Access Manager	UDP/TCP 4070	UDP/TCP 4070	HID VertX/Edge controllers
			HID Vertx/Edge EVO controllers
	TCP 20	TCP 21, 23	HID VertX/Edge controllers
		TCP 4050	HID VertX/Edge controllers
			HID Vertx/Edge EVO controllers
		TCP 22	HID Vertx/Edge EVO controllers
		TCP 2000	Default Synergis™ unit discovery port (this port can be modified in Config Tool)

The *discovery port* of an HID unit is fixed at 4070. Once it is discovered, the unit is assigned to an *Access Manager* that uses the ports shown in the table above to control it.

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

Omnicast-specific ports

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

Computer	Inbound	Outbound	Port usage
Archiver	TCP 555		Live and playback stream requests
	UDP 15000–20000[1]	UDP 15000–20000[1]	Live unicast audio and video streams
	TCP & UDP		Vendor specific ports for events and unit discovery
	UDP 47806	UDP 47806	Live multicast audio and video streams
	UDP 47807	UDP 47807	Live multicast audio and video streams
		TCP 554 or HTTP 80	Typical port used to request video from a unit
	Telnet 5602		Telnet Console connection requests
Auxiliary Archiver	TCP 558		Playback stream requests
Media Router	TCP 554		Live and playback stream requests
Redirector	TCP 560		Live and playback stream requests
	UDP 8000–12000		Live unicast audio and video streams
	UDP 47806	UDP 47806	Live multicast audio and video streams
		TCP 555	Communication with Archiver
RTSP Media Router	TCP 654		Live and playback stream requests
	UDP 51914	UDP 51914	Live multicast audio and video streams
Omnicast™ Federation™	UDP 1024-2048		Security Desk when viewing video from an Omnicast™ Federation™ in Security Center
Client workstations (Security Desk and Config Tool)	UDP 6000–6500		Live unicast audio and video streams
	UDP 47806		Live multicast video streams
	UDP 47807		Live multicast audio streams
		TCP 554–560	Live and playback audio and video requests

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

C

HID reference

This section includes the following topics:

Supported HID hardware

HID Global has two product lines. The newer product line is called EVO, and the older one is called Legacy. There are two product families in each product line: VertX and Edge. Products from different families cannot mix. Security Center supports them all.

About HID controllers

The Access Manager communicates directly with HID controllers over an IP network. Therefore, all HID controllers are called *access control units* in Security Center.

Platform differences between EVO and Legacy

Characteristics	EVO	Legacy
Processor / Speed	ARM9 / 200 Mips	ETRAX / 100 Mips
RAM	64 MB	32 MB
Operating system	Linux 2.6	Linux 2.4
Secure shell and protocol	Yes	No
Maximum event buffer	99,999	5,000

Limitations

On a *Card and PIN* door controlled by an HID Edge EVO unit, if a host lookup is necessary (an unknown credential is entered and the unit must query the Access Manager before making a decision), the cardholder must wait a few seconds after presenting their card, before entering their PIN. Entering the PIN too quickly might result in a denied access because the first few digits of the PIN might not have been registered by the unit.

HID documentation download

You can find all HID product documentation online.

Click on the links below to download desired document.

Product line	Product name	Document links
EVO	VertX EVO V1000	VertX EVO V1000 Network Controller Datasheet VertX EVO V1000 Wiring Example
	VertX EVO V2000	VertX EVO V2000 Reader Interface/Networked Controller Datasheet VertX EVO V2000 Wiring Example
	Edge EVO EH400-K	Edge EVO EH400-K Datasheet
	Edge EVO EHR40-K	Edge EVO EHR40-K Controller/Reader and Module Datasheet
	Edge EVO EHRP40-K	Edge EVO EHRP40-K Controller/Reader and Module Datasheet
Legacy	VertX V1000	VertX V1000 Network Controller Datasheet
	VertX V2000	VertX V2000 Reader Interface/Network Controller Datasheet
	EdgePlus E400	EdgePlus E400 Datasheet
	EdgeReader ER40	EdgeReader ER40 Datasheet
	EdgeReader ERP40	EdgeReader ERP40 Datasheet

Supported HID VertX controllers

HID has two lines of VertX controllers: EVO (newer) and Legacy. The newer line of controllers have significantly more processing power and memory than the older line. Both lines of controllers use the same interface modules (V100, V200, V300) that remain unchanged.

In the following tables, we compare the characteristics of the EVO controllers with that of their Legacy counterparts.

VertX platform differences between EVO and Legacy

Characteristics	EVO	Legacy
Flash memory	256 MB	8 MB
Maximum cardholder capacity[1]	250,000	44,000
Power supply	12 – 24 VDC	12 – 18 VDC
Operating temperature range	32 ° – 120 ° F (0 ° – 49 ° C)	32 ° – 122 ° F (0 ° – 50 ° C)
Humidity tolerance	5% to 85% non-condensing	5% to 95% non-condensing

[1] In Security Center, a cardholder can have multiple credentials. A cardholder with two credentials is counted as two by HID. The VertX controller capacity tested by Genetec Inc. is 22,000 credentials, up to 125,000 credentials with full memory upgrade.

VertX V1000 differences between EVO and Legacy

Characteristics	EVO	Legacy
Maximum current at 12 – 24 VDC per unit	1 A	1 A
Average operating current at 12 VDC	210 mA	140 mA
Downstream device capacity[2]	Up to 32 interface modules (or 64 readers)	Up to 32 interface modules (or 64 readers)
Downstream device compatibility	VertX V100, V200, V300	VertX V100, V200, V300
RTC backup	Coin cell battery	Coin cell battery
RS-232 ports	1	2
USB ports	1 (reserved for future use)	0

[2] HID states that a V1000 controller can support a maximum of 32 downstream interface modules (16 on each RS-485 serial bus). However, the performance tests run by Genetec Inc. indicate that as a “best practice”, 20 downstream interface modules should not be exceeded (10 per serial bus).

VertX V2000 differences between EVO and Legacy

Characteristics	EVO	Legacy
Maximum current at 12 – 24 VDC per unit	1 A	1 A
Average operating current at 12 VDC (0 reader)	125 mA	160 mA
Average operating current at 12 VDC (2 readers)	625 mA	660 mA
Relay outputs	30 VDC, 2 A	30 VDC, 2 A

Supported HID VertX sub-panels

The HID VertX sub-panels (also known as *interface panels*) can be used with either HID VertX V1000 network controllers or Genetec™ access control appliances (Synergis™ Master Controller and Synergis™ Cloud Link).

VertX V100

Characteristics	Specifications
Power supply	9 – 18 VDC
Average operating current at 12 VDC (0 readers)	60 mA
Average operating current at 12 VDC (2 readers)	600 mA
Operating temperature range	32 ° – 122 ° F (0 ° – 50 ° C)
Humidity	5% to 95% non-condensing

VertX V200

Characteristics	Specifications
Power supply	9 – 18 VDC
Average operating current at 12 VDC	50 mA
Resistors for input supervision	1 – 10 kohm
Operating temperature range	32 ° – 122 ° F (0 ° – 50 ° C)
Humidity	5% to 95% non-condensing

VertX V300

Characteristics	Specifications
Power supply	9 – 18 VDC
Average operating current at 12 VDC	60 mA
Relay rating	2 A @ 30 VDC (maximum load)
Operating temperature range	32 ° – 122 ° F (0 ° – 50 ° C)
Humidity	5% to 95% non-condensing

Cable specifications

When attaching the interface modules to their controllers, make sure you do not exceed the recommended cable lengths.

Cable type	Maximum length	Description
Wiegand	500 ft. (152 m) to reader	ALPHA 1299C, 22AWG, 9-conductor, stranded, overall shield. Fewer conductors needed if all control lines are not used.
RS-485	4000 ft. (1220 m) to controller	Belden 3105A, 22AWG twisted pair, shielded 100 Ω cable, or equivalent.
Ethernet	328 ft. (100 m)	Cat5, Cat5E and Cat6.
Hi-O CAN bus	100 ft. (30 m)	22AWG gauge. Maximum between drops 30 ft. (10 m).

Supported HID Edge controllers

HID has two lines of Edge controllers: EVO (newer) and Legacy. The newer line of controllers can take an optional 2nd reader and have enhanced power efficiency (12 to 24 VDC), therefore, can support 12 V or 24 V locks.

In the following series of tables, we compare the characteristics of the EVO controllers to their Legacy counterparts.

Edge platform differences between EVO and Legacy

Characteristics	EVO	Legacy
Flash memory	128 MB	8 MB
Maximum cardholder capacity[3]	125,000	44,000
Power over Ethernet (PoE) standard	802.3af	802.3af
RTC backup	Super-cap (2-5 ddays) No replacement required	Battery (3-5 days) Requires replacement
Tamper	Optical and external switch	Mechanical and external switch
Door communication	Discrete I/O, Wiegand, Hi-O	Discrete I/O, Wiegand
Mounting holes and wiring termination	US Single-Gang, EU/ASIA 60 mm	US Single-Gang
Standby condition currrent	85 – 180 mA	1 A
Maximum current	1.5 A	1.5 A
Maximum combined output rating	1.2 A	700 mA
Operating temperature range	32 ° – 120 ° F (0 ° – 49 ° C)	32 ° – 120 ° F (0 ° – 49 ° C)
Humidity	5% to 85% non-condensing	5% to 85% non-condensing

[3] In Security Center, a cardholder can have multiple credentials. A cardholder with two credentials is counted as two by HID. The Edge controller capacity tested by Genetec Inc. is 22,000 credentials. No memory upgrades are possible.

Edge controller differences between EVO and Legacy

Characteristics	EVO (EH400-K)	Legacy (E400)
Lock power provided by controller	12 V or 24 V	12 V
Reader power provided by controller	12 V	12 V
Input power	PoE, 12 V, 24 V	PoE, 12 V

Characteristics	EVO (EH400-K)	Legacy (E400)
Device periphery power using PoE	340 mA @ 24 V	700 mA @ 12 V
I/O reading (2 Readers)	Yes	No
Inputs/Outputs	5 inputs & 2 outputs	5 inputs & 2 outputs

Edge reader/controller differences between EVO and Legacy

Characteristics	EVO (EHR40-K, EHRP40-K)	Legacy (ER40, ERP40)
Input power	PoE, 12 V, 24 V	PoE, 12 V
Device periphery power using PoE	310 mA @ 24 V	600 mA @ 12 V
13.56 MHz "Smart card" credential compatibility	iCLASS	iCLASS
125 kHz "Prox" credential compatibility	HID Prox, Indala, EM4102, AWID	HID Prox
Inputs/Outputs	5 inputs & 2 outputs	5 inputs & 2 outputs
Packaging: number of pieces to install	2	1
Only secure side access to lock output	Yes	No

Supported Edge interface modules

The HID Edge interface modules (also known as *interface panels* and *sub-panels*) can only be used with HID Edge EVO controllers.

Click on the link to download the product datasheet.

- EDWM-M Door & Wiegand Module
- EDM-M Door Module
- EWM-M Wiegand Module
- EIM-M Input Module

HID hardware installation do's and don'ts

For your safety and for getting the best performance out of your equipment, follow the recommended mounting and wiring instructions.

Mounting recommendations

- The controllers and interface modules must always be mounted in a secure area.
- Mount using the four mounting screws (provided) or other appropriate fasteners. Place the fasteners in the corner holes of the base.
- The VertX devices can be stacked with or without the cover. Do not remove the plastic base. Make sure you position the VertX devices in such a way as to provide room for wiring, air-flow and cable runs.

Wiring recommendations

CAUTION: VertX controllers and interface modules are sensitive to Electrostatic Discharges (ESD). Exercise precautions while handling the circuit board assembly by using proper grounding straps at all times.

- Power and alarm input connections (all VertX devices): Connect power by providing 12 VDC to the P7 connector. +12 VDC goes to Pin 1 and ground to Pin 2. Connect the *Bat Fail* and *AC Fail* inputs to battery low/failure and AC failure contacts provided on the power supply. Connect the *Tamper* input to a tamper switch on the enclosure.

  NOTE: Connect the data return line to the same ground as the reader power if the reader is not powered by the VertX controller's 12 VDC.
- The VertX controller should have a separate power supply than the mag lock and other devices such as the PIR (Passive Infrared Sensor).
- The relay output should be protected with a diode. On a PoE powered Edge controller, a non-protected relay could cause the unit to restart or go into read-only mode.
- If in-rush current with mag lock exceeds the specifications, a snubber circuit on the relay output should be added.
- Configure the tamper input to its proper state (NO/NC) even if it’s going to be disabled.
- For setups with REX mechanism built in the door handle, it is recommended to increase the debounce time for the door sensor to avoid false *Door forced open* events.
- The door sensor is by default set to NC and unsupervised, while all other inputs are by default set to NO and unsupervised (no EOL resistors). Any input can be configured as NO or NC, as well as supervised or unsupervised. They can be configured for supervisory resistors of 1 to 6 kΩ. The supervised inputs should be configured in Security Center through Config Tool and pushed to the VertX interface modules by the Access Manager. The default supervised input configuration is done using two EOL 2 kΩ resistors.
- By default, doors relock on door open. For double doors, it is recommended to set a minimum action time on the relay to maintain it active for the whole duration of the grant time.
- A V300 interface module dedicated to elevator control should only be used for elevator control and should not be used to trigger non-elevator related outputs.

Network recommendations

- It is recommended to set a static IP address on the HID controller. The discovery process is different for controllers that have a DHCP-assigned IP address. Discovery for DCHP address through multiple VLAN is not supported. If the Access Manager is on a different VLAN than the HID controller, the controller's IP address cannot be assigned by DCHP.

- It is recommended to isolate the controller on the network from broadcast traffic or unhandled multicast.
- The maximum number of character for the controller name should be 15, without spaces and special characters.
- All HID controllers has the same factory-assigned IP address 169.254.242.121. You can always log on to an HID unit from your computer using a network cable. The default logon username and password are `root/pass`.

HID VertX V1000 RS-485 connections

The VertX V1000 controller has two RS-485 serial buses with two ports each.

The two RS-485 serial buses are labeled **P3** and **P4**. Each serial bus has a 10-pin connector divided into two ports, labeled **Port 1** and **Port 2** on the **P3** bus, and **Port 3** and **Port 4** on the **P4** bus. Having two ports on each bus provides the option of splitting each RS-485 bus into two physical connections, allowing a total of four physical connections.

The followings are the do's and don'ts.

- The interface modules must be connected to the RS-485 serial buses using the daisy chain topology, not the star topology.
- Use only the "In" ports on the interface modules. This eliminates the possibility of many interface modules dropping offline because one interface module died or lost power.
- Terminate appropriately. The RS-485 serial bus expects a 120 Ω resistor to "terminate" the ends of the loop. All the devices (including the V1000 controller) have jumpers for this.
- The termination jumpers on the V1000 should be in the "Out" position if there are no interface modules attached to the port. If there are interface modules attached, then the termination jumper should be in the "In" position.
- All interface modules, except the ends of the serial chains, must have their termination jumpers in the "Out" position.
- The dial on the interface module indicates its physical address (factory default=0) to the controller it is attached to. Do not duplicate addresses on the same serial bus.
- It is recommended to wire the RS-485 to the position of the **P9** terminal block of the Vx00-series interface module. This is especially important when the RS-485 communication is in a "daisy chain" configuration. If the RS-485 is wired In and Out , and power is lost, or the **P9** terminal block is unplugged on a Vx00-series interface module, RS-485 communications will be lost to downstream Vx00-series interface modules.

HID VertX V1000 I/O behavior

The following applies to HID VertX V1000 controller inputs and outputs:

- By default, the door monitor input is configured as normally closed (NC), and not supervised (no EOL resistors). As a result, if nothing is connected to the door monitor input, the unit emits beeps to signal that the door is open. To correct this, connect the door monitor input to an actual door monitor, or reconfigure the input to normally open (NO).
- All other inputs are configured as normally open (NO), not supervised (no EOL resistors).
- It is not recommended to use HID VertX V1000 controller inputs and outputs for special purpose requirements such as:
  - A door: REX, door sensor, door lock
  - Interlock override or lockdown
  - Elevator control floor tracking
  - Door buzzer
  - I/O linking (*Hardware zone*)

  Instead, you should use the inputs and outputs from the V1000's sub-panels (V200's, V300's) for these purposes.
- Any unused inputs (including AC Fail, Battery Fail and REX) can be used for other purposes except the *Tamper* and *Door Monitor* inputs. These two types of inputs can only be used for their specified purpose.
- The states of HID output relays cannot be shown in the *System status* task.

HID I/O linking considerations

Whenever a change is made to *I/O linking* on an HID unit, an internal task (called IOLinker) must be restarted in order to take the new configuration into consideration. When this happens, all output relays controlled by the unit are set to the *Normal* state for half a second before they return to their expected state. This behavior may cause temporary disruptions to the operation of your system.

The following actions applied to entities controlled by HID units may cause the output relays to reset:

- Overriding the unlock schedules of a door from Security Desk.
- Changing the unlock schedules assigned to a door.
- Changing the unlock schedule exceptions on a door.
- Configuring readers on a door that has unlock schedules assigned.
- Changing the *Door held* option of a door.
- Changing the *Door forced* option of a door.
- Changing the *Interlock* restrictions on an area using an HID controlled doors on its perimeter.
- Configuring exceptions to the floor operating schedules of an elevator.
- Configuring an event-to-action to trigger an output based on the inputs of a *hardware zone* controlled by the same HID unit.

Related Topics
Door configuration tabs on page 818
Selecting who has access to doors on page 514
Selecting who has access to elevators on page 522
Configuring hardware zone settings on page 762

HID Power and Comm LEDs

HID units are equipped with 2 status LEDS; One is labelled *Power*, and the other is labelled *Comm*. You can find these LED's on top of the face plate for V1000's and V2000's. For Edge and Edge Plus devices, the LED's are found on the bottom of the unit.

V1000, V2000 and Edge Reader power & Comm LED's

LED indicator	State	Description
Power	Off	Check input voltage to the unit
	Solid red	No network activity
	Blinking (Red/Off)	Network activity
Comm	Solid green	All interfaces found (eg. V100, V200, V300)
	Solid red	No interfaces found
	Blinking (Red/Green)	Some interfaces were found (the duty cycle changes according to the number of interfaces found).
	Blinking (Amber/Green)	The unit is in "*Locate me*" mode (somebody clicked the *Identity* button).

For VertX V1000 units: If the *Comm* LED indicator is off, update the firmware for the interface (V100) part of the unit.

VertX interface boards (sub-panels) V100, V200, V300

LED indicator	State	Description
Power	Solid red	OK
	Anything other than solid red	Check input voltage
Comm	Blinking (Red/Green)	RS-485 bus activity
	Amber	Firmware download in progress

If the *Comm* LED indicator for an interface board is off, verify the wiring for the RS-485 bus. Then try updating the firmware.

HID features and models supported by Security Center

This section lists the Security Center access control features that are supported by each HID unit model.

Supported keypad reader options

Card and PIN operation depends on the type of unit and the keypad reader installed.

For both HID iCLASS and Prox readers, the *Keypad configuration setting* option is selected at the time of purchase. Supported options include the following:

- Option 00: “Keypad configuration setting option” of 00 = Buffer one key, no parity, 4-bit message.
- Option 14: “Keypad configuration setting option” of 14 = Buffer one to five keys (Standard 26-bit output). This reader option is also known as “Galaxy Mode”.

Unit type	HID keypad reader option	Online operation	Offline operation	Observation
V1000 with V100 V2000 EdgePlus E400	Option 14	Card or PIN.	Card or PIN.	The keypad readers can be used to enroll PINs.
	Option 00	Card or PIN. Card and PIN on schedule. When off-schedule, operation reverts to card only.		An unknown PIN will not generate the *Access denied: Unknown credential* event in Security Center. The reader cannot be used to enroll PINs for credential creation.
EdgeReader ER40 EdgeReader ERP40 EdgeReader ERW400	These units cannot be ordered with a keypad.	Card only.	Card only.	—

For HID SmartID keypad readers (SK10), the following option is required to support card and PIN functionality:

- Option 02PIN-0000: “Pincode Wiegand 4 bit per key no parity”.

Supported PIN length

By default, HID controllers only accept PIN numbers up to 5 digit long. You can increase this limit to 8 digits for readers using *Card and PIN* mode, and to 15 digits for readers using *Card* or *PIN* mode.

Supported readers

HID units support most industry standard card readers that output card data using the Wiegand protocol (up to 128-bit card formats).

HID SmartID readers (MIFARE and DESFire) are also supported.

Supported RF Ideas USB enrollment readers

The RF Ideas readers only support card data formats up to 64 bits. The following USB enrollment readers are supported:

- pcProx HID USB reader for enrolling proximity cards
- AIR ID Enroll iCLASS ID# USB reader for enrolling HID iCLASS cards
- AIR ID Enroll 14443/15693 CSN USB reader for enrolling a MIFARE card using the CSN (card serial number)

Support for Power over Ethernet (PoE)

The following units support PoE (15.4W):

Unit type	Support
HID V1000, V100, V200, V300	Not supported
HID V2000	Not supported
HID EdgeReader / EdgePlus	Supported

Supported unit and reader cardholder capacity

The number of *cardholders* (or *credentials*) that a unit can support offline is as follows:

Unit type	Supported number of cardholders
HID V1000 / V100	22,000, up to 125,000 cardholders with full memory upgrade.
HID V2000	22,000, up to 125,000 cardholders with full memory upgrade.
HID EdgeReader / EdgePlus	22,000 cardholders (maximum). No memory upgrades are possible.

The number of readers that a unit can support is as follows:

Unit type	Supported number of readers
HID V1000 / V100	64 readers with 32 V100 reader interface modules[1] 32 doors configured as card in/card out 64 doors configured as card in/REX out
HID V2000	2 readers 1 door configured as card in/card out 2 doors configured as card in/REX out
HID EdgeReader / EdgePlus	1 reader 1 door configured as card in/REX out

[1] HID states that a V1000 controller can support a maximum of 32 downstream interface modules (16 on each RS-485 serial bus). However, the performance tests run by Genetec Inc. indicate that as a “best practice”, 20 downstream interface modules should not be exceeded (10 per serial bus).

Enabling long PIN support on HID units

You can enable the long PIN (longer than 5 digits) support on HID controllers (legacy and EVO) by changing a configuration file (gconfig) on the servers hosting the Access Manager role.

What you should know

By default, HID controllers only accept PIN numbers up to 5 digit long. You can increase this limit to 8 digits for readers using Card and PIN mode, and to 15 digits for readers using Card or PIN mode.

To enable long PIN support on HID controllers:

1 Create the *VertXConfig.gconfig* file with the following content:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
<Vertx
MaximumPinLength="nn"
/>
</configuration>
```

where `nn` is the maximum PIN length in digits.

If this file already exists, simply add the tag `MaximumPinLength=”nn”`.

2 Copy this file to the Security Center installation folder, on all servers hosting the Access Manager role.

The default is *C:\Program Files (x86)\Genetec Security Center 5.5\ConfigurationFiles* on a 64-bit machine.

The next time you synchronize a unit (HID controller) with the Access Manager, the unit will accept PIN numbers up to the maximum PIN length. For every PIN credential that is longer than the specified maximum, a warning message will be issued during synchronization, and the PIN will not be synchronized to the unit.

To synchronize a unit:

1 Connect to Security Center with Config Tool.

2 Open the **Access control** task, and select the **Roles and units** page.

3 Select a unit (HID controller), select **Synchronization**, and then click **Synchronize now**.

Supported HID unit configurations

This section describes the supported HID access control unit configurations in Security Center.

General vs. dedicated inputs

When a controller is used to control a door, some inputs must be used only for their intended purpose (dedicated inputs). For example, if a door has a REX sensor or a door sensor, the controller's inputs intended for these sensors must be used.

Input	When used as	Required configuration
Request-to-Exit	Request-to-Exit input signal.	• Set **Automatically grant REX** to ON in the **Door** > **Properties** tab to generate *Request to exit* events when the input is triggered. Events are logged, and can be used for event-to-actions. • Assign the REX input to a door side in the **Door** > **Hardware** tab to program the controller to react to the REX input by releasing the lock.
	General purpose input (for zone monitoring for example)	• Set **Automatically grant REX** to OFF in the **Door** > **Properties** tab. • Configure the input for a zone, interlock, etc.
Door monitor	Door position sensor input (door open or door closed)	• Assign this input to the **Door sensor** in the **Door** > **Hardware** tab. **NOTE:** This input cannot be used for any other purpose.

HID door configuration with readers

A door with a reader assigned to a V2000, V100, or an Edge device, must have all inputs (for example door contact, REX) and outputs (for example door lock) associated to that same device. Inputs and outputs must not be distributed across several devices.

HID door configuration with two door sensors

It is not recommended to configure a door with two door sensors (or door contacts) without physically wiring the sensors in series. In the Security Center, only a single door sensor should be configured per door.

Security Center features supported by HID units

This section lists the standard Security Center access control features that HID units support.

Readerless door

Readerless doors (doors that use an I/O module for a REX, door state, and door lock only) are supported, both when the unit is operating online and offline.

For readerless doors to work, the following is required:

- The inputs of an HID VertX V1000 must be not used for this feature.
- All inputs and outputs must belong to the same HID controller (one V2000 or one Edge).

NOTE: A readerless door does not support the buzzer feature.

Door control

- **Card and PIN:** Card and PIN reader mode is supported if the installed reader supports it.

  For card and PIN reader mode to work, all reader interfaces/inputs/outputs for a door must be controlled by the same HID unit (HID Edge, VertX V2000, or VertX V100 interface module).
- **PIN entry timeout:** Supported as per door configuration.
- **Extended grant time:** Supported as per door configuration.
- **Entry time (standard and extended):** Supported as per door configuration.
- **Door relock:** The relock option on door closed is not supported. Only the delayed locking after the door opens is supported, and the maximum delay is 27 minutes.
- **Door held event and buzzer:** Both the *Door open too long* event and the reader buzzer are supported as per door configuration.
- **Door forced event and buzzer:** Both the *Door forced open* event and the reader buzzer are supported as per door configuration.
- **Request to exit (REX):** All REX handling behavior are supported as per door configuration.
- **Shunting:** Reader shunting is not supported. Only inputs can be shunted.

People counting

People counting is supported only when all units used for this feature are connected to the same Access Manager. The moment a unit assigned to one of the perimeter doors of an area is offline, the feature is disabled for the entire area.

Security clearance

The concept of security clearance is not supported for areas controlled by HID units.

Elevator control

For elevator control to work, the following is required:

- All interface modules used for elevator control (HID VertX V100, V200, and V300) must be assigned to the same VertX V1000. Reader, inputs and outputs must be assigned to the same V2000 (max. of 4 floors) or Edge (max. of 2 floors).
- All units used for this feature must be assigned to the same Access Manager.

- The reader interface, inputs, and outputs must be connected to the same HID controller (VertX V1000, V2000, or Edge). A maximum of 1 elevator cab reader can be assigned per HID controller (VertX V1000, V2000, or Edge).

NOTE: If you plan to offer both periods of controlled access and free access to your elevators, contact your representative of Genetec Inc. for a custom firmware to use with the units controlling elevators.

The use of HID VertX controllers (V1000 and V2000) for elevator control is subject to the following limitations:

- A VertX controller should be dedicated to the control of a single elevator cab.
- Once a VertX controller has been assigned to perform elevator control, it should only be used for that purpose. Door and zone control should not be mixed with elevator control, even when the unit has unused readers, inputs and outputs.
- When *elevator* floors are operating under controlled access mode, schedules from different *access rules* applied to different floors are merged when the rules are granted to a same cardholder.

  Example: Bob is granted access to Floor-1 from 9 a.m. to 10 a.m. through access rule 1, and to Floor-2 from 10 a.m. to 11 a.m. through access rule 2. When Bob presents his card in the elevator, the VertX controller actually grants access to Robert from 9 a.m. to 11 a.m. on both floors.
- Unlock schedules cannot be used on elevators controlled by HID units.

Elevator floor tracking

Floor tracking is only supported when the unit is online, and when all units used for this feature are assigned to the same Access Manager.

NOTE: Elevator floor tracking is not supported when the unit is offline because event reporting is unavailable. Events are not regenerated when the unit reconnects to Security Center.

Antipassback feature

The *antipassback* feature is supported both when the unit is operating online and offline.

For antipassback to work, the following is required:

- Use either VertX V1000 (multiple areas and multiple doors per area) or VertX V2000 (area with a single door) controllers. HID Edge products are not supported.
- All units used for antipassback must be assigned to the same Access Manager.
- The interlock feature must be disabled. Interlock (including the lockdown and override functions) and antipassback are mutually exclusive; both features cannot be enabled for an area at the same time.

Antipassback works best once the access control system has been configured and the system is operational and relatively static. It is recommended to enable antipassback once the following entities have been properly configured in Security Center and are not expected to change on a daily basis:

- Unit time zones
- Doors and associated readers
- Areas (groups of doors)
- Elevators and associated floors (including unlocking schedules)
- Cardholder groups
- Schedules (including card and PIN schedules)
- Access rules

The following section provides guidelines for configuring, enabling, and managing antipassback with HID VertX controllers (units):

- You must use either the V1000 or V2000 for antipassback.
  - V2000: Antipassback is only supported for an area with a single door having both entry and exit readers.
  - V1000: Antipassback is supported for multiple areas, with each area supporting multiple doors with entry and exit readers. Limitation in the number of doors is based on the number of V100 modules installed.
- Antipassback is not recommended with the Edge product line for the following reasons:
  - Only a single reader can be specified for either entry or exit (not both) while antipassback typically requires both entry and exit readers.
  - Peer-to-peer communication between Edge devices is not supported by Security Center.
- An area with antipassback must be configured for readers wired to, and doors managed by, the same unit (V1000 or V2000) because:
  - Antipassback functions are handled by the unit (V1000 or V2000).
  - The Security Center does not support peer-to-peer communication between either VertX V1000 or V2000 devices.
- Antipassback can be reset using the following methods:
  - A unit synchronization operation
  - An action (manually or with an event-to-action)
- The following system behavior will reset a unit's antipassback state:
  - Initial unit synchronization when the Security Center services are started or restarted.
  - Unit synchronization following the loss and recovery of a connection with the unit (V1000 or V2000).
  - Unit synchronization following certain configuration changes (see below for more details).
  - Manual synchronization of the unit through the Config Tool page.

Antipassback options

The following antipassback options are supported:

- Soft antipassback (passback violation event generated and access is granted) is only supported when the unit is online. Soft antipassback is not supported when the unit is offline because event reporting is unavailable. Events are not regenerated when the unit reconnects to Security Center.
- Hard antipassback (passback violation event generated and access is denied) is supported both when the unit is operating online and offline.
- Strict antipassback (passback violation event is generated when a cardholder attempts to leave an area that they were never granted access to). With HID units, hard and strict antipassback are one and the same. There is no distinction between the two.
- Antipassback on schedule is supported both when the unit is operating online and offline.
- Antipassback on schedule is not supported with hard antipassback.

NOTE: The timed antipassback option is not supported.

Interlock feature

The interlock feature is supported both when the unit is operating online and offline.

For interlock to work, the following is required:

- The antipassback feature must be disabled. *Interlock* (including the lockdown and override functions) and *antipassback* are mutually exclusive; both features cannot be enabled for an area at the same time.

- The inputs of an HID VertX V1000 must be not used for this feature.
- All perimeter doors of an interlocked area must be assigned to the same HID controller (one VertX V1000 or one V2000).

NOTE: If a perimeter door of an interlock is open, when an authorized cardholder accesses a second perimeter door of the same interlock, an *Access granted* event for the second door might be generated, even through the second door does not unlock.

Interlock options

The following interlock options are supported both when the unit is operating online and offline:

- Lockdown
- Override

First-person-in rule

First-person-in rule is not supported by HID units.

Two-person-in rule

Two-person rule is not supported by HID units.

Visitor escort rule

Visitor escort rule is not supported by HID units.

Event-to-actions

Event-to-action is supported when the unit is operating online and offline, with limitations.

- **Event-to-actions with Trigger output action:** The *Trigger output* action type can be used in event-to-actions when the unit is online, and is partially supported when the unit is offline. For the *Trigger output* action type to work, all units used for this feature must be assigned to the same Access Manager.
- **Event-to-actions with Silence buzzer or Sound buzzer actions:** The *Silence buzzer* and *Sound buzzer* action types can be used in event-to-actions both when the unit is operating online and offline. For these actions to work, all inputs and outputs must belong to the same HID controller (one VertX V1000, one V2000, or one Edge).

  NOTE: The *Action* feature is not available with a readerless door.
- **Access granted events are not supported when the unit is offline:** Event-to-actions based on the *Access granted* event do not work when the unit is disconnected from the Access Manager.

I/O Linking

The I/O linking feature is supported both when the unit is operating online and offline, with the following limitations.

- The inputs of an HID VertX V1000 must be not be used for this feature.
- All inputs and outputs must be controlled by the same HID controller.
- Only the *Trigger output* action is supported when the unit is operating offline.

Related Topics
HID features and models supported by Security Center on page 962

D

Multiple-Swipe feature

This section includes the following topics:

About the multi-swipe feature

The multi-swipe feature allows cardholders to badge their credentials multiple times at a door in order to generate a custom event. This event can then be used to trigger an action through an *event-to-action*.

The MultiSwipe macro

The MultiSwipe macro enables a specific group of cardholders to generate two distinct custom events when they swipe their credentials a given number of times at door, within the prescribed delay. N swipes generates the first custom event, and N+1 swipes generates the second custom event. All cardholders in the designated group must be granted access to the door.

The MultiSwipe macro is provided with your Security Center software to help you implement this feature.

Implementing the multi-swipe feature

You can implement the multi-swipe feature using the macro provided with your Security Center software.

Before you begin

You need to create the following entities in order to implement the multi-swipe feature:

- A door equipped with a reader, to be used for the multi-swipe feature.
- A cardholder group authorized to use the multi-swipe feature. All members of this group must have access to the designated door.
- Two custom events: a first one to be generated when an authorized cardholder swipes N times at the door, and a second one to be generated when the cardholder swipes N+1 times.
- A schedule that defines when the multi-swipe feature is available.

What you should know

All macros provided with the Security Center software are found in the folder *Add-On\Macros* under the Security Center installation folder (default=*C:\Program Files (x86)\Genetec Security Center 5.5*).

To implement the multi-swipe feature at a door:

1. Create a macro and name it *Multi-Swipe at <Door>*, where *<Door>* is the name of the door where the multi-swipe feature is enabled.

   Instead of a door, you can also select an area. In this case, the multi-swipe feature is enabled on all doors within the area.
2. Select the **Properties** tab, click **Import from file**, select *MultiSwipe.cs*, and click **Open**.
3. Click **Check syntax**, then click **Close**, and then click **Apply**.
4. Select the **Default execution context** tab, and set the following properties.
   - **CardholderGroup:** Cardholder group authorized to use the multi-swipe feature.
   - **DoorOrArea:** Door or area for which the multi-swipe feature is being enabled.
   - **DelayInSecondsBetweenEachSwipe:** The maximum delay in seconds between two consecutive swipes from the same authorized cardholder for the swipe to be considered as part of the multi-swipe action.
   - **NumberOfSwipes:** Number of swipes (N) to generate the first custom event.
   - **NSwipesCustomEventId:** Value assigned to the first custom event. Note that the first custom event is only generated *n* seconds after the last swipe, *n* being the maximum delay in seconds between two consecutive swipes.
   - **Np1SwipesCustomEventId:** Value assigned to the second custom event. Note that the second custom event is immediately generated after N+1 swipes.
   - **Schedule:** Schedule during which the multi-swipe feature is in effect.
5. Click **Apply**.
6. Create a scheduled task and name it *RunMultiSwipe-OnStartup*.
7. Select the **Properties** tab, and set its properties as follows.
   - **Status:** Set the status to ON.
   - **Recurrence:** Set the recurrence to **On startup**.
   - **Action:** Select **Run a macro**, and set **Macro** to the macro you just created.
8. Click **Apply**.

   This makes sure that the multi-swipe macro is always running, even after a system restart.

9. Create an event-to-action to link the first custom event to the desired action.

   Example: Temporarily override unlock schedule, arm a zone, and so on.

10. Create an event-to-action to link the second custom event to the desired action.

    Example: Cancel the unlock schedule override, disarm a zone, and so on.

E

Point of Sale integration

This section includes the following topics:

About the Point of Sale role

The *Point of Sale* role imports transaction data from an external *point of sale (POS)* system so that transaction reports can be generated from Security Desk for investigation purpose.

The transactions are tied to the *cash registers* that were used to capture these transactions. Security Center can link Omnicast™ cameras to these cash registers, allowing users to search video sequences based on the transaction details.

For a user to view transaction reports in Security Desk, the Point-of-Sale plugin must be enabled on the machine where Security Desk is installed.

About cash registers

A cash register is a type of entity that represents a single cash register (or terminal) in a point of sale system.

Cash register entities are created by the Point of Sale role. They identify the transaction data imported by the Point of Sale role from an external POS system. Security Center can link Omnicast™ cameras to cash registers to provide video support to help security officers in their investigations.

Enabling Point of Sale plugin

To view POS (transaction) reports in Security Desk, you must enable the Point of Sale plugin on each computer where Security Center Client is installed.

To enable the Point of Sale plugin in Security Center:

1 Open the *SecurityDesk.plugins.xml* file, located in *C:\Program files (x86)\Genetec Security Center 5.5* on a 64-bit computer, and in *C:\Program files\Genetec Security Center 5.5* on a 32-bit computer.

2 Set the **Genetec.PointOfSale.Reporting.dll** parameter to **true.**

Example: `<Assembly Name="Genetec.PointOfSale.Reporting.dll" Enabled="true" />`

After you finish

Perform this procedure on each computer hosting a Security Center Client.

Adding cash registers

To import cash register transactions from your external POS system, you must add cash registers to the Point of Sale plugin.

To add a cash register:

1 Open the **System** task, and click the **Roles** view.

2 Select the Point of Sale role, click the **Cash registers** tab, and click **Add an item** (✚).

3 In the **Cash register properties** dialog box, enter the following information:

- **Name:** Name of the cash register entity.
- **Description:** Description of the cash register entity.
- **ID:** External identifier (or primary key) used to identify the cash register in the external POS database.
- **Partition:** Partition the created cash register entity should belong to.

4 Click **Save** > **Apply**.

The new cash register is added in the list.

After you finish

To view video for the events related to the cash register, you must link cameras to the cash register.

Linking cameras to cash registers

To view video with the events related to cash registers, you must link Security Center cameras to the cash registers.

To link cameras to a cash register:

1 Open the **Area view** task.

2 Select the cash register to configure, and click the **Cameras** tab.

3 Click **Add an item** (✚).

4 Select the cameras to link the cash register to, and click **OK** > **Apply**.

TIP: Hold **SHIFT** to select multiple cameras.

The cameras are added in the list. Events that are received in Security Desk from that cash register on the external POS system now display video.

Glossary

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

Access control

The Access control task is a type of administration task that allows you to configure access control roles, units, rules, cardholders, credentials, and related entities and settings.

Access control health history

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

access control unit

An access control unit is a type of entity that represents an intelligent access control device, such as a Synergis™ appliance or an HID network controller, that communicates directly with the Access Manager over an IP network. An access control unit operates autonomously when it is disconnected from the Access Manager.

Access control unit events

Access control unit events is a type of maintenance task that reports on events pertaining to selected access control units.

Access Manager

Access Manager is the role that manages and monitors access control units on the system.

access point

An access point is any entry (or exit) point to a physical area where access can be monitored and governed by access rules. An access point is typically a door side or an elevator floor.

access right

An access right is the basic right users must have over any part of the system before they can do anything with it. Other rights, such as viewing and modifying entity configurations, are granted through privileges. In the context of a Synergis™ system, an access right is the right granted to a cardholder to pass through an access point at a given date and time.

access rule

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

Access rule configuration

Access rule configuration is a type of maintenance task that reports on entities and access points affected by a given access rule.

Access troubleshooter

Access troubleshooter is a tool that helps you detect and diagnose access configuration problems. With this tool, you can find out about the following:

- Who is allowed to pass through an access point at a given date and time
- Which access points a cardholder is allowed to use at a given date and time
- Why a given cardholder can or cannot use an access point at a given date and time

action

An action is a user-programmable function that can be triggered as an automatic response to an event, such as door held open for too long or object left unattended, or that can be executed according to a specific time table.

active alarm

An active alarm is an alarm that has not yet been acknowledged.

Active Directory

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

Active Directory Federation Services

Active Directory Federation Services (ADFS) is a component of the Microsoft® Windows® operating system that issues and transforms claims, and implements federated identity. It is also a type of role that enables Security Center to receive claims from an external ADFS server.

Activity trails

Activity trails is a type of maintenance task that reports on the user activity related to video, access control, and LPR functionality. This task can provide information such as who played back which video recordings, who used the Hotlist and permit editor, who enabled hotlist filtering, and much more.

Advanced Systems Format

The Advanced Systems Format (ASF) is a video streaming format from Microsoft. The ASF format can only be played in media players that support this format, such as Windows Media Player.

agent

An agent is a subprocess created by a Security Center role to run simultaneously on multiple servers for the purpose of sharing its load.

alarm

An alarm is a type of entity that describes a particular trouble situation that requires immediate attention and how it can be handled in Security Center. For example, an alarm can indicate which entities (usually cameras and doors) best describe it, who must be notified, how it must be displayed to the user, and so on.

alarm acknowledgement

An alarm acknowledgement is a user response to an alarm. In Security Center, the default acknowledgement and alternate acknowledgement are the two variants of alarm acknowledgements. Each variant is associated to a different event so that specific actions can be programmed based on the alarm response selected by the user.

Alarms

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

Alarm monitoring

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

Alarm report

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

analog monitor

An analog monitor is a type of entity that represents a monitor that displays video from an analog source, such as a video decoder or an analog camera. This term is used in Security Center to refer to monitors that are not controlled by a computer.

antipassback

Antipassback is an access restriction placed on a secured area that prevents a cardholder from entering an area that they have not yet exited from, and vice versa.

Archive transfer

The Archive transfer task is a type of administration task that allows you to configure settings for retrieving recordings from a video unit, duplicating archives from one Archiver to another, or backing up archives to a specific location.

archive transfer

Archive transfer is the process of transferring your video data from one location to another. The video is recorded and stored on the video unit itself or on an Archiver storage disk, and then the recordings are transferred to another location.

Archiver

Archiver is the role that is responsible for the discovery, status polling, and control of video units. The Archiver also manages the video archive and performs motion detection if it is not done on the unit itself.

Archiver events

Archiver events is a type of maintenance task that reports on events pertaining to selected Archiver roles.

Archives

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

Archive storage details

Archive storage details is a type of maintenance task that reports on the video files (file name, start and end time, file size, protection status, and so on) used to store video archive, and which allows you to change the protection status of those files, among other things.

area

An area is a type of entity that represents a concept or a physical location (room, floor, building, site, and so on) used for grouping other entities in the system.

Area activities

Area activities is a type of maintenance task that reports on events pertaining to selected Archiver roles.

Area presence

Area presence is a type of investigation task that provides a snapshot of all cardholders and visitors currently present in a selected area.

Area view

The Area view task is a type of administration task that allows you to configure areas, doors, cameras, tile plugins, intrusion detection areas, zones, and other entities found in the area view.

area view

The area view is a view that organizes the commonly used entities such as doors, cameras, tile plugins, intrusion detection areas, zones, and so on, by areas. This view is primarily created for the day to day work of the security operators.

asset

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

asynchronous video

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

audio decoder

An audio decoder is a device or software that decodes compressed audio streams for playback. Synonym of *speaker*.

audio encoder

An audio encoder is a device or software that encodes audio streams using a compression algorithm. Synonym of *microphone*.

Audit trails

Audit trails is a type of maintenance task that reports on the configuration changes of the selected entities in the system and also indicates the user who made the changes.

authentication

The process of verifying that an entity is what it claims to be. The entity could be a user, a server, or a client application.

authorization

The process of establishing the rights an entity has over the features and resources of a system.

authorized user

An authorized user is a user who can see (has the right to access) the entities contained in a partition. Users can only exercise their privileges on entities they can see.

automatic enrollment

Automatic enrollment is when new IP units on a network are automatically discovered by and added to Security Center. The role that is responsible for the units *broadcasts* a discovery request on a specific port, and the units listening on that port respond with a message that contains the connection information about themselves. The role then uses the information to configure the connection to the unit and enable communication.

Automatic License Plate Recognition

Automatic License Plate Recognition (ALPR) is the term used for *License Plate Recognition (LPR)* in Europe.

AutoVu™

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

AutoVu™ LPR Processing Unit

AutoVu™ LPR Processing Unit is the processing component of the SharpX system. The LPR Processing Unit is available with two or four camera ports, with one dedicated processor per camera (if using SharpX) or per two cameras (if using SharpX VGA). This ensures maximum, per-camera, processing performance. The LPR Processing Unit is sometimes referred to as the *trunk unit* because it is typically installed in a vehicle's trunk.

Auxiliary Archiver

Auxiliary Archiver is the role that supplements the video archive produced by the Archiver. Unlike the Archiver, the Auxiliary Archiver is not bound to any particular *discovery port*, therefore, it can archive any camera in the system, including cameras federated from other Security Center systems. The Auxiliary Archiver depends on the Archiver to communicate with the video units. It cannot operate on its own.

B

Badge designer

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

badge template

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

block face (2 sides)

A block face (2 sides) is a type of parking regulation characterizing an overtime rule. A block face is the length of a street between two intersections. A vehicle is in violation if it is seen parked within the same block over a specified period of time. Moving the vehicle from one side of the street to the other does not make a difference.

bookmark

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

Bookmarks

Bookmarks is a type of investigation task that searches for bookmarks related to selected cameras within a specified time range.

Breakout box

The breakout box is the proprietary connector box of Genetec Inc. for AutoVu™ mobile solutions that use Sharp cameras. The breakout box provides power and network connectivity to the Sharp units and the in-vehicle computer.

broadcast

Broadcast is the communication between a single sender and all receivers on a network.

C

camera

A camera is a type of entity that represents a single video source in the system. The video source can either be an IP camera, or an analog camera that is connected to the video encoder of a video unit. Multiple video streams can be generated from the same video source.

camera blocking

Camera blocking is an Omnicast™ feature that lets you restrict the viewing of video (live or playback) from certain cameras to users with a minimum user level.

Camera Configuration

Camera Configuration is a type of maintenance task that reports on the properties and settings of local cameras in your system (manufacturer, resolution, frame rate, stream usage, and so on).

Camera events

Camera events is a type of investigation task that reports on events pertaining to selected cameras within a specified time range.

camera sequence

A camera sequence is a type of entity that defines a list of cameras that are displayed one after another in a rotating fashion within a single tile in Security Desk.

canvas

Canvas is one of the panes found in the Security Desk's task workspace. The canvas is used to display multimedia information, such as videos, maps, and pictures. It is further divided into three panels: the tiles, the dashboard, and the properties.

card and PIN

Card and PIN is an access point mode that requires a cardholder to present their card, and then enter a personal identification number (PIN).

cardholder

A cardholder is a type of entity that represents a person who can enter and exit secured areas by virtue of their credentials (typically access cards) and whose activities can be tracked.

Cardholder access rights

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

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

Cardholder configuration Cardholder configuration is a type of maintenance task that reports on cardholder properties, such as first name, last name, picture, status, custom properties, and so on.

cardholder group A cardholder group is a type of entity that configures the common access rights of a group of cardholders.

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

cash register A cash register is a type of entity that represents a single cash register (or terminal) in a point of sale system.

certificate Designates one of the following: (1) *digital certificate*; (2) *SDK certificate*.

cyphertext In cryptography, cyphertext is the encrypted data.

certificate authority A certificate authority or certification authority (CA) is an entity or organization that signs identity certificates and attests to the validity of their contents.

City Parking Enforcement City Parking Enforcement is a Patroller software installation that is configured for the enforcement of parking permit and overtime restrictions.

City Parking Enforcement with Wheel Imaging City Parking Enforcement with Wheel Imaging is a *City Parking Enforcement* installation of a Patroller application that also includes wheel imaging. The use of maps and of the Navigator is mandatory.

claim A claim is a statement, such as a name, identity, key, or group, made by one subject about itself or another subject. Claims are issued by a provider, and they are given one or more values and then packaged in security tokens that are issued by a security token service (STS).

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

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

client-specific key stream

The client-specific key stream is the encrypted form of the *master key stream*. The master key stream is encrypted with the *public key* contained in an *encryption certificate*, specifically issued for one or more client machines. Only the client machines that have the encryption certificate installed have the required *private key* to decrypt the encrypted key stream.

Config Tool

Config Tool is a Security Center administrative application used to manage all Security Center users, and configure all Security Center entities such as areas, cameras, doors, schedules, cardholders, Patroller/LPR units, and hardware devices.

Conflict resolution utility

Conflict resolution utility is a tool that helps you resolve conflicts caused by importing users and cardholders from an Active Directory.

context camera

A context camera is a camera connected to an LPR unit that produces a wider angle color image of the vehicle whose license plate was read by the LPR camera.

controlled exit

A controlled exit is when credentials are necessary to leave a secured area.

controller module

Controller module is the processing component of Synergis™ Master Controller with IP capability. This module comes pre-loaded with the controller firmware and the web-based administration tool, Synergis™ Applicance Portal.

Copy configuration tool

The Copy configuration tool helps you save configuration time by copying the settings of one entity to many others that partially share the same settings.

covert hit

A covert hit is a read (captured license plate) that is matched to a covert hotlist. Covert hits are not displayed on the Patroller screen, but can be displayed in Security Desk by a user with proper privileges.

covert hotlist

A covert hotlist is a hotlist hidden from the AutoVu™ Patroller users. Reads matching a covert hotlist generate covert hits.

credential

A credential is a type of entity that represents a proximity card, a biometrics template, or a PIN required to gain access to a secured area. A credential can only be assigned to one cardholder at a time.

Credential activities

Credential activities is a type of investigation task that reports on credential related activities, such as access denied due to expired, inactive, lost, or stolen credential, and so on.

credential code

A credential code is a textual representation of the credential, typically indicating the Facility code and the Card number. For credentials using custom card formats, the user can choose what to include in the credential code.

Credential configuration

Credential configuration is a type of maintenance task that reports on credential properties, such as status, assigned cardholder, card format, credential code, custom properties, and so on.

Credential management

Credential management is a type of operation task that allows you to create, modify, and delete credentials. It also allows you to print badges and enroll large numbers of card credentials into the system, either by scanning them at a designated card reader or by entering a range of values.

Credential request history

Credential request history is a type of investigation task that reports on which users requested, cancelled, or printed cardholder credentials.

custom event

A custom event is an event added after the initial system installation. Events defined at system installation are called system events. Custom events can be user-defined or automatically added through plugin installations. Unlike system events, custom events can be renamed and deleted.

custom field

A custom field is a user defined property that is associated to an entity type and is used to store additional information that is useful to your particular organization.

cyphertext

In cryptography, cyphertext is the encrypted data.

D

Daily usage per Patroller

Daily usage per Patroller is a type of investigation task that reports on the daily usage statistics of a selected Patroller (operating time, longest stop, total number of stops, longest shutdown, and so on) for a given date range.

dashboard

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

database server

A database server is an application that manages databases and handles data requests made by client applications. Security Center uses Microsoft SQL Server as its database server.

debounce

A debounce is the amount of time an input can be in a changed state (for example, from active to inactive) before the state change is reported. Electrical switches often cause temporarily unstable signals when changing states, possibly confusing the logical circuitry. Debouncing is used to filter out unstable signals by ignoring all state changes that are shorter than a certain period of time (in milliseconds).

degraded mode

Degraded mode is an offline operation mode of the interface module when the connection to the Synergis™ unit is lost. The interface module grants access to all credentials matching a specified facility code. Only Mercury and HID VertX interface modules can operate in degraded mode.

dependent mode

Dependent mode is an online operation mode of the interface module where the Synergis™ unit makes all access control decisions. Not all interface modules can operate in dependent mode.

dewarping

Dewarping is the transformation used to straighten a digital image taken with a fish-eye lens.

digital certificate

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

Directory

Directory is the main role that identifies your system. It manages all entity configurations and system wide settings in Security Center. Only a single instance of this role is permitted on your system. The server hosting the Directory role is called the *main server*, and must be set up first. All other servers you add in Security Center are called *expansion servers*, and must connect to the main server to be part of the same system.

Directory authentication

Directory authentication is a Security Center option that forces all client and server applications on a given machine to validate the identity certificate of the Directory before connecting to it. This measure prevents man-in-the-middle attacks.

Directory gateway

Directory gateways allow Security Center applications located on a non-secured network to connect to the main server that is behind a firewall. A Directory gateway is a Security Center server that acts as a proxy for the main server. A server cannot be both a Directory server and a Directory gateway; the former must connect to the Directory database, while the latter must not, for security reasons.

Directory Manager

Directory Manager is the role that manages the Directory failover and load balancing in order to produce the high availability characteristics in Security Center.

Directory server

A Directory server is any one of the multiple servers simultaneously running the Directory role in a high availability configuration.

discovery port

A discovery port is a port used by certain Security Center roles (Access Manager, Archiver, LPR Manager) to find the units they are responsible for on the LAN. No two discovery ports can be the same on one system.

district

A district is a type of parking regulation characterizing an overtime rule. A district is a geographical area within a city. A vehicle is in violation if it is seen within the boundaries of the district over a specified period of time.

door

A door is a type of entity that represents a physical barrier. Often, this is an actual door but it could also be a gate, a turnstile, or any other controllable barrier. Each door has two sides, named *In* and *Out* by default. Each side is an access point (entrance or exit) to a secured area.

Door activities

Door activities is a type of investigation task that reports on door related activities, such as access denied, door forced open, door open too long, hardware tamper, and so on.

door contact

A door contact monitors the state of a door, whether it is open or closed. It can also be used to detect an improper state, such as door open too long.

door side

Every door has two sides, named *In* and *Out* by default. Each side is an access point to an area. For example, passing through one side leads into an area, and passing through the other side leads out of that area. For the purposes of access management, the credentials that are required to pass through a door in one direction are not necessarily the same that are required to pass through in the opposite direction.

Door troubleshooter

Door troubleshooter is a type of maintenance task that lists all the cardholders who have access to a particular door side or elevator floor at a specific date and time.

Driver Development Kit

Driver Development Kit is a SDK for creating device drivers.

duress

A duress is a special code used to disarm an alarm system. This code quietly alerts the monitoring station that the alarm system was disarmed under threat.

E

edge recording

Edge recording is the process of recording and storing video recordings locally, thus removing the need for a centralized recording server or unit. With edge recording, you can store video directly on the camera’s internal storage device.

electric door strike

An electric door strike is an electric device that releases the door latch when current is applied.

elevator

An elevator is a type of entity that provides access control properties to elevators. For an elevator, each floor is considered an access point.

Elevator activities

Elevator activities is a type of investigation task that reports on elevator related activities, such as access denied, floor accessed, unit is offline, hardware tamper, and so on.

encryption certificate

An encryption certificate, also known as a *digital certificate* or *public key certificate*, is an electronic document that contains a public and private key pair used in Security Center for *fusion stream encryption*. Information encrypted with the *public key* can only be decrypted with the matching *private key*.

enforce

To enforce is to take action following a confirmed hit. For example, a parking officer can enforce a scofflaw violation (unpaid parking tickets) by placing a wheel boot on the vehicle.

entity

Entities are the basic building blocks of Security Center. Everything that requires configuration is represented by an entity. An entity can represent a physical device, such as a camera or a door, or an abstract concept, such as an alarm, a schedule, a user, a role, a plugin, or an add-on.

entity tree

An entity tree is the graphical representation of Security Center entities in a tree structure, illustrating the hierarchical nature of their relationships.

event

An event indicates the occurrence of an activity or incident, such as access denied to a cardholder or motion detected on a camera. Events are automatically logged in Security Center, and can be programmed to trigger actions. Every event mainly focuses on one entity, called the event source.

event-to-action

An event-to-action links an action to an event. For example, you can configure Security Center to trigger an alarm when a door is forced open.

expansion server

An expansion server is any server machine in a Security Center system that does not host the Directory role. The purpose of the expansion server is to add to the processing power of the system.

F

failover

A failover is a backup operational mode in which a role (system function) is automatically transferred from its primary server to a secondary server that is on standby. This transfer between servers occurs only when the primary server becomes unavailable, either through failure or through scheduled downtime.

federated entity

A federated entity is any entity that is imported from an independent system through one of the Federation roles.

federated identity

A federated identity is a security token that is generated outside of your own realm that you accept. Federated identity enables single sign-on, allowing users to sign on to applications in different realms without needing to enter realm-specific credentials.

federated system

A federated system is a independent system (Omnicast™ or Security Center) that is unified under your local Security Center via a Federation™ role, so that the local users can view and control its entities, as if they belong to the local system.

Federation™

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

Federation™ host

The Federation™ host is the Security Center system that runs Federation™ roles. Users on the Federation™ host can view and control entities that belong to federated systems directly from their local system.

first-person-in rule

The first-person-in rule is the additional access restriction placed on a secured area that prevents anyone from entering the area until a supervisor is on site. The restriction can be enforced when there is free access (on door unlock schedules) and when there is controlled access (on access rules).

Forensic search

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

four-port RS-485 module

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

free access

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

free exit

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

fusion stream

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

fusion stream encryption

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

G

G64

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

G64x

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

Genetec Server

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

Genetec Update Service

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

Genetec Video Player

The Genetec Video Player is a media player that is used to view exported G64 and G64x video files from Security Desk, or on a computer that does not have Security Center installed.

geocoding

Geocoding is the process of finding associated geographic coordinates (latitude and longitude) from a street address.

Geographic information system

Geographic information system (GIS) is a system that captures spatial geographical data. Map Manager can connect to third-party vendors that provide GIS services in order to bring maps and all types of geographically referenced data to Security Center.

ghost camera

A ghost camera is an entity used as a substitute camera. This entity is automatically created by the Archiver when video archives are detected for a camera whose definition has been deleted from the Directory, either accidentally or because the physical device no longer exists. Ghost cameras cannot be configured, and only exist so users can reference the video archive that would otherwise not be associated to any camera.

ghost Patroller

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

global antipassback

Global antipassback is a feature that extends the antipassback restrictions to areas controlled by multiple Synergis™ units.

Global Cardholder Synchronizer

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

global entity

A global entity is an entity that is shared across multiple independent Security Center systems by virtue of its membership to a global partition. Only cardholders, cardholder groups, credentials, and badge templates are eligible for sharing.

global partition

Global partition is a partition that is shared across multiple independent Security Center systems by the partition owner, called the sharing host.

H

hardware integration package

A hardware integration package, or HIP, is an update that can be applied to Security Center. It enables the management of new functionalities (for example, new video unit types), without requiring an upgrade to the next Security Center release.

Hardware inventory

Hardware inventory is a type of maintenance task that reports on the characteristics (unit model, firmware version, IP address, time zone, and so on) of access control, video, intrusion detection, and LPR units in your system.

hardware zone

A hardware zone is a zone entity in which the I/O linking is executed by a single access control unit. A hardware zone works independently of the Access Manager, and consequently, cannot be armed or disarmed from Security Desk.

Health history

Health history is a type of maintenance task that reports on health issues.

Health Monitor

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

Health statistics

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

High availability

High availability is a design approach that enables a system to perform at a higher than normal operational level. This often involves failover and load balancing.

hit

A hit is a license plate read that matches a hit rule, such as a hotlist, overtime rule, permit, or permit restriction. A Patroller user can choose to reject or accept a hit. An accepted hit can subsequently be enforced.

hit rule

Hit rule is a type of LPR rule used to identify vehicles of interest (called "hits") using license plate reads. The hit rules include the following types: hotlist, overtime rule, permit, and permit restriction.

Hits

Hits is a type of investigation task that reports on hits reported within a selected time range and geographic area.

hot action

A hot action is an action mapped to a PC keyboard function key (Ctrl+F1 through Ctrl+F12) in Security Desk for quick access.

hotlist

A hotlist is a type of entity that defines a list of wanted vehicles, where each vehicle is identified by a license plate number, the issuing state, and the reason why the vehicle is wanted (stolen, wanted felon, Amber alert, VIP, and so on). Optional vehicle information might include the model, the color, and the vehicle identification number (VIN).

Hotlist and permit editor

Hotlist and permit editor is a type of operation task used to edit an existing hotlist or permit list. A new list cannot be created with this task, but after an existing list has been added to Security Center, users can edit, add, or delete items from the list, and the original text file is updated with the changes.

hotspot

Hotspot is a type of map object that represents an area on the map which requires special attention. Clicking on a hotspot displays associated fixed and PTZ cameras.

I

I/O zone

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

identity certificate

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

identity provider

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

illuminator

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

Import tool

Import tool is a tool that allows you to import cardholders, cardholder groups, and credentials from a CSV (Comma Separated Values) file.

inactive entity

An inactive entity is an entity that is shaded in red in the entity browser. It signals that the real world entity it represents is either not working, offline, or incorrectly configured.

incident

An incident is an unexpected event reported by a Security Desk user. Incident reports can use formatted text and include events and entities as support material.

incident (Mission Control)

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

incident category

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

Incident configuration

The *Incident configuration* task is the administration task that you can use to configure the incident types, the incident categories, and the support documents for Mission Control. You can also use this task to generate reports on the changes made to incident types.

Incident Manager

The Incident Manager is the central role that recognizes situational patterns, and triggers incidents in the Mission Control system. This role manages the incident workflows and keeps track of all user activities that are related to incidents.

Incident monitoring

The *Incident monitoring* task is a type of operation task that you can use to monitor and respond to incidents. From this task, you can see the incidents displayed on a map, thus improving your situational awareness.

incident owner The incident owner is the incident recipient who took ownership of the incident. Only the incident owner can take actions to resolve the incident. An incident can only have one owner at a time.

incident recipient The incident recipient is the user that the incident has been dispatched to. This user can see the incident in the *Incident monitoring* task.

Incident report The *Incident report* task is a type of investigation task that you can use to search, review, and analyze Mission Control incidents.

incident trigger Incident triggers are rules that are applied by the Mission Control Rules Engine to detect and trigger incidents. These incidents are triggered based on events in Security Center.

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

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

interface module An interface module is a third-party security device that communicates with an access control unit over IP or RS-485, and provides additional input, output, and reader connections to the unit.

interlock An interlock (also known as sally port or airlock) is an access restriction placed on a secured area that permits only one door to be open at any given time.

Intrusion detection The Intrusion detection task is a type of administration task that allows you to configure intrusion detection roles and units.

intrusion detection area An intrusion detection area is a type of entity that corresponds to a zone or a partition (group of sensors) on an intrusion panel.

Intrusion detection area activities Intrusion detection area activities is a type of investigation task that reports on activities (master arm, perimeter arm, duress, input trouble, and so on) in selected intrusion detection areas.

intrusion detection unit An intrusion detection unit is a type of entity that represents an intrusion panel (or alarm panel) that is monitored and controlled by Security Center.

Intrusion detection unit events
Intrusion detection unit events is a type of investigation task that reports on events (AC fail, battery fail, unit lost, input trouble, and so on) related to selected intrusion detection units.

Intrusion Manager
Intrusion Manager is a type of role that monitors and controls *intrusion panels* (or alarm panels). It listens to the events reported by the intrusion panels, provides live reports to Security Center, and logs the events in a database for future reporting.

intrusion panel
An intrusion panel is a wall-mounted unit where the alarm sensors (motion sensors, smoke detectors, door sensors, and so on) and wiring of the intrusion alarms are connected and managed.

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

Inventory report
Inventory report is a type of investigation task that allows you to view a specific inventory (vehicle location, vehicle length of stay, and so on) or compare two inventories of a selected parking facility (vehicles added, vehicles removed, and so on).

I/O configuration
I/O configuration is a type of maintenance task that reports on the I/O configurations (controlled access points, doors, and elevators) of access control units.

I/O linking
I/O (input/output) linking is controlling an output relay based on the combined state (normal, active, or trouble) of a group of monitored inputs. A standard application is to sound a buzzer (through an output relay) when any window on the ground floor of a building is shattered (assuming that each window is monitored by a "glass break" sensor connected to an input).

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

IP camera
An IP camera is a video unit incorporating a camera.

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

IPv6
IPv6 is a video unit incorporating a camera.

K

Keyhole Markup Language

Keyhole Markup Language (KML) is a file format used to display geographic data in an Earth browser such as Google Earth and Google Maps.

L

Law Enforcement

Law Enforcement is a Patroller software installation that is configured for law enforcement: the matching of license plate reads against lists of wanted license plates (hotlists). The use of maps is optional.

license key

A license key is the software key used to unlock the Security Center software. The license key is specifically generated for each computer where the Directory role is installed. To obtain your license key, you need the *System ID* (which identifies your system) and the *Validation key* (which identifies your computer).

license plate inventory

A license plate inventory is a list of license plate numbers of vehicles found in a parking facility within a given time period, showing where each vehicle is parked (sector and row).

license plate read

A license plate read is a license plate number captured from a video image using LPR technology.

License Plate Recognition

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

live hit

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

live read

A live read is a license plate captured by the Patroller and immediately sent to the Security Center over a wireless network.

load balancing

Load balancing is the distribution of workload across multiple computers.

logical ID

Logical ID is a unique ID assigned to each entity in the system for ease of reference. Logical IDs are only unique within a particular entity type.

Logons per Patroller

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

long term

Long term is a type of parking regulation characterizing an overtime rule. The *long term* regulation uses the same principle as the *same position* regulation, but the parking period is over 24 hours. No more than one overtime rule may use the long term regulation in the entire system.

LPR

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

LPR camera

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

LPR Manager

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

LPR rule

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

LPR unit

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

M

macro

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

main server

Main server is the only server in a Security Center system hosting the Directory role. All other servers on the system must connect to the main server in order to be part of the same system. In an high availability configuration where multiple servers host the Directory role, it is the only server that can write to the Directory database.

man-in-the-middle

In computer security, man-in-the-middle (MITM) is a form of attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

manual capture

Manual capture is when license plate information is entered into the system by the user and not by the LPR.

manufacturer extension

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

map

A map in Security Center is a two-dimensional diagram that helps you visualize the physical locations of your security equipment in a geographical area or a building space.

Map designer

Map designer is a type of administration task that allows you to create and edit maps that represent the physical locations of your equipment to Security Desk users.

map link

A map link is a map object that brings you to another map with a single click.

Map Manager

Map Manager is the central role that manages all mapping resources in Security Center, including imported map files, external map providers, and KML objects. It acts as the map server to all client applications that require maps.

map mode

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

map object

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

map view

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

Maps

Maps is a type of operation task that heightens your situational awareness by providing the context of a map to your security monitoring and control activities.

master arm

Master arm is arming an intrusion detection area in such a way that all sensors attributed to the area would set the alarm off if one of them is triggered.

master key stream

In *fusion stream* encryption, the master key stream is the sequence of symmetric keys generated by the Archiver to encrypt one data stream. The symmetric keys are randomly generated and change every minute. For security reasons, the master key stream is never transmitted or stored anywhere as plaintext.

Media Gateway

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

Media Router

Media Router is the central role that handles all stream (audio and video) requests in Security Center. It establishes streaming sessions between the stream source (camera or Archiver) and its requesters (client applications). Routing decisions are based on the location (IP address) and the transmission capabilities of all parties involved (source, destinations, networks, and servers).

Migration tool

Migration tool is a tool used to migrate Omnicast™ 4.x systems to Security Center 5. This tool must be executed on every server computer where Omnicast™ 4.x components are installed.

Mission Control

Mission Control is a *Decision Support System* that provides organizations with new levels of situational intelligence, visualization, and complete incident management capabilities. Using Mission Control, operators can monitor and resolve incidents in a way that is responsive and compliant with their established standard operating procedures.

Mobile Admin

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

Mobile app

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

Mobile Data Computer

Mobile Data Computer is a tablet computer or ruggedized laptop used in patrol vehicles to run the AutoVu™ Patroller application. The MDC is typically equipped with a touch-screen with a minimum resolution of 800 x 600 pixels and wireless networking capability.

Mobile License Plate Inventory

Mobile License Plate Inventory is the Patroller software installation that is configured for collecting license plates and other vehicle information for creating and maintaining a license plate inventory for a large parking area or parking garage.

Mobile Server

Mobile Server is the server component of Security Center Mobile that connects Mobile apps and Web Clients to Security Center. The Mobile Server connects to Security Center, and synchronizes the data and video between Security Center and supported Mobile client components.

monitor group

A monitor group is a type of entity used to designate analog monitors for alarm display. Besides the monitor groups, the only other way to display alarms in real time is to use the Alarm monitoring task in Security Desk.

monitor ID

Monitor ID is an ID used to uniquely identify a workstation screen controlled by Security Desk.

Monitoring

The *Monitoring* task is a type of operation task that you can use to monitor and respond to real-time events that relate to selected entities. Using the *Monitoring* task, you can also monitor and respond to alarms.

motion detection

Motion detection is the feature that watches for changes in a series of video images. The definition of what constitutes motion in a video can be based on highly sophisticated criteria.

Motion search

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

motion zone

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

Move unit

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

multifactor authentication

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

N

Navigator box

The Navigator box is a proprietary in-vehicle device of Genetec Inc. that provides GPS coordinates and odometer readings to Patroller. Because it taps into the vehicle’s odometry signal, it is more accurate than a standard GPS device. The Navigator box can be used with any type of AutoVu™ mobile deployment that requires positioning information, but it is required for City Parking Enforcement with Wheel Imaging.

network

The network entity is used to capture the characteristics of the networks used by your system so that proper stream routing decisions can be made.

network address translation

Network address translation is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device, for the purpose of remapping one IP address space into another.

network view

The network view is a browser view that illustrates your network environment by showing each server under the network they belong to.

Network view

The Network view task is a type of administration task that allows you to configure your networks and servers.

new wanted

A new wanted is a manually entered hotlist item in Patroller. When you are looking for a plate that does not appear in the hotlists loaded in the Patroller, you can enter the plate in order to raise a hit if the plate is captured.

notification tray

The notification tray contains icons that allow quick access to certain system features, and also displays indicators for system events and status information. The notification tray display settings are saved as part of your user profile and apply to both Security Desk and Config Tool.

O

OCR equivalence

OCR equivalence is the interpretation of OCR (Optical Character Recognition) equivalent characters performed during license plate recognition. OCR equivalent characters are visually similar, depending on the plate's font. For example, the letter "O" and the number "0", or the number "5" and the letter "S". There are several pre-defined OCR equivalent characters for different languages.

Omnicast™

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

Omnicast™ compatibility pack

Omnicast™ compatibility pack is the software component that you need to install to make Security Center compatible with an Omnicast™ 4.x system.

Omnicast™ Federation™

The Omnicast™ Federation™ role connects an Omnicast™ 4.x system to Security Center. That way, the Omnicast™ entities and events can be used in your Security Center system.

output behavior

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

overtime rule

An overtime rule is a type of entity that defines a parking time limit and the maximum number of violations enforceable within a single day. Overtime rules are used in city and university parking enforcement. For university parking, an overtime rule also defines the parking zone where these restrictions apply.

P

parking facility

A parking facility is a type of entity that defines a large parking area as a number of sectors and rows for the purpose of inventory tracking.

parking lot

A parking lot is a polygon that defines the location and shape of a parking area on a map. By defining the number of parking spaces inside the parking lot, Security Center can calculate its percentage of occupancy during a given time period.

parking zone

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

partition

A partition is a type of entity that defines a set of entities that are only visible to a specific group of users. For example, a partition could include all areas, doors, cameras, and zones in one building.

partition administrator

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

Patroller

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

Patroller Config Tool

Patroller Config Tool is the Patroller administrative application used to configure Patroller-specific settings, such as adding Sharp cameras to the in-vehicle LAN, enabling features such as Manual Capture or New Wanted, and specifying that a username and password are needed to log on to Patroller.

Patroller tracking

Patroller tracking is a type of investigation task that allows you to replay the route followed by a Patroller on a given date on a map, or view the current location of Patroller vehicles on a map.

People counting

People counting is a type of operation task that keeps count in real-time of the number of cardholders in all secured areas of your system.

perimeter arm

Perimeter arm is arming an intrusion detection area in such a way that only sensors attributed to the area perimeter set the alarm off if triggered. Other sensors, such as motion sensors inside the area, are ignored.

permit

A permit is a type of entity that defines a single parking permit holder list. Each permit holder is characterized by a category (permit zone), a license plate number, a license issuing state, and optionally, a permit validity range (effective date and expiry date). Permits are used in both city and university parking enforcement.

permit hit

A permit hit is a hit that is generated when a read (license plate number) does not match any entry in a permit or when it matches an invalid permit.

permit restriction

A permit restriction is a type of entity that applies time restrictions to a series of parking permits for a given parking zone. Permit restrictions are only used by AutoVu™ Patrollers configured for University Parking Enforcement.

plaintext

In cryptography, plaintext is the data that is not encrypted.

Plan Manager

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

Plate Reader

Plate Reader is the software component of the Sharp unit that processes the images captured by the LPR camera to produce license plate reads, and associates each license plate read with a context image captured by the context camera. The Plate Reader also handles the communications with the Patroller and the LPR Manager. If an external wheel imaging camera is connected to the Sharp unit, the Plate Reader also captures wheel images from this camera.

plugin

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

Plugin

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

Plugins

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

Point of sale

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

primary server

Primary server is the default server chosen to perform a specific function (or role) in the system. To increase the system's fault-tolerance, the primary server can be protected by a secondary server on standby. When the primary server becomes unavailable, the secondary server automatically takes over.

private IP address

A private IP address is an IP address chosen from a range of addresses that are only valid for use on a LAN. The ranges for a private IP address are: 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.16.255.255, and 192.168.0.0 to 192.168.255.255. Routers on the Internet are normally configured to discard any traffic using private IP addresses.

private key

In cryptography, a private or secret key is an encryption/decryption key known only to one of the parties that exchange secret messages.

private task

A private task is a saved task that is only visible to the user who created it.

privilege

Privileges define what users can do, such as arming zones, blocking cameras, and unlocking doors, over the part of the system they have access rights to.

public key

In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key that is generated at the same time, can be used to effectively encrypt messages and verify digital signatures.

public key encryption

Public key encryption, also known as *asymmetric encryption*, is a type of encryption where two different keys are used to encrypt and decrypt information. The private key is a key that is known only to its owner, while the public key can be made known and available to other entities on the network. What is encrypted with one key can only be decrypted with the other key.

public key infrastructure

A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to support the distribution and identification of public encryption keys. This enables users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party.

public task

A public task is a saved task that can be shared and reused among multiple Security Center users.

R

reader

A reader is a sensor that reads the credential for an access control system. For example, this can be a card reader, or a biometrics scanner.

Reads

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

Reads/hits per day

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

Reads/hits per zone

Reads/hits per zone is a type of investigation task that reports on the number of reads and hits per parking zone for a selected date range.

realm

In identity terms, a realm is the set of applications, URLs, domains, or sites for which a token is valid. Typically a realm is defined using an Internet domain such as genetec.com, or a path within that domain, such as genetec.com/support/GTAC. A realm is sometimes described as a security domain because it encompasses all applications within a specified security boundary.

recording mode

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

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

recording state

Recording state is the current recording status of a given camera. There are four possible recording states: *Enabled*, *Disabled*, *Currently recording (unlocked)*, and *Currently recording (locked)*.

redirector

A redirector is a server assigned to host a redirector agent created by the Media Router role.

redirector agent

A redirector agent is an agent created by the Media Router role to redirect data streams from one IP endpoint to another.

redundant archiving

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

Remote

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

rendering rate

Rendering rate is the comparison of how fast the workstation renders a video with the speed the workstation receives that video from the network.

Report Manager

Report Manager is a type of role that automates report emailing and printing based on schedules.

report pane

Report pane is one of the panes found in the Security Desk task workspace. It displays query results or real-time events in a tabular form.

request to exit

Request to exit (REX) is a door release button normally located on the inside of a secured area that when pressed, allows a person to exit the secured area without having to show any credential. This can also be the signal from a motion detector. It is also the signal received by the controller for a request to exit.

reverse geocoding

Reverse geocoding is an AutoVu™ feature that translates a pair of latitude and longitude into a readable street address.

role

A role is a software module that performs a specific job within Security Center. Roles must be assigned to one or more servers for their execution.

roles and units view

The roles and units view is a browser view that lists the roles on your system with the units they control as child entities.

route

Route is a setting that configures the transmission capabilities between two end points in a network for the purpose of routing media streams.

Rules Engine

The Rules Engine is the component of Mission Control that analyzes and correlates the data (events) collected by Security Center, based on predefined rules. The Rules Engine uses this data to detect and trigger incidents in Mission Control.

S

same position

Same position is a type of parking regulation characterizing an overtime rule. A vehicle is in violation if it is seen parked at the exact same spot over a specified period of time. Patroller must be equipped with GPS capability in order to enforce this type of regulation.

schedule

A schedule is a type of entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).

scheduled task

A scheduled task is a type of entity that defines an action that executes automatically on a specific date and time, or according to a recurring schedule.

Software Development Kit

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

SDK certificate

An SDK certificate allows an SDK application (or plugin) to connect to Security Center. The certificate must be included in the Security Center license key for the SDK application to work.

secondary server
A secondary server is any alternate server on standby intended to replace the primary server in the case the latter becomes unavailable.

Secure Socket Layer
The Secure Sockets Layer (SSL) is a computer networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients.

secured area
A secured area is an area entity that represents a physical location where access is controlled. A secured area consists of perimeter doors (doors used to enter and exit the area) and access restrictions (rules governing the access to the area).

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

Security Center Federation™
The Security Center Federation™ role connects a remote, independent Security Center system to your local Security Center. That way, the remote system's entities and events can be used in your local system.

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

security clearance
A security clearance is a numerical value used to further restrict the access to an area when a threat level is in effect. Cardholders can only access (enter or exit) an area if their security clearance is equal or higher than the minimum security clearance set on the area.

Security Desk
Security Desk is the unified user interface of Security Center. It provides consistent operator flow across all of the Security Center's main systems, Omnicast™, Synergis™, and AutoVu™. Security Desk's unique task-based design lets operators efficiently control and monitor multiple security and public safety applications.

security token
An on-the-wire representation of claims that is cryptographically signed by the issuer of the claims, providing strong proof to any relying party as to the integrity of the claims and the identity of the issuer.

security token service
Secure token service (STS) is a claims provider implemented as a web service that issues security tokens. Active Directory

Federation Services (ADFS) is an example of a security token service. Also known as an issuer.

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

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

server mode The server mode is a special online operation mode restricted to Synergis™ units, in which the unit allows the Access Manager (the server) to make all access control decisions. The unit must stay connected to the Access Manager at all times to operate in this mode.

Server Admin Server Admin is the web application running on every server machine in Security Center that allows you to configure the settings of Genetec Server. Server Admin also allows you to configure the Directory role on the main server.

sharing guest Sharing guest is when Security Center system gives the rights to view and modify entities shared by another system.

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

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

SharpOS SharpOS is the software component of a Sharp or SharpX unit. SharpOS is responsible for everything related to plate capture, collection, processing, and analytics. For example, a SharpOS update may include new LPR contexts, new firmware, Sharp Portal updates, and updates to the Sharp's Windows services (Plate Reader, HAL, updater service, and so on).

Sharp Portal Sharp Portal is a web-based administration tool used to configure Sharp cameras for fixed or mobile AutoVu™ systems. From a web browser, you log on to a specific IP address (or the Sharp name in certain cases) that corresponds to the Sharp you want to configure. When you log on, you can configure options such as selecting the LPR context (e.g. Alabama, Oregon, Quebec, etc), selecting the read strategy (e.g. fast moving or slow moving vehicles), viewing the Sharp’s live video feed, and more.

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

Sharp VGA Sharp VGA is a Sharp unit that integrates the following components: an infrared illuminator; a standard definition

(640 x 480) LPR camera for plate capture; an integrated image processor; an NTSC or PAL color context camera with video streaming capabilities.

SharpX

SharpX is the camera component of the SharpX system. The SharpX camera unit integrates a pulsed LED illuminator that works in total darkness (0 lux), a monochrome LPR camera (1024 x 946 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The LPR data captured by the SharpX camera unit is processed by a separate hardware component called the AutoVu™ LPR Processing Unit.

Sharp XGA

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

SharpX VGA

SharpX VGA is the camera component of the SharpX system. The SharpX VGA camera unit integrates a pulsed LED illuminator that works in total darkness (0 lux), a monochrome LPR camera (640 x 480 @ 30 fps), and a color context camera (640 x 480 @ 30 fps). The LPR data captured by the SharpX VGA camera unit is processed by a separate hardware component called the AutoVu™ LPR Processing Unit.

single sign-on

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

standalone mode

Standalone mode is an offline operation mode of the interface module where it operates autonomously, making decisions based on the access control settings previously downloaded from the Synergis™ unit. Activity reporting occurs on schedule, or when the connection to the unit is available. Not all interface modules can operate in standalone mode.

standard schedule

A standard schedule is a type of schedule entity that may be used in all situations. Its only limitation is that it does not support daytime or nighttime coverage.

strict antipassback

A strict antipassback is an antipassback option. When enabled, a passback event is generated when a cardholder attempts to leave an area that they were never granted access to. When disabled, Security Center only generates passback events for cardholders entering an area that they never exited.

supervised mode

Supervised mode is an online operation mode of the interface module where the interface module makes decisions based on the access control settings previously downloaded from the Synergis™ unit. The interface module reports its activities in real time to the unit, and allows the unit to override a decision if it contradicts the current settings in the unit. Not all interface modules can operate in supervised mode.

SV appliance An SV appliance is a turnkey network security appliance that comes preinstalled with an embedded operating system and Genetec's Security Center. You can use SV appliances to quickly deploy a unified or standalone video surveillance and access control system.

SV-16 The SV-16 is a sub-compact network security appliance that comes preinstalled with Windows Embedded Standard and Genetec security software. The SV-16 is for small-scale, single server installations, and can support both cameras and access control readers.

SV-32 The SV-32 is a compact-sized network security appliance that comes pre-installed with Windows Embedded Standard and Genetec's Security Center. It enables you to quickly deploy a unified or standalone video surveillance and access control system.

SV-PRO The SV-PRO is a rack-mount appliance that comes preloaded with Genetec security software, and Windows 10 Enterprise LTSB. The SV-PRO is for small to mid-scale, single or multiple server installations, and can support both cameras and access control readers.

symmetric encryption Symmetric encryption is a type of encryption where the same key is used for both encryption and decryption.

synchronous video A synchronous video is a simultaneous live video or playback video from more than one camera that are synchronized in time.

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

Synergis™ appliance A Synergis™ appliance is an IP-ready security appliance manufactured by Genetec Inc. that is dedicated to access control functions. All Synergis™ appliances come preinstalled with Synergis™ Softwire and can be enrolled as access control units in Security Center.

Synergis™ Appliance Portal Synergis™ Appliance Portal is the web-based administration tool used to configure and administer the Synergis™ appliance, as well as upgrade its firmware.

Synergis™ Cloud Link Synergis™ Cloud Link is an intelligent and PoE-enabled access control appliance of Genetec Inc. that supports a variety of third-party interface modules over IP and RS-485. Synergis™ Cloud Link is seamlessly integrated with Security Center and is capable of making access control decisions independently of the Access Manager.

Synergis™ Master Controller
Synergis™ Master Controller (SMC) is an access control appliance of Genetec Inc. that supports a variety of third-party interface modules over IP and RS-485. SMC is seamlessly integrated with Security Center and is capable of making access control decisions independently of the Access Manager.

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

Synergis™ unit
A Synergis™ unit is a Synergis™ appliance that is enrolled as an access control unit in Security Center.

System
The System task is an administration task that allows you to configure roles, macros, schedules, and other system entities and settings.

system event
A system event is a predefined event that indicates the occurrence of an activity or incident. System events are defined by the system and cannot be renamed or deleted.

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

T

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

task
A task is the central concept on which the entire Security Center user interface is built. Each task corresponds to one aspect of your work as a security professional. For example, use a monitoring task to monitor system events in real-time, use an investigation task to discover suspicious activity patterns, or use an administration task to configure your system. All tasks can be customized and multiple tasks can be carried out simultaneously.

taskbar
A taskbar is a user interface element of the Security Center client application window, composed of the Home tab and the active task list. The taskbar can be configured to appear on any edge of the application window.

task cycling
A task cycling is a Security Desk feature that automatically cycles through all tasks in the active task list following a fixed dwell time.

task workspace
A task workspace is an area in the Security Center client application window reserved for the current task. The workspace is typically devided into the following panes: canvas, report pane, dashboard, and Logical view.

threat level
Threat level is an emergency handling procedure that a Security Desk operator can enact on one area or the entire system to deal promptly with a potentially dangerous situation, such as a fire or a shooting.

tile
A tile is an individual window within the canvas, used to display a single entity. The entity displayed is typically the video from a camera, a map, or anything of a graphical nature. The look and feel of the tile depends on the displayed entity.

tile ID
The tile ID is the number displayed at the upper left corner of the tile. This number uniquely identifies each tile within the canvas.

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

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

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

Time and attendance
Time and attendance is a type of investigation task that reports on who has been inside a selected area and the total duration of their stay within a given time range.

timed antipassback
Timed antipassback is an antipassback option. When Security Center considers a cardholder to be already in an area, a passback event is generated when the cardholder attempts to access the same area again during the time delay defined by *Presence timeout*. When the time delay has expired, the cardholder can once again pass into the area without generating a passback event.

timeline
A timeline is a graphic illustration of a video sequence, showing where in time, motion, and bookmarks are found. Thumbnails can also be added to the timeline to help the user select the segment of interest.

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

Transmission Control Protocol

A connection-oriented set of rules (protocol) that, along with the IP (Internet Protocol), is used to send data over an IP network. The TCP/IP protocol defines how data can be transmitted in a secure manner between networks. TCP/IP is the most widely used communications standard and is the basis for the Internet.

Transport Layer Security

Transport Layer Security (TLS) is a protocol that provides communications privacy and data integrity between two applications communicating over a network. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

twilight schedule

A twilight schedule is a type of schedule entity that supports both daytime and nighttime coverages. A twilight schedule cannot be used in all situations. Its primary function is to control video related behaviors.

two-person rule

The two-person rule is the access restriction placed on a door that requires two cardholders (including visitors) to present their credentials within a certain delay of each other in order to gain access.

U

unit

A unit is a hardware device that communicates over an IP network that can be directly controlled by a Security Center role. We distinguish four types of units in Security Center:

- Access control units, managed by the Access Manager role
- Video units, managed by the Archiver role
- LPR units, managed by the LPR Manager role
- Intrusion detection units, managed by the Intrusion Manager role

Unit discovery tool

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

Unit enrollment tool

The *Unit enrollment tool* allows you to discover IP units (video and access control) connected to your network, based on their manufacturer, and network properties (discovery port, IP address range, password, and so on). Once discovered, the units can be added to your system.

Unit replacement

Unit replacement is a tool that is used to replace a failed hardware device with a compatible one, while ensuring that the data associated to the old unit gets transferred to the new one. For an access control unit, the configuration of the old unit is copied to the new unit. For a video unit, the video archive associated to the old unit is now associated to the new unit, but the unit configuration is not copied.

unit synchronization

Unit synchronization is the process of downloading the latest Security Center settings to an access control unit. These settings, such as access rules, cardholders, credentials, unlock schedules, and so on, are required so that the unit can make accurate and autonomous decisions in the absence of the Access Manager.

University Parking Enforcement

University Parking Enforcement is a Patroller software installation that is configured for university parking enforcement: the enforcement of scheduled parking permits or overtime restrictions. The use of maps is mandatory. Hotlist functionality is also included.

unlock schedule

An unlock schedule defines the periods of time when free access is granted through an access point (door side or elevator floor).

unreconciled read

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

user

A user is a type of entity that identifies a person who uses Security Center applications and defines the rights and privileges that person has on the system. Users can be created manually or imported from an Active Directory.

user group

A user group is a type of entity that defines a group of users who share common properties and privileges. By becoming member of a group, a user automatically inherits all the properties of the group. A user can be a member of multiple user groups. User groups can also be nested.

user level

A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera PTZ, viewing the video feed from a camera, or to stay logged on when a threat level is set. The smaller the value, the higher the priority.

User management

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

V

validation key

A validation key is a serial number uniquely identifying a computer that must be provided to obtain the license key.

Vault

Vault is a tool that displays your saved snapshots and exported G64, G64x, and GEK (encrypted) video files. From the Vault, you can view the video files, encrypt and decrypt files, convert files to ASF, or package files with the Genetec Video Player.

vehicle identification number

A vehicle identification number (VIN) is an identification number that a manufacturer assigns to vehicles. This is usually visible from outside the vehicle as a small plate on the dashboard. A VIN can be included as additional information with license plate entries in a hotlist or permit list, to further validate a hit and ensure that it is the correct vehicle.

video analytics

Video analytics is the software technology that is used to analyze video for specific information about its content. Examples of video analytics include counting the number of people going through a door, license plate recognition, detection of unattended objects, or the direction of people walking or running.

video archive

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

video decoder

A video decoder is a device that converts a digital video stream into analog signals (NTSC or PAL) for display on an analog monitor. The video decoder is one of the many devices found on a video decoding unit.

video encoder

A video encoder is a device that converts an analog video source to a digital format, by using a standard compression algorithm, such as H.264, MPEG-4, MPEG-2, or M-JPEG. The video encoder is one of the many devices found on a video encoding unit.

video file

A video file is a file created by an archiving role (Archiver or Auxiliary Archiver) to store archived video. The file extension is G64 or G64x. You need Security Desk or the Genetec Video Player to view video files.

Video file explorer

Video file explorer is a type of investigation task that browses through your file system for video files (G64 and G64x) and allows you to play, convert to ASF, and verify the authenticity of these files.

video sequence

A video sequence is any recorded video stream of a certain duration.

video stream

A video stream is an entity representing a specific video quality configuration (data format, image resolution, bit rate, frame rate, and so on) on a camera.

Video

The Video task is a type of administration task that allows you to configure video management roles, units, analog monitors, and cameras.

video unit

A video unit is a type of video encoding or decoding device that is capable of communicating over an IP network and can incorporate one or more video encoders. Video units are available in a variety of brands and models, some of which support audio and others support wireless communication.

The high-end encoding models also include their own recording and video analytic capabilities. Cameras (IP or analog), video encoders, and video decoders are all examples of video units. In Security Center, a video unit refers to a type of entity that represents a video encoding or decoding device.

video watermarking

Video watermarking is the process by which a digital signature (watermark) is added to each recorded video frame to ensure its authenticity. If anyone later tries to make changes to the video (add, delete or modify a frame), the signatures will no longer match, which shows that the video has been tampered with.

virtual zone

A virtual zone is a zone entity where the I/O linking is done by software. The input and output devices can belong to different units of different types. A virtual zone is controlled by the Zone Manager and only works when all the units are online. It can be armed and disarmed from Security Desk.

Visit details

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

Visitor activities

Visitor activities is a type of investigation task that reports on visitor activities (access denied, first person in, last person out, antipassback violation, and so on).

visitor escort rule

The visitor escort rule is the additional access restriction placed on a secured area that requires visitors to be escorted by a cardholder during their stay. Visitors who have an escort are not granted access through access points until both they and their assigned escort (cardholder) present their credentials within a certain delay.

Visitor management

Visitor management is a type of operation task that allows you to check in, check out, and modify visitors, as well as manage their credentials, including temporary replacement cards.

visual tracking

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

VSIP port

The VSIP port is the name given to the discovery port of Verint units. A given Archiver can be configured to listen to multiple VSIP ports.

W

watchdog

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

Web-based SDK

The Web-based SDK role exposes the Security Center SDK methods and objects as web services to support cross-platform development.

Web Client

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

Web Map Service

Web Map Service (WMS) is a standard protocol for serving georeferenced map images over the Internet that are generated by a map server using data from a GIS database.

wheel imaging

Wheel imaging is a virtual tire-chalking technology that takes images of the wheels of vehicles to prove whether they have moved between two license plate reads.

widget

A widget is a component of the graphical user interface (GUI) with which the user interacts.

Windows Communication Foundation

Windows Communication Foundation (WCF) is a communication architecture used to enable applications, in one machine or across multiple machines connected by a network, to communicate. AutoVu™ Patroller uses WCF to communicate wirelessly with Security Center.

Z

zone

A zone is a type of entity that monitors a set of inputs and triggers events based on their combined states. These events can be used to control output relays.

Zone Manager

Zone Manager is a type of role that manages virtual zones and triggers events or output relays based on the inputs configured for each zone. It also logs the zone events in a database for zone activity reports.

Zone occupancy

Zone occupancy is a type of investigation task that reports on the number of vehicles parked in a selected parking zone, and the percentage of occupancy.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ Technical Information Site:** The latest documentation is available on the Technical Information Site. To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. Can't find what you're looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explain how the product works and provide instructions on how to use the product features. Patroller and the Sharp Portal also include context-sensitive help for each screen. To access the help, click **Help**, press F1, or tap the **?** (question mark) in the different client applications.

Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to the Genetec™ Technical Information Site, where you can find information and search for answers to your product questions.

- **Genetec™ Technical Information Site:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

  Before contacting GTAC or opening a support case, it is recommended to search the Technical Information Site for potential fixes, workarounds, or known issues.

  To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. Can't find what you're looking for? Contact documentation@genetec.com.
- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: EN_GLM_ASSURANCE and EN_GLM_ADVANTAGE.

Additional resources

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

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss a variety of topics, ranging from technical questions to technology tips. You can log in or sign up at https://gtapforum.genetec.com.
- **Technical training:** In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to http://www.genetec.com/support/training/training-calendar.

Licensing

- For license activations or resets, please contact GTAC at https://gtap.genetec.com.
- For issues with license content or part numbers, or concerns about an order, please contact Genetec™ Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, please contact Genetec™ Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Please contact GTAC at https://gtap.genetec.com to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.

Index