



Security Desk User Guide

5.5

Copyright notice

© Genetec Inc., 2016

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

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

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

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

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

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

All specifications are subject to change without notice.

Document information

Document title: Security Desk User Guide 5.5

Document number: EN.500.004-V5.5.B(4)

Document update date: July 28, 2016

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

About this guide

This guide describes Security Desk features and commands, and provides instruction on how to perform tasks, such as live monitoring of events, video playback and instant replay, report generation, LPR route playback, alarm management, and visitor management.

Notes and notices

The following notes and notices might appear in this guide:

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

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

Contents

Preface: Preface

Copyright notice	ii
About this guide	iii

Part I: Introduction to Security Desk

Chapter 1: Security Desk at a glance

About Security Desk	3
How Security Center is organized	4
Logging on to Security Desk	5
Closing Security Desk	6
Defining how your workspace is saved	6
Home page overview	7
UI component overview	9
Overview of the About page	11
About the area view	13
Changing passwords	15
Sending feedback	16

Chapter 2: Canvas

About tiles	18
Tile menu commands	20
Viewing entities in the canvas	22
Customizing how entities are displayed in the canvas	22
How maps are displayed in the Security Desk canvas	23
Unpacking content in tiles	24
Customizing entity cycling options	25
Maximizing the canvas to full screen	26
Selecting which monitors can switch to full screen	26
Changing tile patterns	27
Editing and creating tile patterns	28
Customizing how tiles are displayed	29

Chapter 3: Widgets

Alarm widget	31
Area widget	33
Camera widget	34
Door widget	37
Intrusion detection area widget	38
PTZ widget	39

Tile widget	41
Zone widget	43
Chapter 4: Tasks	
Opening tasks	45
Saving tasks	46
Adding tasks to your Favorites list	47
Hiding the Favorites and Recent items lists from your home page	47
Sending tasks to other users	48
Sending tasks using a manual action	48
Closing tasks using a system action	50
Customizing task behaviour	51
Chapter 5: Reports	
Reporting task workspace overview	53
Generating reports	55
Selecting date and time ranges for reports	55
Exporting generated reports	56
Printing generated reports	57
Customizing time zone settings	57
Generating and saving reports	59
Generating and saving reports using a system action	59
Customizing the report pane	61
Customizing report behavior	62
Chapter 6: Basic tasks	
Monitoring events	64
Selecting events to monitor	65
Selecting entities to monitor	65
Event colors	66
Customizing Monitoring task options	67
Event occurrence period	68
Searching for entities	69
Searching for entities using the search tool	69
Triggering hot actions	71
Triggering one-time actions	72
Configuring the notification tray	73
Notification tray icons	73
Moving the taskbar	76
Remote monitoring	77
Connecting to remote Security Desks	78
Monitoring events on remote Security Desks	80
Monitoring alarms on remote Security Desks	81

Actions you can perform on remote Security Desks	82
Chapter 7: Working with maps	
About Plan Manager	86
Working with maps	87
Basic map commands	87
Showing or hiding information on your maps	88
Differences between Monitoring and Maps tasks	89
Supported map objects	91
Chapter 8: Advanced tasks	
Starting macros	96
Finding out what changes were made to the system configuration	97
Report pane columns for the Audit trails task	97
Investigating user related activity on the system	98
Report pane columns for the Activity trails task	100
Viewing properties of units	101
Report pane columns for the Hardware inventory task	101
Monitoring your computer resources	103
Hardware information dialog box	103
Using the hardware benchmark tool	105
Shortcuts to external tools	107
Customizing user logon options	109
Customizing network options	111
Chapter 9: Keyboard shortcuts	
Default keyboard shortcuts	113
Switching tasks using your keyboard	119
Switching tasks on a remote monitor using your keyboard	119
Displaying cameras using your keyboard	120
Displaying cameras on a remote monitor using your keyboard	120
Customizing keyboard shortcuts	122
Part II: Video	
Chapter 10: Video at a glance	
About Omnicast	125
Chapter 11: Cameras	
About cameras (video encoders)	127
Viewing cameras in tiles	128
On-tile video controls	129
Controlling camera sequences	130
How PTZ cameras are displayed in the canvas	131

Controlling PTZ cameras	132
Dewarping 360 degree camera lenses	133
Viewing video on analog monitors	135
Synchronizing video in tiles	137
Changing the video stream	138
Zooming in and out of video	139
Creating digital zoom presets	140
About visual tracking	141
Tracking moving targets	141
Adding bookmarks to video sequences	143
Viewing bookmarked videos	143
Customizing snapshot options	145
Taking snapshots of video	146
Editing video snapshots	147
Camera blocking	148
Blocking users from viewing video	149
How video is displayed if the Directory role disconnects	150
Viewing camera settings	152

Chapter 12: Video archives

Live and playback video modes	155
Switching between video modes	157
About the video timeline	159
Creating a playback loop	160
Viewing video archives	161
Report pane columns for the Archives task	162
Investigating Archiver events	163
Report pane columns for the Archiver events task	163
Searching video archives for motion events	164
Report pane columns for the Motion search task	165
Searching video archives for camera events	167
Report pane columns for the Camera events task	167
Preparing Bosch units to record video analytics events	168
Searching for video analytics events stored on Bosch units	169
Report pane columns for the Forensic search task	169
Effects of Daylight Saving Time on video archives	171
Effects of time adjusted backward	171
Effects of time adjusted forward	171
Changing the time zone to UTC	173

Chapter 13: Video export

Video export formats	175
Watermarks with exported video files	176

Configuring settings for exporting video	177
Exporting video	179
The Export video dialog box	182
Viewing exported video files	184
Viewing exported files in the Video file explorer	185
Sharing exported video files	187
Converting video files to ASF or MP4 format	188
Conversion dialog box	188
Re-exporting G64 and G64x video files	190
Viewing the properties of video files	192
Report pane columns for the Archive storage details task	193
Protecting video files from being deleted	195
Encrypting exported video files	197
Decrypting exported video files	197

Chapter 14: Video options

Configuring joysticks	199
Configuring CCTV keyboards	201
Customizing video stream options	202
Video options	203

Part III: Access control

Chapter 15: Access control at a glance

About Synergis	208
How access events are displayed in tiles	210

Chapter 16: Cardholders and visitors

About cardholders	212
How cardholders are displayed in the Security Desk canvas	213
Creating cardholders	214
Assigning access rules to cardholders	216
Checking in new visitors	218
Checking in returning visitors	220
Cropping pictures	221
Applying transparent backgrounds to pictures	222
Assigning credentials	223
Requesting credential cards	225
Printing paper credentials	226
Assigning temporary cards	227
Restoring original cards to cardholders and visitors	227
Using signature pads	229
Checking out visitors	230

Investigating cardholder events	231
Report pane columns for the Cardholder activities task	231
Investigating visitor events	233
Report pane columns for the Visitor activities task	234
People counting	235
Tracking cardholders present in an area	236
Report pane columns for the Area presence task	236
Tracking attendance in an area	238
Report pane columns for the Time and attendance task	238
Tracking the duration of a visitor's stay	239
Report pane columns for the Visit details task	239
Viewing properties of cardholder group members	241
Report pane columns for the Cardholder configuration task	242
The modify cardholder dialog box	243
The modify visitor dialog box	245
Searching for cardholders and visitors	247
Report pane columns for the Cardholder management and Visitor management tasks	248
Searching for cardholders and visitors using their credential	248

Chapter 17: Credentials

About credentials	251
Credential enrollment methods	254
Enrolling multiple credentials automatically	255
Enrolling multiple credentials manually	257
Creating credentials	259
Responding to credential card requests	262
Investigating request history of credential cards	263
Report pane columns for the Credential request history task	263
Investigating credential events	265
Report pane columns for the Credential activities task	265
Viewing credential properties of cardholders	267
Report pane columns for the Credential configuration task	267
Searching for credentials	269
Report pane columns for the Credential management task	269

Chapter 18: Areas, doors, and elevators

How areas are displayed in the canvas	272
How doors are displayed in the Security Desk canvas	273
Allowing access through doors	274
Preventing access through doors	276
Investigating area events	277
Report pane columns for the Area activities task	277
Investigating door events	279

Report pane columns for the Door activities task	279
Investigating elevator events	281
Report pane columns for the Elevator activities task	281
Identifying who is granted/denied access at access points	283
Report pane columns for the Cardholder access rights task	283
Identifying who is granted access to doors and elevators	284
Report pane columns for the Door troubleshooter task	284
Identifying which entities are affected by access rules	285
Report pane columns for the Access rule configuration task	285

Chapter 19: Access control units

Investigating events related to access control units	287
Report pane columns for the Access control unit events task	287
Viewing I/O configuration of access control units	288
Report pane columns for the I/O configuration task	288
Enabling external access control devices	289

Part IV: License Plate Recognition

Chapter 20: LPR at a glance

About AutoVu	292
------------------------	-----

Chapter 21: LPR events

How LPR events are viewed in Security Desk	294
Configuring Security Desk to automatically display high-resolution context images	295
Customizing which LPR information to display in Security Desk	296
Monitoring LPR events in tile mode	298
Monitoring LPR events in map mode	300

Chapter 22: Reads, hits, hotlists, and permits

About hotlists	303
About permits	304
Editing hotlists and permit lists	306
Hotlist annotation fields	307
Investigating reported hits	308
Report pane columns for the Hits task	309
Investigating reported hit statistics	311
Printing hit reports	313
Editing plate reads	315
Investigating reported license plate reads	316
Report pane columns for the Reads task	317
Investigating reported read statistics	318
Investigating reported reads (Multi-region)	320
Report pane columns for the Reads (Multi-region) task	321

Investigating reported hits (Multi-region)	322
Report pane columns for the Hits (Multi-region) task	323
Investigating reported reads and hits per day	324
Report pane columns for the Reads/hits per day task	324
Investigating reported reads and hits per parking zone	326
Report pane columns for the Reads/hits per zone task	326

Chapter 23: Patroller

About AutoVu Patroller	329
Replaying Patroller routes	330
Tracking the current location of a Patroller	331
Investigating how Patroller applications are used daily	332
Report pane columns for the Daily usage per Patroller task	333
Investigating logon/logoff records of Patrollers	334
Report pane columns for the Logons per Patroller task	334
Investigating the number of vehicles in parking zones	335
Report pane columns for the Zone occupancy task	336

Chapter 24: Mobile License Plate Inventory

How AutoVu MLPI works	338
Removing license plate reads from offload files	339
Removing data from offload files	340
Creating parking facility inventories	341
Viewing and comparing parking facility inventories	344
Report pane columns for the Inventory report task	345

Part V: Alarms and critical events

Chapter 25: Alarms

How alarms are displayed in the Security Desk canvas	348
Enabling alarm monitoring in the Monitoring task	350
Acknowledging alarms	351
Alarm information available when monitoring alarms	352
Filtering and grouping alarms in Security Center	354
Muting repeated alarm sounds	356
Forwarding alarms to other users automatically	357
Forwarding alarms to other users manually	358
Investigating current and past alarms	359
Report pane columns for the Alarm report task	360
Triggering alarms manually	362
Customizing alarm behavior	363
Customizing picture-in-picture windows for alarms	364

Chapter 26: Incidents and threat levels

Reporting incidents	366
Creating incident packages	368
Reviewing and modifying reported incidents	371
Report pane columns for the Incidents task	372
Responding to critical events through threat levels	373
Clearing threat levels	374

Chapter 27: Zones and intrusion detection

How zones are displayed in the Security Desk canvas	377
Arming and disarming zones	378
Investigating zone events	379
Report pane columns for the Zone activities task	379
Changing intrusion detection area statuses	380
Investigating intrusion detection area events	381
Report pane columns for the Intrusion detection area activities task	381
Investigating intrusion detection unit events	383
Report pane columns for the Intrusion detection unit events task	383

Part VI: Troubleshooting

Chapter 28: General troubleshooting

Viewing system messages	386
Viewing system health events	388
Report pane columns for the Health history task	389
Viewing the health status and availability of entities	390
Report pane columns for the Health statistics task	390
Monitoring the status of your system	392
Entity states	394
Troubleshooting: entities	395
Deactivating and activating roles	396
Troubleshooting: query filters	397
Collecting diagnostic data	398

Chapter 29: Troubleshooting video

Troubleshooting: Video units are offline	401
Troubleshooting: Cannot view live video	402
Troubleshooting: Video stream issues	405
Troubleshooting: Determining whether the workstation or the network cause video degradation	406
Troubleshooting: "Impossible to establish video session with the server" errors	408
Troubleshooting: No playback video available	409
Troubleshooting: Cameras are not recording	410
Troubleshooting: Video units cannot be added	413

Troubleshooting: Video units cannot be deleted	416
Troubleshooting: H.264 video stream issues	417
Troubleshooting: Hardware acceleration issues	418
Chapter 30: Troubleshooting access control	
Viewing access control health events	420
Report pane columns for the Access control health history task	420
Access troubleshooter tool	421
Testing access rules at doors and elevators	422
Testing cardholder access rights	423
Testing cardholder access rights based on credentials	423
Troubleshooting: Driver fails to install for HID OMNIKEY USB readers	424
Security Desk reference	
Appendix A: Events and actions	426
Event types	427
Action types	443
Appendix B: Graphical overview of Security Desk tasks	452
Overview of the Monitoring task	453
Overview of the Maps task	455
Maps toolbar	456
Overview of the Remote task	458
Overview of the Bookmarks task	459
Overview of the Archives task	461
Overview of the Motion search task	462
Overview of the Video file explorer task	464
Overview of the Archive storage details task	466
Overview of the Cardholder management task	468
Overview of the Visitor management task	470
Overview of the Credential management task	472
Overview of the Hotlist and permit editor task	474
Overview of the Inventory management task	475
Overview of the Patroller tracking task	476
Patroller tracking timeline controls	477
Overview of the System status task	479
System status task columns	479
Overview of the Alarm monitoring task	484
Overview of the Alarm report task	485
Overview of the Enhanced cardholder access rights task	486
Enabling the Enhanced cardholder access rights task	487
Glossary	488

Where to find product information	524
Technical support	525

Part I

Introduction to Security Desk

This part includes the following chapters:

- Chapter 1, "[Security Desk at a glance](#)" on page 2
- Chapter 2, "[Canvas](#)" on page 17
- Chapter 3, "[Widgets](#)" on page 30
- Chapter 4, "[Tasks](#)" on page 44
- Chapter 5, "[Reports](#)" on page 52
- Chapter 6, "[Basic tasks](#)" on page 63
- Chapter 7, "[Working with maps](#)" on page 85
- Chapter 8, "[Advanced tasks](#)" on page 95
- Chapter 9, "[Keyboard shortcuts](#)" on page 112

Security Desk at a glance

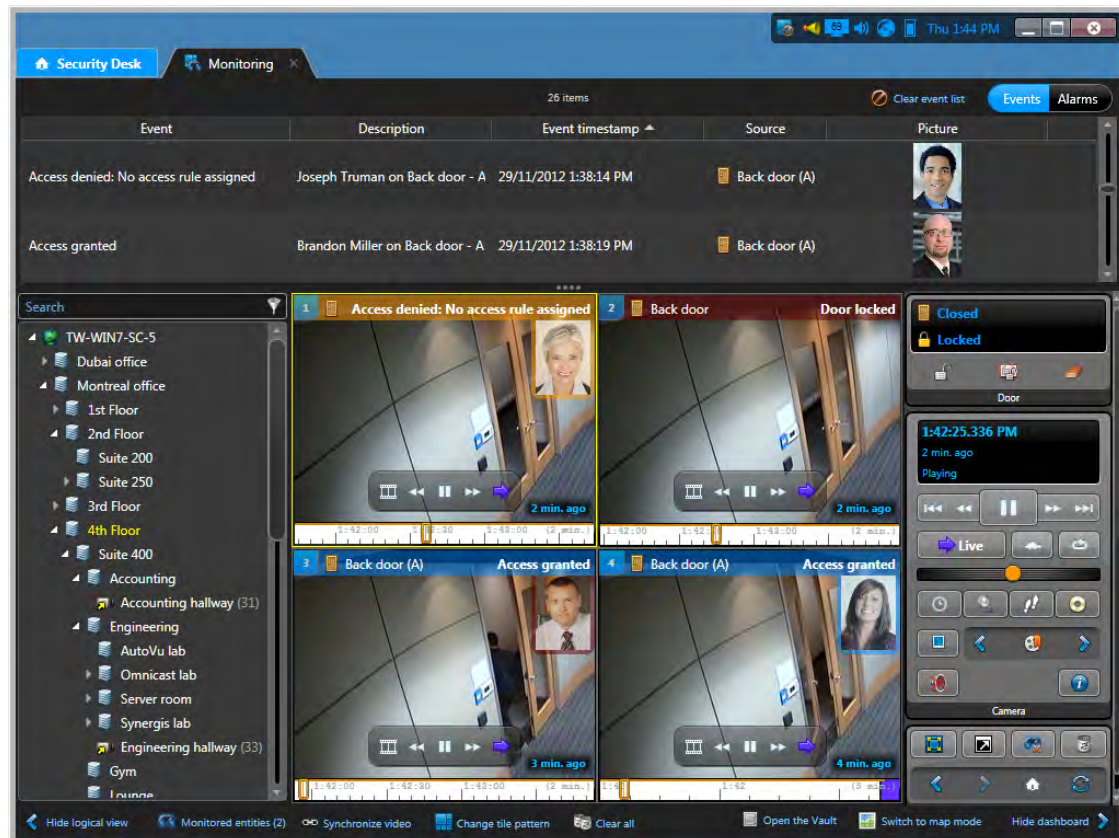
This section includes the following topics:

- ["About Security Desk "](#) on page 3
- ["How Security Center is organized"](#) on page 4
- ["Logging on to Security Desk"](#) on page 5
- ["Closing Security Desk"](#) on page 6
- ["Home page overview"](#) on page 7
- ["UI component overview"](#) on page 9
- ["Overview of the About page"](#) on page 11
- ["About the area view"](#) on page 13
- ["Changing passwords"](#) on page 15
- ["Sending feedback"](#) on page 16

About 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.

Within a single interface, you can monitor real-time events and alarms, generate reports, track door and cardholder activity, and view live and recorded video. When connected to a *Federation* of multiple systems, Security Desk allows you to monitor, report on, and manage hundreds of sites.



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)*. 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 Desk

To log on to Security Desk, you must open the Security Desk application and connect to the Security Center server.

Before you begin


Make sure that you have your username, password, and the name of the *Directory* that you want to connect to.

What you should know

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

NOTE: After a period of inactivity you might be locked out of Security Desk, and have to enter your credentials to use the application again.

To log on to Security Desk:

- 1 To open Security Desk, click **Start > All programs > Genetec Security Center 5.5 > Security Desk**.
- 2 In the *Logon* dialog box, do one of the following:
 - Enter your Security Center username and password.
 - Log on using your Windows user account by selecting **Use Windows credentials**.
- 3 In the **Directory** field, enter the name or IP address of the main Security Center server.
- 4 If you are required to log on with supervision, your supervisor must provide a username and password.
- 5 Click **Log on**.
- 6 To log off, click the home tab () and then click **Log off**.


Closing Security Desk

You can close Security Desk and save your workspace for the next time you log on.

What you should know

By default, you are asked to save your workspace when you close Security Desk. You can change this behavior from the *Options* dialog box.

To close Security Desk:

- 1 In the upper-right corner of the Security Desk window, click the exit button .
- 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 Security Desk, click **Save**.

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 application to behave regardless of whether you have unsaved changes in your task list.

What you should know

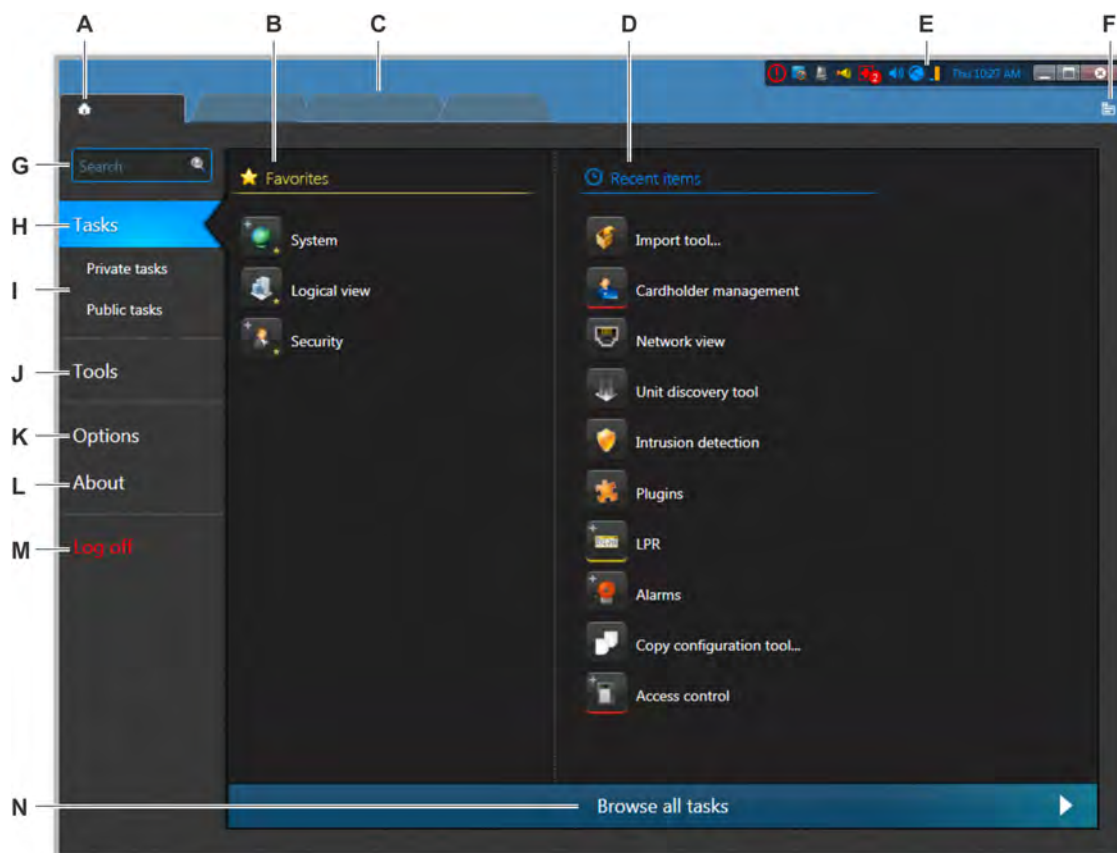
This setting is saved as part of your user profile and applies to Security Desk and Config Tool.

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	<p>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.</p> <p>From the <i>Options</i> dialog box, you can choose which icons you want to have appear in the notification bar.</p>
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	<p>Click to view the saved tasks that are available to you.</p> <ul style="list-style-type: none"> • 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	<p>Click to view the tools that you can start directly from your home page. The Tools page is divided into the following two sections:</p> <ul style="list-style-type: none"> • 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 73

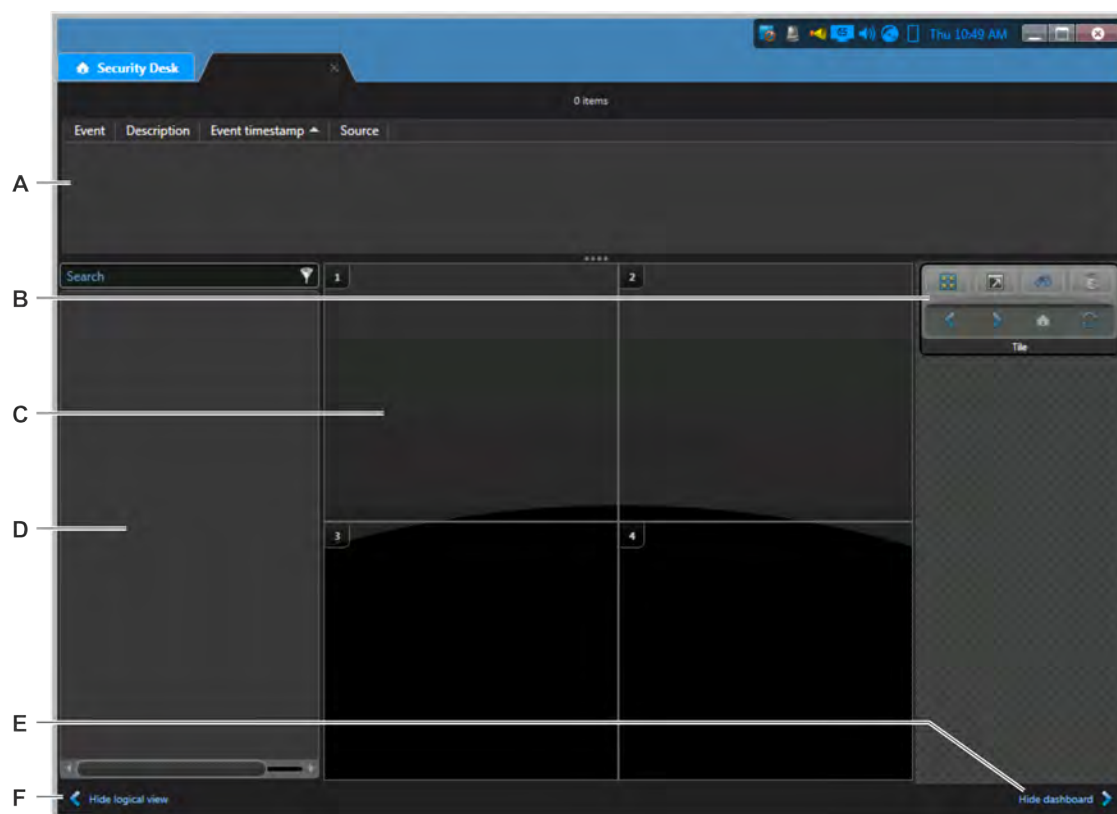
[Saving tasks](#) on page 46

[Opening tasks](#) on page 45

[Shortcuts to external tools](#) on page 107

UI component overview

There are a few main parts in the Security Desk user interface: the *area view*, *report pane*, *canvas*, and *dashboard*. These components are displayed in most tasks. This section gives you a general overview of where these components are located in the user interface.



- | | |
|----------------------|--|
| A Report pane | Displays information in the form of a table listing events, active alarms, or query results, depending on the task you are using. The information can appear as text or graphics (cardholder picture, timeline, thumbnails, and so on). |
| B Dashboard | Contains widget commands related to the entity type displayed in the selected tile in the canvas. |
| C Canvas | <p>Allows you to view and control entities such as videos, tile plugins, road maps, cardholder pictures, and so on. The canvas only appears in certain tasks. There are two canvas display modes:</p> <ul style="list-style-type: none"> • 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. • 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. This display mode is used in the <i>Monitoring</i> task, and in some LPR-related tasks. |
| D Area view | Lists all the entities that are part of your system, and allows you to bring them into the canvas. |

E Hide dashboard Click to hide or show the dashboard.

F Hide area view Click to hide or show the area view.

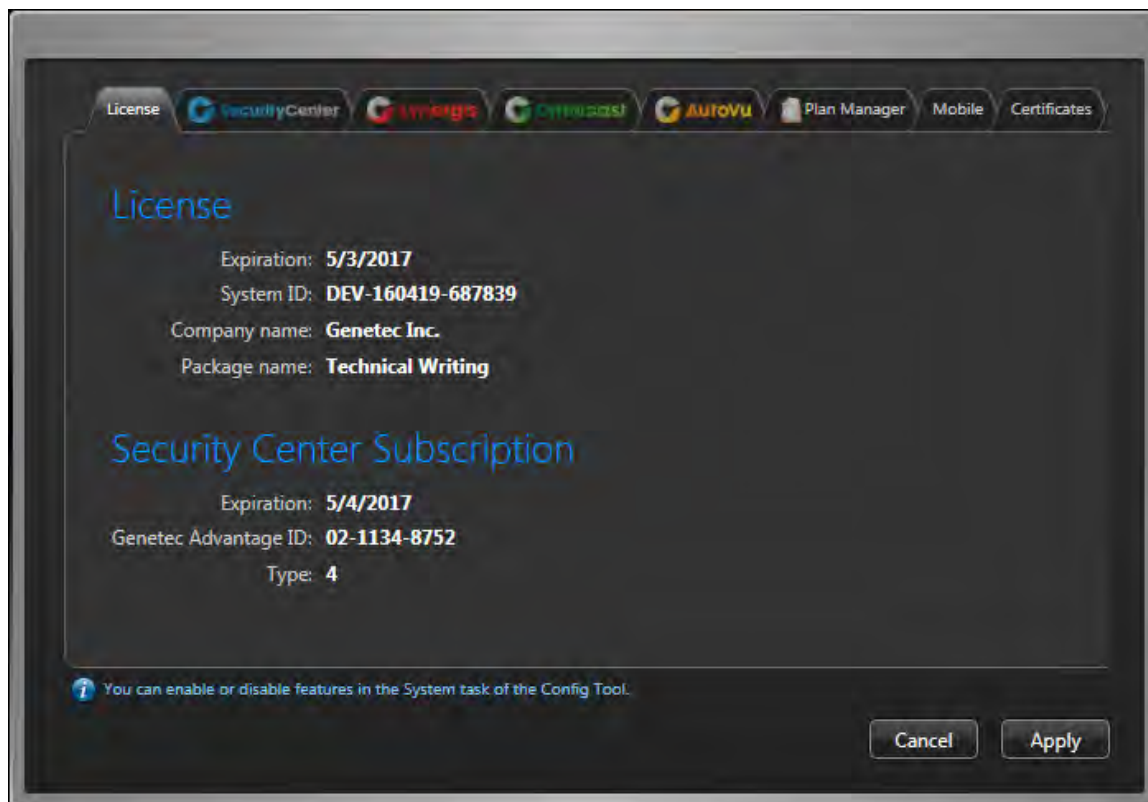
Related Topics

[Monitoring LPR events in map mode](#) on page 300

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.



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.

Related Topics

[Changing passwords](#) on page 15

[Sending feedback](#) on page 16

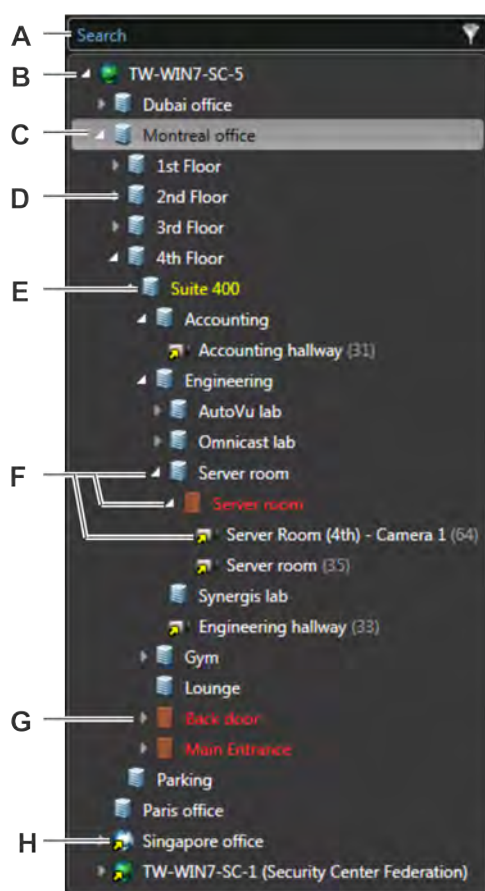
About the area view

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 <i>Search</i> 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	Configure entity	Right-click an entity in the area view, and then click Configure entity (⚙️) to jump to that entity's configuration page in Config Tool. You need the user privilege to modify entity properties to use this command.

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 <i>federated systems</i> are shown with a yellow arrow superimposed on the regular entity icon (). They are called <i>federated entities</i> .

Related Topics

[Viewing entities in the canvas](#) on page 22

[Searching for entities](#) on page 69

[Entity states](#) on page 394

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**.

Sending feedback

You can send feedback to Genetec 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 feedback**.
- 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**.

Canvas

This section includes the following topics:

- ["About tiles"](#) on page 18
- ["Tile menu commands"](#) on page 20
- ["Viewing entities in the canvas"](#) on page 22
- ["How maps are displayed in the Security Desk canvas"](#) on page 23
- ["Unpacking content in tiles"](#) on page 24
- ["Maximizing the canvas to full screen"](#) on page 26
- ["Changing tile patterns"](#) on page 27
- ["Editing and creating tile patterns"](#) on page 28
- ["Customizing how tiles are displayed"](#) on page 29

About tiles

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.

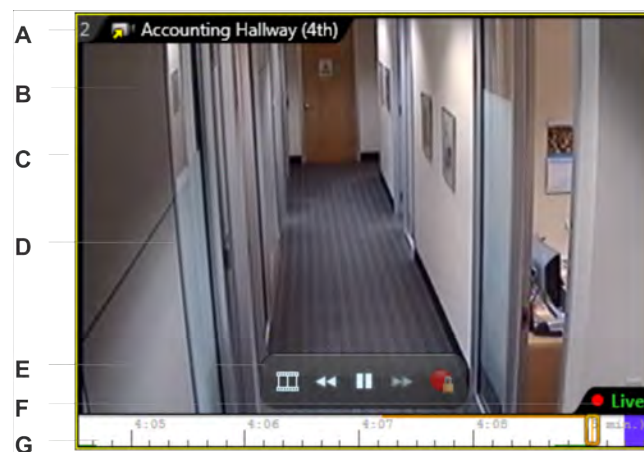
Tiles can display the following:

- Entities
- Event information
- Live and playback video
- Video images
- Cardholder and visitor pictures and information
- LPR reads
- Web pages
- Tile plugins
- maps

Content is automatically displayed in tiles when events occur related to the entities you are monitoring. You can also display entities by dragging them into a tile. Security Desk tiles have a *tile-memory*, meaning that Security Desk remembers the last 8 entities displayed in each tile. Using the commands in tile widget, you can switch to the previous, next, and initial tile content.

You can right-click inside the tile to view tile menu commands.

The following figure shows a tile displaying a camera.



A	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. If the tile ID is blue, it means event monitoring is enabled for the tile. If it is black, monitoring is disabled. If it is red with a narrow band of blue, event and alarm monitoring are enabled for the tile.
B	Tile toolbar	Displays the entity name. When an event occurs, information corresponding to the event is also shown in the tile toolbar.
C	Yellow frame	Indicates that the tile is selected.

D	Video stream	The streaming video is displayed inside the tile. Double-click to expand the tile to the whole canvas.
E	On-tile video controls	Use the on-tile video controls while viewing video in a tile.
F	Recording state	Recording state is the current recording status of a given camera. There are four possible recording states: <i>Enabled</i> , <i>Disabled</i> , <i>Currently recording (unlocked)</i> , and <i>Currently recording (locked)</i> . Green indicates that it is not recording. Red indicates that it is recording.
G	timeline	<p>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.</p> <p>Use the timeline to control playback video.</p>

Related Topics








[Customizing how tiles are displayed](#) on page 29

Tile menu commands

You can control your tiles and the entities displayed in tiles using commands in the tile menu.

Some commands always appear, and other contextual commands change depending on the entity type displayed in the tile. The following table lists the commands available from the tile menu:

Command	Description
Camera	Commands related to video surveillance.
 Protect video from deletion	Prevent the current video recording from being deleted due to the Archiver's disk space constraints. This command is only available when video content is displayed in the tile.
 Block	Prevent users from viewing the selected video stream. This command is only available when video content is displayed in the tile.
 Unblock	Allow users to view the selected video stream. This command is only available when video content is displayed in the tile.
 Select live stream	Select the camera's video stream to be displayed in the current tile. By default, the Live stream is displayed. This command is only available when live video is displayed in the tile and the video unit supports multiple streams.
 Select video playback source	Select which archiving source (Archiver or Auxiliary Archivers) to view the playback video from. For example, if you want to view a specific resolution, frame rate, or video stream, you can select the Archiver that is configured to record with those settings. By default, All sources is displayed. This command is only available when playback video is displayed in the tile.
 Commands	Select additional camera-specific commands, such as play audio clip, turn on white light, auto focus, and so on. These contextual camera command are currently supported on some Axis, Panasonic, and Bosch cameras.
 Monitoring	
Monitor alarms	Select to turn alarm monitoring on and off for the tile. A blue check mark indicates that alarm monitoring is turned on.
Monitor events	Select to turn event monitoring on and off for the tile. A blue check mark indicates that event monitoring is turned on.
 Investigate	Click to open an <i>Investigation</i> task based on the selected entity. That entity will already be selected in the report query filters.
 Report an incident	Create an incident report for something you see happening in the tile.
 Start incident recording	Start recording the video related to every entity that is placed in the tile (cameras, areas, doors, cardholders, and so on), to create a incident report package.

Command		Description
	Maximize tile	Expand the current tile to fill the canvas. Hides all other tiles.
	Maximize tile fullscreen	Hide the area view and dashboard, and make the current tile fill the canvas. Forces the tile to be displayed in full screen mode.
Navigate	 Back	Show previous tile content.
	 Forward	Show next tile content.
	 Home	Show initial tile content.
	 Refresh	Refresh tile content.
	Clear all	Empty all content from tiles.

Viewing entities in the canvas

You can view an entity in a canvas tile from the area view or the report pane.

What you should know

All entities listed in the area view and some entities and events in the report pane can be viewed in a canvas tile, with the exception of the System entity (🟢). Entities can also appear automatically in a tile when an event occurs.

If it is helpful for you, you can show more information next to the entities in the area view by customizing how entities are displayed.

To view an entity in the canvas:

- 1 From the area view or the report pane, do one of the following:
 - To view a single entity, double-click or drag the entity into a tile.
 - To view multiple entities, hold **CTRL** or **SHIFT**, select the entities, and drag them into a tile. This method only works if there enough free tiles.
- 2 To control the entities, right-click inside the tile and use the tile menu commands, or use the widgets in the dashboard.
- 3 To clear entities from the canvas, do one of the following:
 - Right-click on a tile, and then click **Clear all** (🗑️).
 - Select a tile, and then press the **BACKSPACE** key.
 - (Empties all tiles) At the bottom of the canvas, click **Clear all** (🗑️).
 - (Empties all tiles) Press **Ctrl+BACKSPACE**.

Related Topics

[Entity states](#) on page 394

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.

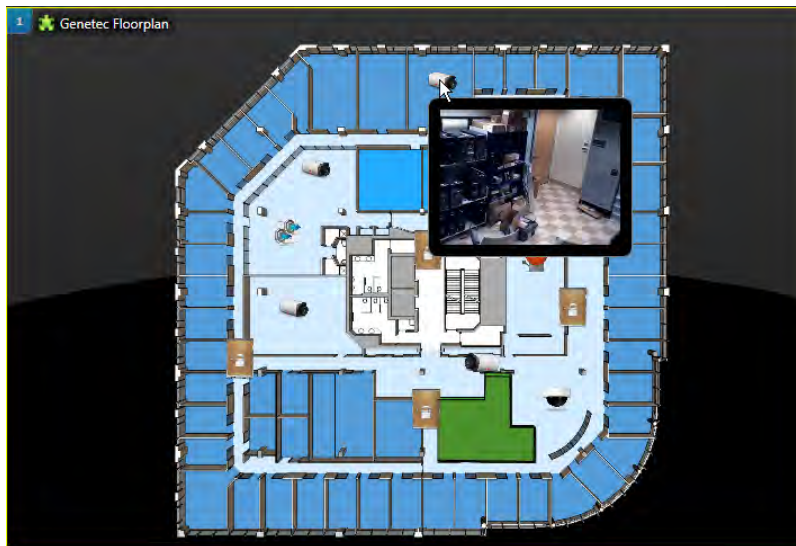
To customize how entities are displayed:

- 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**.

How maps are displayed in the Security Desk canvas

In Security Desk, maps are represented in a web page (🌐) or tile plugin (🧩). You can display maps in the canvas by dragging the web page or tile plugin into a tile.

Your map can contain interactive icons that represent the positions of cameras, doors, areas, and other entities around your site. Depending on the complexity of the map, you can view live video from cameras, change the lock state of doors, monitor zones, alarms, areas, and so on.




Unpacking content in tiles

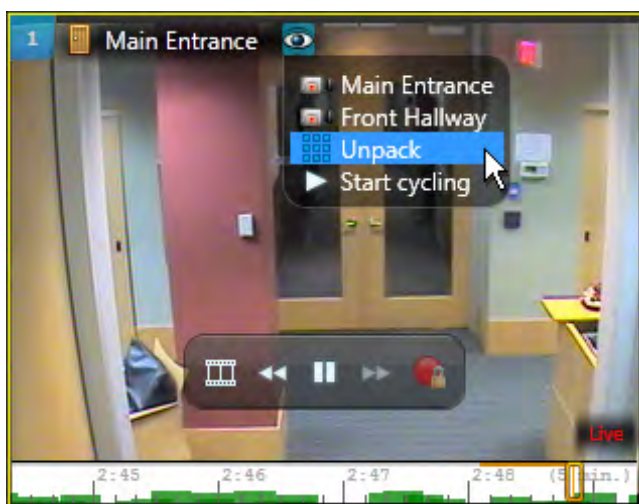
When an entity is displayed in a tile that has other entities associated with it, you can unpack the entity and view all the attached entities in separate tiles.

What you should know

Entities that have two or more entities attached to them are called *composite entities* (for example, a door that has multiple cameras associated to it). If you are monitoring the door and an event occurs at the door, only the first camera is displayed because the multiple cameras are *packed*. If you unpack the door, you can view all the cameras in separate tiles.


To unpack content in a tile:

- 1 Select a tile that is displaying a composite entity.
- 2 Beside the entity name in the tile toolbar, click .
- 3 From the drop-down menu, click one of the following:



- An attached camera (in the example, *Main Entrance* or *Front Hallway*).
- **Unpack:** View all entities attached to the selected entity in separate tiles.
- **Start cycling:** Rotate through the entities that are attached to the composite entity within the tile. The amount of time each entity is displayed can be configured from the *Options* dialog box.

NOTE: If there is a PTZ camera attached to the composite entity and you start controlling the PTZ, the cycling stops. You can click **Start cycling** again once you are done controlling the PTZ.

- 4 To repack the tiles when you have finished viewing what you need to see, click **Pack**  in the upper-left corner of the tile.

Example

The *Main Entrance* door has two cameras associated to it: the *Main Entrance* camera and the *Front Hallway* camera. An *Access denied* event occurs at the main door, and the event is displayed in a tile. Since the tile is packed, only the first camera is displayed (Main Entrance), until you unpack the tile content.

Customizing entity cycling options

You can select how many seconds Security Desk dwells on each entity when rotating through composite entities (such as an alarm, area, or a camera sequence) in a tile.

What you should know

This setting is saved as part of your user profile.

To customize entity cycling options:

- 1 From the home page, click **Options > General**.
- 2 In the **Dwell time** section, set the **Entity cycling** value.
- 3 Click **Save**.

Maximizing the canvas to full screen

When Security Desk is in full screen mode, you can hide the area view, taskbar, and dashboard so only the *canvas* and the video streams you are monitoring are shown, or you can maximize one tile to focus on a particular video image.

What you should know

The full screen video mode looks similar to an analog monitor. If Security Desk is connected to multiple monitors and you switch the canvas to full screen mode, each monitor displays a separate canvas. You can select which monitors switch to full screen mode from the *Options* dialog box.

To maximize the canvas to full screen mode:

- 1 Do one of the following:
 - To maximize the canvas, press **F11 > F10**.
Everything is hidden except for the canvas tiles.
 - To maximize one tile, press **Alt+ENTER**.
- 2 Use your keyboard shortcuts to control the video streams.
- 3 To show the taskbar, hover your mouse at the top of the Security Desk window.
- 4 To exit full screen mode, do one of the following:
 - If your canvas is maximized, press **F11 > F10**.
 - If one tile is maximized, press **Alt+ENTER**.

Related Topics

[Default keyboard shortcuts](#) on page 113

Selecting which monitors can switch to full screen

If Security Desk is connected to multiple monitors, you can choose which monitors are able to switch to full screen mode, from the *Options* dialog box.

What you should know

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

To select which monitors can switch to full screen:

- 1 From the home page, click **Options > General**.
- 2 In the **Full screen monitors** section, select which monitors can switch to full screen.
This section only appears if Security Desk is connected to more than one monitor.
- 3 Click **Save**.


Changing tile patterns

You can change the tile pattern of the canvas.

What you should know

The default tile pattern in the canvas displays four viewing tiles in a 2x2 formation.

To change the tile pattern:

- 1 At the bottom of the canvas, click **Change tile pattern** ().
- 2 Do one of the following:
 - Select one of the displayed tile patterns.
These patterns are either the default ones, or patterns that you have set as favorites.
 - Click **More**, and select one of the additional tile patterns.
They range between 1 large tile to 64 small tiles.

Related Topics

[Editing and creating tile patterns](#) on page 28

Editing and creating tile patterns






To customize your workspace, you can modify the 26 tile patterns that are available in the canvas, delete default patterns, and create new tile patterns.

What you should know

The tile pattern editor in Security Desk only allows you to create patterns that are a maximum of 8x8 files.

Tile pattern settings are saved as part of the workstation. You require the *Edit tile patterns* user privilege to edit and create tile patterns.

To edit or create a tile pattern:

- 1 At the bottom of the canvas, click **Change tile pattern** .
- 2 Click **More > Edit patterns**.
- 3 Do one of the following:
 - Select an existing pattern.
 - To create a new tile pattern, click .
- 4 In the **Name** field, type a name for the pattern.
- 5 In the **Category** field, select which group to place the pattern in.
- 6 To display the pattern in the main dialog box when you click **Change tile pattern** , select **Display as favorite** .
- 7 To change the number of rows and columns, use the **Rows** and **Columns** selector, or click the lines in the graph.
- 8 To delete a pattern, select the pattern, and click .
- 9 To revert all the tile patterns to their default configuration, click **Revert to default**.

IMPORTANT: All patterns that are not default patterns are deleted.

- 10 Click **Save and close**.

Customizing how tiles are displayed

You can customize what to show in the canvas tiles depending on how you use them, from the *Options* dialog box.



What you should know

The parts of a tile that can be hidden are the timeline, on-tile video controls, tile toolbar, and *tile ID*. The tile settings are saved as part of your user profile.

To customize how tiles are displayed:

- 1 From the home page, click **Options > Visual**.
- 2 From the **Display timeline** drop-down list, select when to show the timeline in tiles, in live and in playback:
 - **Auto-hide**: Only show the timeline when the mouse cursor hovers inside the tile boundaries.
 - **Always**: Always show the timeline.
 - **Never**: Never show the timeline.
- 3 To show the on-tile video controls when you hover your mouse cursor inside a tile (play, pause, and so on), select the **Display overlay video controls** option.
- 4 To show an entity's full path with the entity name in the tile toolbar, select the **Display entity names with their full path** option.

An entity's path is the hierarchy of *areas* above that entity in the area view. When the path is too long, an "*" is displayed instead.

Example: " Montreal office/Main entrance", or " */*/Back entrance".

- 5 To show the tile toolbar only when you hover your mouse cursor inside a tile, select the **Auto-hide tile toolbar** option.

When this option is cleared, the tile toolbar is always displayed.

- 6 To show the tile ID number only when you hover your mouse cursor over inside the tile, select the **Auto-hide tile number** option.

When this option is cleared, the tile ID is always displayed.

- 7 Click **Save**.

Related Topics

[On-tile video controls](#) on page 129

[About tiles](#) on page 18

Widgets

This section includes the following topics:

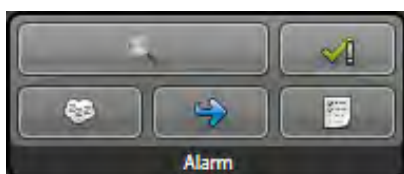
- ["Alarm widget"](#) on page 31
- ["Area widget"](#) on page 33
- ["Camera widget"](#) on page 34
- ["Door widget"](#) on page 37
- ["Intrusion detection area widget"](#) on page 38
- ["PTZ widget"](#) on page 39
- ["Tile widget"](#) on page 41
- ["Zone widget"](#) on page 43

Alarm widget

The *Alarm* widget appears whenever an alarm entity is displayed in the current tile. It offers you different ways to respond to an alarm.





If an alarm is triggered that requires an acknowledgement condition (for example, *Door closed*), the *Investigate* button appears in the alarm widget when that alarm entity is displayed in the current tile and the acknowledgement condition is not yet cleared.



The commands in the alarm widget are available in the [Monitoring](#), [Alarm monitoring](#), and [Alarm report](#) tasks.

The alarm widget commands are described below:

Button	Command	Description
	Acknowledge (Default) ¹	Acknowledge the alarm. The alarm is no longer active, and is removed from the canvas and the alarm list.
	Acknowledge (Alternate) ¹	Set the alarm to the <i>alternate</i> acknowledged state. The reasons for using this acknowledgement type are defined by your company. For example, if a false alarm is triggered, you can acknowledge the alarm this way. This state can be used as a filter in alarm queries.
	Forcibly acknowledge ¹	Force the alarm to be acknowledged. This is helpful for clearing alarms that are currently under investigation and their acknowledgement condition is not yet cleared. You can only force acknowledge an alarm if you are logged on as an administrator.
	Investigate	Investigate the alarm. This button is only available if an alarm is triggered that has an acknowledgement condition attached to it, and the condition is not yet cleared. This lets other users in the system know that you have seen the alarm.
	Snooze alarm ¹	Put the alarm to sleep for 30 seconds. When the alarm is snoozing, it is temporarily removed from the canvas. You can change the default snooze time from the Options dialog box.

Button	Command	Description
	Forward alarm ¹	Forward the alarm to another user in the system. Before forwarding the alarm, you must select a user, and you can also type a message.
	Show alarm procedure	Show the alarm's specific procedure (if one is defined by the administrator). Alarm procedures are simple to create and can take the form of HTML pages or a web application developed by the end user.

¹ If you hold **CTRL + SHIFT** when clicking the command, that command applies to all alarms displayed in the canvas.

Related Topics

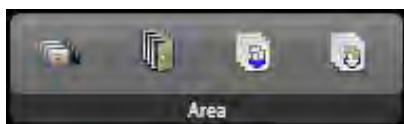
[Forwarding alarms to other users automatically](#) on page 357

[Customizing alarm behavior](#) on page 363

[Overview of the Alarm report task](#) on page 485





Area widget

The *Area* widget appears when the current tile is showing an area.



The commands included in the area widget are *recursive*, meaning that they apply to all the entities that are members of the selected area. Click on one of the commands to view a menu of commands you can pick from.

The area widget commands are described below:

Button	Command	Description
	Cameras	Apply commands to all cameras that are members of the area: <ul style="list-style-type: none"> • Start recording : Start recording on the cameras. • Stop recording: Stop recording on the cameras. • Add bookmark: Add a bookmark to the cameras. • Block: Prevent users from viewing the video streams. • Unblock (recursive): Allow users to view the video streams.
	Doors	Apply commands to all doors that are members of the area: <ul style="list-style-type: none"> • Override unlock schedules : Lockdown the doors that might be on an unlock schedule. • Cancel override: Put the doors back on their unlock schedules.
	Zones	Apply commands to all zones that are members of the area: <ul style="list-style-type: none"> • Arm: Arm the zones. • Disarm: Disarm the zones.
	Intrusion detection areas	Apply commands to all intrusion detection areas that are members of the area: <ul style="list-style-type: none"> • Disarm: Tell the intrusion panel to ignore all sensors attributed to the selected intrusion detection area. • Perimeter arm: Arm the intrusion detection areas so that only sensors attributed to the area perimeter set off the alarm if triggered. • Master arm: Arm the intrusion detection areas so that all sensors attributed to the area set off the alarm if triggered. • Trigger intrusion alarm: Trigger an intrusion alarm on the intrusion detection areas.

Camera widget







The *Camera* widget appears in the dashboard when the currently selected tile is displaying a camera.















The buttons displayed in the camera widget change depending on the task you are performing, and the camera type. For example, if the camera displayed in the tile is streaming live video, you find one set of buttons. If the camera displayed in the tile is playing back a recording, some of the buttons change. If the camera supports audio, the audio buttons appear, otherwise, they are grayed out.














The following two images show the camera widget when live video with no audio is selected in a tile, and when playback video with audio selected in a tile.



The camera widget commands are described below:

Button	Command	Description
	Jump backward ¹	Jump backward. Each click of this button forces the recording playback to jump backwards by 15 seconds. You can configure this value from the Options dialog box.
	Rewind ¹	Reverse the playback. Each click of this button adjusts the reverse playback speed from -1x to -2x, -4x, -6x, -8x, -10x, -20x, -40x, -100x. Click the Play button to revert playback to 1x (normal speed) in the forward direction.
	Previous frame ¹	Reverse the video by one frame. You can also use the jog wheel to achieve the same result. This button is only available when the video is paused.
	Pause ¹	Pause the playback at the current frame.
	Play ¹	Play back the recording at normal speed (1x).
	Next frame ¹	Advance the video by one frame. You can also use the jog wheel to achieve the same result. This button is only available when the video is paused.

Button	Command	Description
	Forward¹	Fast forward the playback. Each click of this button increases the playback speed from 1x to 2x, 4x, 6x, 8x, 10x, 20x, 40x, 100x. Click the Play button to revert playback to normal speed (1x).
	Jump forward¹	Jump forward. Each click of this button forces the recording playback to jump forward by 15 seconds. You can configure this value from the Options dialog box.
	Switch to live¹	Switch the displayed images from playback to live video.
	Recording on	(Solid red) The camera is currently recording. Click to stop recording.
	Recording on	(Blinking red) The camera is currently recording, but almost at the end of its manual recording duration (30 seconds remaining). Click to reset timer for another five minutes.
	Recording on (locked by system)	The camera is currently recording, and is controlled by a system configuration. You cannot click to stop recording.
	Recording off	The camera is not currently recording. Click to start recording. The recording stops automatically after five minutes. You can also stop the recording manually.
	Recording off (locked by system)	The camera is not currently recording, and is controlled by a system configuration. You cannot click to start recording.
	Slow motion¹	Switch between normal playback speed (1x) and slow motion (1/8x). While in slow motion mode, click the Forward or Rewind button to change the playback speed from 1/8x to 1/4x, 1/3x, 1/2x, in either direction.
	Loop playback	Create a looped playback. When you click this button, two timeline markers (📌) appear at either end of the timeline. Click and drag the markers over the timeline to indicate the start and end points of the looped playback.
	Speed slider	Drag the slider to the right to accelerate playback to 2x, 4x, 6x, 8x, 10x, 20x, 40x, 100x. Drag the slider to the left to force reverse playback at -2x, -4x, -6x, -8x, -10x, -20x, -40x, -100x speeds.
	Speed slider (limited)	Same as the speed slider above except that reverse playback is limited to: -10x, -20x, -40x, -100x. The limited speed slider is used on federated Omnicast 4.x cameras that do not support all rewind speeds.
	Jog wheel	Replaces the speed slider when the video is paused. Use it for frame by frame playback both forwards and backwards.
	Go to specific time¹	Open a browser window, and jump to a precise date and time in the recording.

Button	Command	Description
	Toggle digital zoom	Apply a 2x digital zoom to the image. Further digital zoom adjustments can then be performed within the tile.
	Enable visual tracking¹	Follow an individual or object that is moving across different cameras from the same tile.
	Export video¹	Create stand-alone video files that can be played without being connected to the Security Center Directory.
	Save a snapshot¹	Save the current video frame as an image file.
	Previous bookmark¹	Jump to the previous bookmark.
	Add a bookmark¹	Add a bookmark to the video.
	Next bookmark¹	Jump to the next bookmark.
	Listen¹	Enable the speaker. This button is only available when the camera supports audio.
	Stop listening¹	Disable the speaker. This button is only available when the camera supports audio.
	Talk¹	Enable the microphone. This button is only available when the camera supports audio.
	Stop talking	Disable the microphone. This button is only available when the camera supports audio.
	Show stream properties	Display the properties of the selected video stream.
	Digital zoom presets	When digital zoom is applied to the selected tile, click this button to add a digital zoom preset for the current camera image position.

¹ If you hold CTRL + SHIFT when clicking the command, the command applies to all cameras displayed in the canvas.

Related Topics

[Video options](#) on page 203

[Switching between video modes](#) on page 157

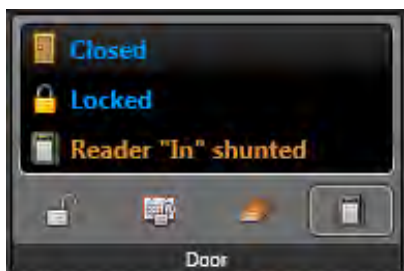
[Zooming in and out of video](#) on page 139

[Adding bookmarks to video sequences](#) on page 143






[Taking snapshots of video](#) on page 146

Door widget

The *Door* widget appears whenever a door entity is displayed in the current tile. It allows you to control the access through that door. The door widget also displays the current door status (closed or opened), the lock status (locked or unlocked), and the readers' status (if they are shunted).



The door widget commands are described below:

Button	Command	Description
	Unlock¹	Temporarily unlock the door for 5 seconds (or whatever the duration of the <i>Standard grant time</i> is, as configured by the system administrator).
	Override unlock schedules	Unlock the door indefinitely for maintenance purposes, or keep the door locked/ unlocked for a predetermined period of time.
	Cancel	Cancel the unlock schedule override.
	Forgive antipassback violation	Forgive an antipassback violation. This button is only available when there is an antipassback violation.
	Reader (Shunt or Activate)	Select the reader to either Shunt (deactivate) or Activate. This button is only available when your access control equipment supports reader shunting.

¹ If you hold CTRL + SHIFT when clicking the command, the command applies to all doors displayed in the canvas.

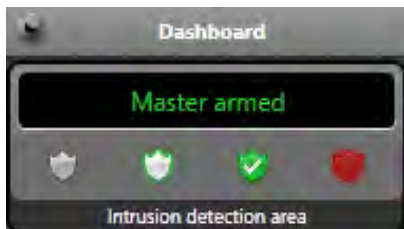
Related Topics

[Allowing access through doors](#) on page 274





[How doors are displayed in the Security Desk canvas](#) on page 273

Intrusion detection area widget

The *Intrusion detection area* widget appears only when the current tile is showing an intrusion detection area.



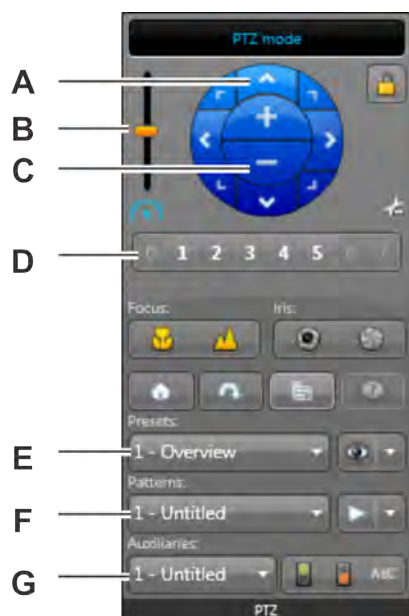
The intrusion detection area widget commands are described in the below table:

Button	Command	Description
	Disarm	Tell the intrusion panel to ignore all sensors attributed to the selected intrusion detection area. If an alarm is set off by this area, disarming it also turns the alarm off.
	Perimeter arm	Arm the selected intrusion detection area so that only sensors attributed to the area perimeter set off the alarm if triggered. Other sensors, such as motion sensors inside the area, are ignored.
	Master arm	Arm the selected intrusion detection area so that all sensors attributed to the area set off the alarm if triggered. Some manufacturers call this arming mode "Away arming".
	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 intrusion alarm input.














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.

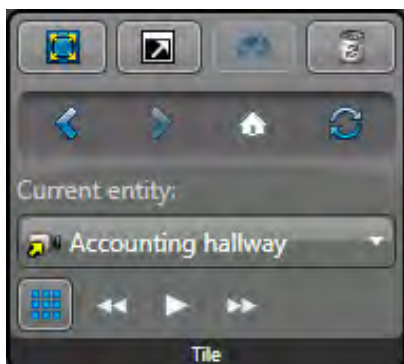


Button/ Letter	Command	Description
A	Direction arrows	Pan the PTZ motor using the eight direction arrows.
B	Speed slider	Adjust the speed of the PTZ motor.
C	Zoom in/out	Zoom in and out using the plus (+) and minus (-) commands.
D	Quick access buttons	Move the PTZ motor to one of the eight quick access 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), 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.

Button/ Letter	Command	Description
	Toggle to advanced mode	Open the PTZ Advanced mode menu.
	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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.

Tile widget

The *Tile* widget controls the properties of the current tile. It is always shown in the dashboard.



The tile widget commands are described below. The same commands appear in the tile menu.

Button	Command	Description
	Maximize tile	Expand the current tile to fill the canvas. Hides all other tiles.
	Maximize tile fullscreen	Hide the area view and dashboard, and make the current tile fill the canvas. Forces the tile to be displayed in full screen mode.
	Monitoring¹	Start alarm or event monitoring in a tile.
	Clear all¹	Empty all content from tiles.
	Back	Show previous tile content.
	Forward	Show next tile content.
	Home	Show initial tile content.
	Refresh	Refresh tile content.
n/a	Current entity	Select which entity to view from the selected composite entity. For example, select a camera attached to the selected area.
	Unpack	View all entities attached to the selected entity in separate tiles.
	Pack	Pack all the attached entities.
	Go to previous content in cycle¹	Switch to the previous entity attached to the composite entity.
	Start cycling¹	Rotate through the entities that are attached to the composite entity within the tile.
	Stop cycling¹	Stop the entity cycling rotation.
	Go to next content in cycle¹	Switch to the next entity attached to the composite entity.

¹ If you hold **CTRL + SHIFT** when clicking the command, that command applies to all tiles displayed in the canvas.

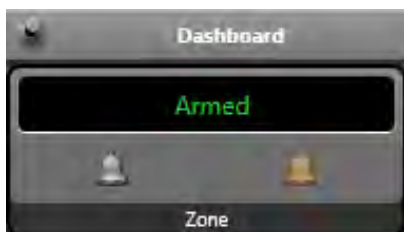
Related Topics

[Selecting entities to monitor](#) on page 65



[Unpacking content in tiles](#) on page 24

Zone widget

The *Zone* widget only appears when the current tile is showing a zone.



The zone widget commands are described below:

Button	Command	Description
	Disarm ¹	Disarm the selected zone (inputs deactivated).
	Arm ¹	Arm the selected zone (inputs activated).

¹ If you hold CTRL + SHIFT when clicking the command, the command applies to all zones displayed in the canvas.

Tasks

This section includes the following topics:

- ["Opening tasks"](#) on page 45
- ["Saving tasks"](#) on page 46
- ["Adding tasks to your Favorites list"](#) on page 47
- ["Sending tasks to other users"](#) on page 48
- ["Closing tasks using a system action"](#) on page 50
- ["Customizing task behaviour"](#) on page 51

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.

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**.

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've selected specific entities to monitor and you want to share the task with someone else. Or, perhaps you've 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.

Sending tasks using a manual action

You can send tasks to another workstation using a manual action.


What you should know

This method of sending tasks is especially useful for sending monitoring tasks to a video wall. By default, workstations receiving the tasks will display a confirmation window to ask their users if they accept them or not. You can avoid the display of the confirmation window on a video wall by disabling the Ask for confirmation when opening tasks sent by other users option on the receiving workstation.

Consider the following when sending tasks using a manual action:

- Only saved *public tasks* can be sent.
- The action is performed immediately.

To send a task using a manual action:

- 1 In the notification tray, click **Hot actions** .
- 2 In the **Hot actions** dialog box, click **Manual action**.
 The Configure an action window opens.
- 3 In the list of actions, click **Send task**.
- 4 From the **Task** drop-down list, select the saved public task that you want to send.
- 5 Select whether to send the task to a user (**User**) or a workstation (**Monitor**).

6 In the **Select destination** list, select the user or the monitor where you want the task to be sent.

TIP: When selecting a monitor (workstation) as a destination, you might see red and white entries in your monitor list. Monitors that appear red are currently disconnected. Monitors that appear white are currently connected.

7 (Optional) If you are sending the task to a user, write a message in the **Message** field.

8 Click **OK**.

The task is immediately sent to the remote workstation. A confirmation message appears on your workstation and a confirmation request is displayed on the receiving workstation when the Ask for confirmation when opening tasks sent by other users option is enabled.

Closing tasks using a system action

You can remove tasks from another workstation using a manual *action*.

What you should know

You cannot remove individual tasks from a remote workstation. The **Clear tasks** command removes all open tasks.

To close a task using a system action:

- 1 In the notification tray, click **Hot actions** (🔊).
- 2 In the **Hot actions** dialog box, click **Manual action**.
- 3 In the list of actions, click **Clear tasks**.
- 4 From the drop-down list, select the saved public task that you want to send.
- 5 Select whether to send the task to a user (**User**) or a workstation (**Monitor**).
- 6 In the **Select destination** list, select the user or the monitor where you want the tasks to be removed.
- 7 Click **OK**.

All open tasks are immediately removed from the remote monitor. A confirmation message is produced on the sender's workstation.

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. However, the **Task cycling** and **Ask for confirmation when opening tasks sent by other users** options are saved as local setting for your Windows user profile.

To customize task behavior:

- 1 From the home page, click **Options > General**.
- 2 To set the amount of time Security Desk dwells on each task when cycling through the open tasks, set the **Task cycling** value.
NOTE: *Task cycling* can be turned on by right-clicking anywhere in the taskbar.
- 3 Click the **User interaction** tab.
- 4 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.
- 5 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.
- 6 Click **Save**.

Reports

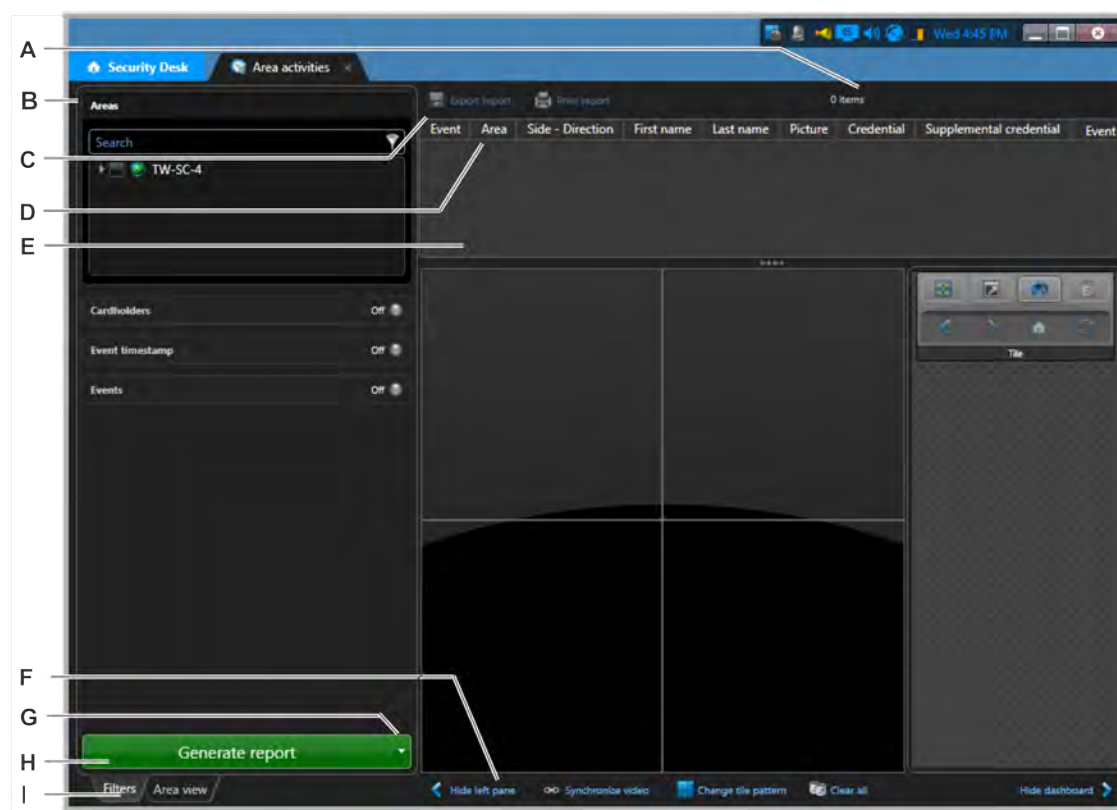
This section includes the following topics:

- ["Reporting task workspace overview"](#) on page 53
- ["Generating reports"](#) on page 55
- ["Generating and saving reports"](#) on page 59
- ["Customizing the report pane"](#) on page 61
- ["Customizing report behavior"](#) on page 62

Reporting task workspace overview

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.

This section takes you on a tour of the reporting task layout, and describes the common elements of most reporting tasks. The Area activities task was used as an example. You can open the Area activities 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 <i>Filters</i> tab to set up your query. Click on a filter heading to turn it on (🟢) or off. Invalid filters display as <i>Warning</i> or <i>Error</i> . 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 in the report pane. |

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 (such as launching another report related that report result).
F	Tile commands	Commands related to canvas tiles: <ul style="list-style-type: none">• Synchronize video: Synchronize the video that is displayed in the canvas.• Clear all: Empty all content from tiles.• Change tile pattern: Change the tile pattern in the canvas.
G	Generate and save report	Click to run and save the report directly to a file (PDF, CSV, or Excel format). This button is disabled if you have not selected any query filters, or when you have invalid filters.
H	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, the button changes to <i>Cancel</i> . Click on <i>Cancel</i> to interrupt the query.
I	Filters tab	Use the Filters tab to customize and filter your searches. The Filters tab only appears in reporting tasks. NOTE: Click the Area view tab to show the area view, and select entities to view in the canvas.

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.

Selecting date and time ranges for reports

You can specify a date time range to filter your report queries.

What you should know

You can choose between a relative date or a specific date:

- **During the last:** Time range using the last number of seconds, minutes, hours, days, weeks, months, or years. The report results will be different every time, since the time range is based on the current time.
- **Specific date:** A From and To date and time range. The same report results will be produced every time you run the query.

If the time range is invalid, an error (🚫) icon appears, and you cannot generate the report. When the time range covers multiple days, a warning (⚠️) icon appears on the filter, informing you the report might take longer to generate.

IMPORTANT: If you have a larger system that includes devices operating in different time zones, your time range filters are affected.

To select and date and time range for a report:

- 1 Open an existing reporting task, or create a new one.
- 2 In the **Triggered on** section, select a time range mode.
Depending on the reporting task you are using, this filter might be called **Time range** or **Event timestamp**.
- 3 If you select **During the last** time range mode, select the number of seconds, minutes, hours, days, weeks, months, or years.
- 4 If you select **Specific date** time range mode, do one of the following:
 - Edit the **From** and **To** date and time fields.
 - Leave the time as **all day**, or choose a specific time.
 - To pick a date, click the arrow, and then choose a date in the calendar.
 - To zoom out and view a whole year, twelve years, or twelve decades, click the calendar heading.
 - To zoom in, click on the desired decade, year, or month.
 - To pick a time, click the **all day** link, then enter the time directly in the time fields.
 - To set the date and time to the current time on your computer, press **Ctrl+Alt+N**.

Related Topics

[Customizing time zone settings](#) on page 57

[Opening tasks](#) on page 45

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.

Generating and saving reports using a system action

You can generate and save a report using a manual action.

Before you begin

- Save the task that you want to generate and export as a *public task*, with the query filters that you want applied, and the report columns you want to include.
- Set the maximum number of report results that can be saved in PDF or Excel format, and the destination folder from the Report Manager *Properties* tab. For more information, see the *Security Center Administrator Guide*.

To generate and save a report using a system action:

- 1 In the notification tray, click **Hot actions** (🔊).
- 2 In the **Hot actions** dialog box, click **Manual action**.
- 3 In the list of actions, click **Export report**.
- 4 From the **Report** drop-down list, select the saved public task that you want to export.
- 5 From the **File format** drop-down list, select PDF, Excel, or CSV.
- 6 (PDF only) From the **Orientation** drop-down list, select whether the PDF file should be in portrait or landscape mode.
- 7 If you want to overwrite a report that was previously exported to the destination folder, then select the **Overwrite existing file** option.
- 8 Click **OK**.

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 57

[Saving tasks](#) on page 46

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**.

Basic tasks

This section includes the following topics:

- ["Monitoring events"](#) on page 64
- ["Event occurrence period"](#) on page 68
- ["Searching for entities"](#) on page 69
- ["Triggering hot actions"](#) on page 71
- ["Triggering one-time actions"](#) on page 72
- ["Configuring the notification tray"](#) on page 73
- ["Moving the taskbar"](#) on page 76
- ["Remote monitoring"](#) on page 77
- ["Connecting to remote Security Desks"](#) on page 78
- ["Monitoring events on remote Security Desks"](#) on page 80
- ["Monitoring alarms on remote Security Desks"](#) on page 81
- ["Actions you can perform on remote Security Desks"](#) on page 82


Monitoring events

Using the Monitoring task, you can monitor *events* such as access control events from doors and cardholders, license plate reads and hits from fixed and mobile LPR units, and camera related events, in real time.


What you should know

When monitoring events, you are actually monitoring the entities that trigger those events. The entities are selected in the Monitoring task. You can customize how the Monitoring task displays information to suit the purpose of the task. For example, if you are monitoring cameras, you can hide everything else except for the canvas tiles to make the camera images bigger. You can create multiple Monitoring tasks to monitor different sets of entities (for example, just cameras or doors).

To monitor events:

- 1 [Select the events to monitor.](#)
- 2 [Select the entities](#) that are linked to the events you want to monitor.
Once the entities are selected, events that occur in your system appear chronologically in the event list and in real time. You cannot change the order of the events.
- 3 To show the event list, from the top of the Monitoring task window, drag the four gray dots downwards.
- 4 To choose what event information to display in the event list, right-click on a column heading, and then click **Select columns** to choose the information you want to display in the list.
Example: In access control systems, you might only want to view cardholder and credential fields. In LPR systems, you might only want to view plate numbers and context images.
- 5 To clear the event list, click **Clear event list**  in the upper-right corner of the Monitoring task.
- 6 To monitor events in the canvas, choose one of the following two modes:
 - **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. In this mode, you can turn monitoring on or off for each tile.
 - **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. You can view LPR events in the map.
- 7 From the area view, select the entities you want to view in the canvas by dragging them into the canvas. You can select multiple entities and drag them onto the canvas all at once.
- 8 (Optional) To protect the content in the tile from being overwritten by new events, turn off monitoring for that tile as follows:

TIP: This is helpful if you have a tile plugin displayed in the canvas, and do not want it to be replaced by an event.

 - a) Select a tile in the canvas.
 - b) In the tile widget, click **Monitoring** , and click **Monitor events**.

The checkmark beside **Monitor events** disappears and tile ID background turns black.

Related Topics

[Monitoring LPR events in tile mode](#) on page 298

[Monitoring LPR events in map mode](#) on page 300

Selecting events to monitor

Before you can use the Monitoring task, you must select the event types you want to monitor.

To select events to monitor:

- 1 From the home page, click **Options > Events**.
- 2 In the **Event options** page, select which events to monitor.
- 3 In the **Display in tile** column, select the check boxes of the events you want to view in the Monitoring task canvas. If the check box is cleared, the event only appears in the event list.
- 4 Click **Save**.

After you finish

[Select the entities you want to monitor](#) that trigger the event types you selected.

Related Topics

[Event types](#) on page 427

Selecting entities to monitor

Before you can monitor events in the Monitoring task, you must select the entities that trigger those events.

Before you begin

[Select the events to monitor](#).

What you should know

To monitor events, it is important to select which entities you want to monitor, because some event types can be generated by multiple entities. For example, an *Access granted* event can be generated by a cardholder, visitor, or credential. If you only monitor cardholders, you will not receive all Access granted events.

To select entities to monitor:

- 1 From the home page, click **Tasks > Monitoring**.
- 2 (Optional) To give the tab a unique name, right-click the tab, click **Rename task**; in the **Task name** box, type a name, then click **Rename**.


Example: You can rename the tab to indicate what is being monitored; for example, *Monitoring camera events*. This is helpful when you have multiple monitoring tabs open at the same time.

- 3 In the area view, select the entities you want to monitor (specific cameras, doors, cardholder, Patrollers, fixed AutoVu Sharp cameras, hotlists, and so on).



To select multiple entities, hold **CTRL** or **SHIFT**, and then select the entities.

- 4 Drag the selected entities over the **Monitoring**  icon at the bottom of the Monitoring task.

The entities you selected are added to the **Event monitoring** list.

NOTE: By default, all tiles are armed to monitor events. You can arm and disarm all tiles at any time by clicking . When a tile is armed to monitor events the tile ID background is blue.

5 (Optional) To add more entities from the *Event monitoring* dialog box, do the following:

- a) Click **Monitoring** () , and then under **Event monitoring** click **Add** ().
- b) Select the entity type you want to monitor (area view, cardholder, cardholder group, visitor, hotlist, permit, user, asset, and so on).

TIP: Certain entity types, such as areas, doors, elevators, zones, and so on, only appear in the *area view* drop-down list.

- c) Select the entities you want to monitor (specific cameras, doors, cardholder, Patrollers, fixed AutoVu Sharp cameras, hotlists, and so on).
- d) To add a conditional filter, select an entity from the **For** drop-down list.

Example: You can monitor events for a cardholder group at a specific door.

NOTE: Only events that are related to the cardholder group *and* the door are monitored. You will not receive other events for the door unless you are also monitoring that door.

- e) Click **Add**.

6 (Optional) In the *Tile* column of the **Event monitoring** list, select a tile to display the entity in.

You can associate more than one entity to the same tile. By default, events are displayed in any tile (All).

Example: You can set Tile 1 to display events happening at the *Main Entrance* door.

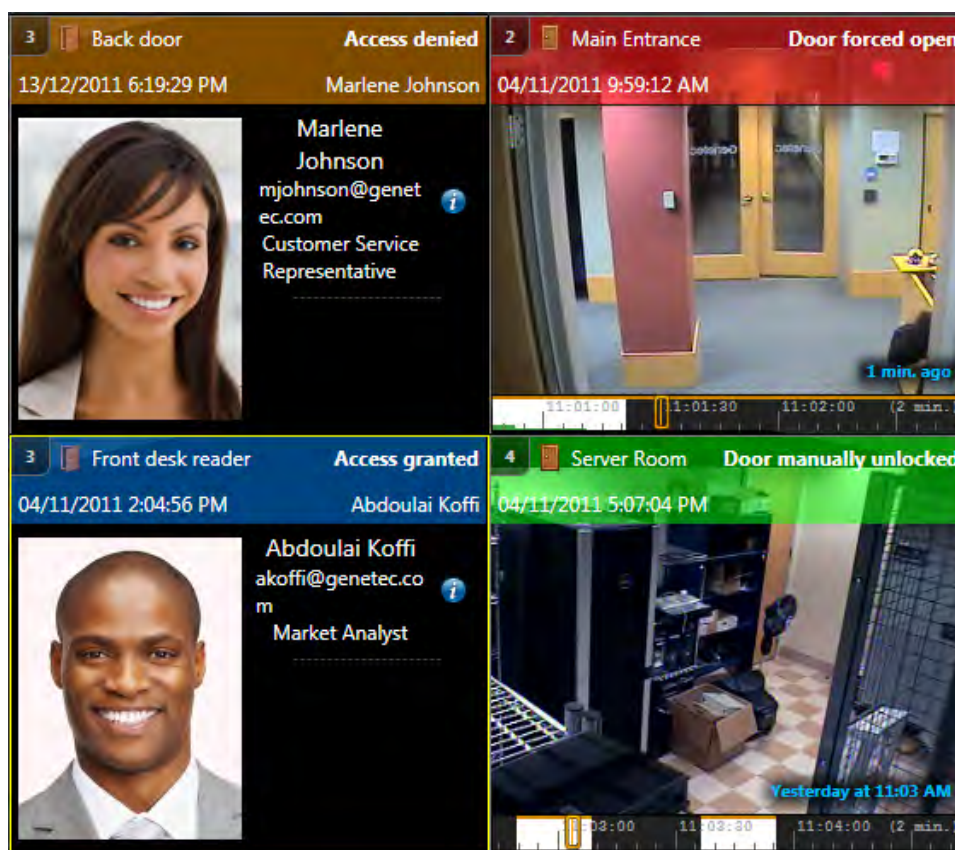
Monitoring is turned on in the canvas tiles. When a new event occurs, Security Desk displays the event in an empty tile. When there are no more empty tiles, the entity that has been displayed for the longest time is replaced by the new event.

Event colors

When you are monitoring entities, events generated by the entity are displayed in the canvas using different colors, depending on the event type. When you have a large system, this helps you focus on the events that are more important.

Event colors are configured in Config Tool. For more information about assigning colors for events, see the *Security Center Administrator Guide*.

The following figure shows four access control event that have been assigned different colors.



Customizing Monitoring task options

You can customize how many events are retrieved from the database and displayed when you load a saved Monitoring task.

What you should know

These settings are saved as part of your user profile.

To customize Monitoring task options:

- 1 From the home page, click **Options > Performance**.
- 2 In the **Show events that occurred during the last** option, select how many days worth of events you want to load.
- 3 In the **Maximum number of events to show** option, select the maximum number of events to load.
- 4 Click **Save**.

Event occurrence period

The event occurrence period applies to access control units and intrusion detection units that were temporarily offline. If a unit is offline in Security Center, but still *physically* running, when the unit is re-connected the events that were stored on the unit while it was offline are received in Security Desk. The occurrence period value indicates how long ago the event occurred before the unit came back online, and determines what happens when the event is received.

Only certain types of units (for example, HID VertX units) keep a record of events that occur while it is offline.

The four event occurrence values are listed below, with a description of what happens when Security Center receives the event:

- **Online:** The event occurred when the unit was online.
- **Grace period:** The event occurred less than 15 minutes before the unit came back online. Security Center treats the event as a normal event. It appears in the event list in the Monitoring task. Actions that are associated with the event using event-to-actions are triggered.
- **Alarm grace period:** The event occurred in between 16 minutes and 72 hours before the unit came back online. When the event is received in Security Center, it does not appear in the event list in the Monitoring task. The only actions that are triggered using event-to-actions are *Trigger alarm* and *Add bookmark*. The event is recorded in the database and is available for reporting.
- **Pre-alarm offline period:** The event occurred more than 72 hours before the unit came back online. When the event is received in Security Center, it is only recorded in the database for reporting.

Reasons why units can be offline

An access control or intrusion detection unit can be offline in Security Center for the following reasons:

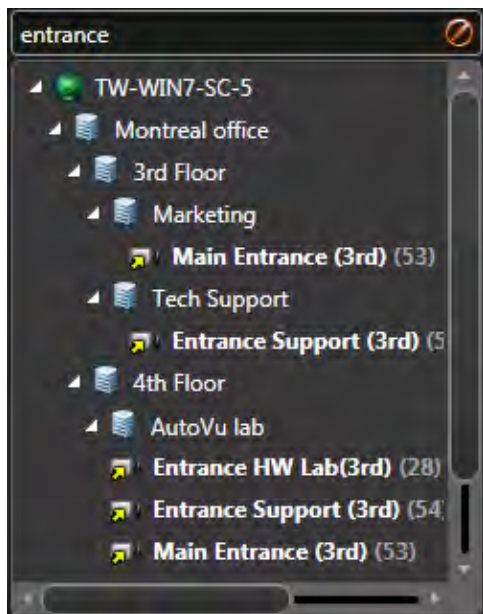
- The unit is rebooting.
- The unit's firmware is being upgraded.
- The connection between the unit and the *Access Manager* or *Intrusion Manager* is lost.
- The connection between the Access Manager or the Intrusion Manager and the *Directory* is lost. When this happens, the role disconnects from its units until the connection with the Directory is re-established.

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** (🔍).



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

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

Related Topics

[Entity states](#) on page 394

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.

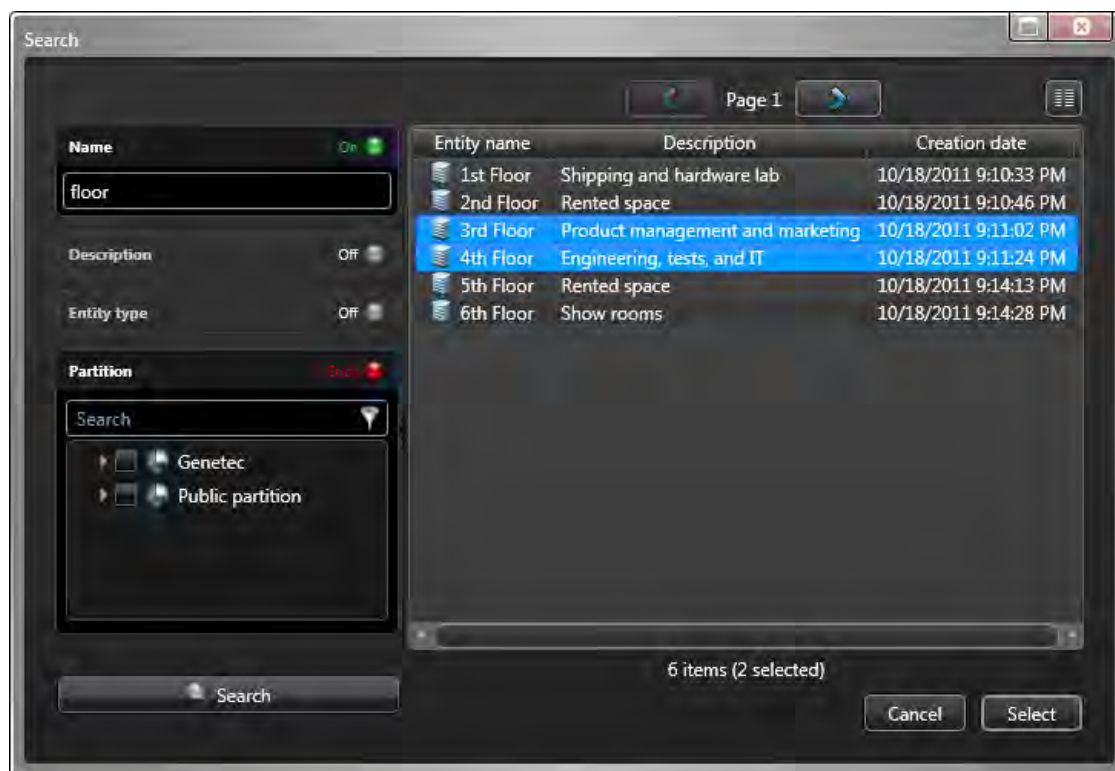
NOTE: Invalid filters are shown in red. Hover your mouse cursor over the heading to see why the filter is invalid.

- 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.



- 6 Click **Select**.

Only the entities you selected appear in the selector.

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

Triggering hot actions



You can trigger a hot action using the function keys on your keyboard, or from the notification tray.

What you should know







A hot action is an *action* that is mapped to a computer keyboard function key. You can trigger a hot action in Security Desk by pressing **Ctrl+ function key** (for example, **Ctrl+F1** triggers the first hot action in the list), or from the notification tray.

NOTE: Mapping a hot action to a function key is specific to your user account.

To trigger a hot action:

- 1 In the notification tray, click **Hot actions** .
- 2 In the **Hot actions** dialog box, click **Edit**.
- 3 To create a hot action, click **Add** .
- 4 In the *Configure an action* window, select an action type, and specify the additional settings required for the action.
- 5 Enter a **Description** that will appear in the hot actions list.
- 6 Click **OK**.

The hot action is created, and the **Hot actions** dialog box closes.

- 7 To open the **Hot actions** dialog box again, click **Hot actions**  in the notification tray.
- 8 (Optional) Click **Edit**, and do one of the following:
 - To create another hot action, click **Add** .
 - To delete the selected hot action, click **Remove** .
 - To edit the selected hot action, click **Edit** .
 - If you have more than one hot action created, click  to move the selected hot action up the list. This changes what function key the action is assigned to.
 - If you have more than one hot action created, click  to move the selected hot action down the list. This changes what function key the action is assigned to.
- 9 Click **Done**.

The hot actions you created are listed with their assigned function keys (F1, F2, and so on).

- 10 Trigger the hot action one of the following ways:
 - Select a hot action, and then click **Execute**.
 - Press **Ctrl+ Fn**.

Related Topics

[Action types](#) on page 443

Triggering one-time actions

You can trigger a one-time action from the notification tray.

What you should know

Although actions are usually triggered through event-to-actions, you can also trigger them manually from the notification tray if needed.

To trigger a one-time action:

- 1 In the notification tray, click **Hot actions** (🔊).
- 2 In the **Hot actions** dialog box, click **Manual action**.

The *Configure an action* window opens.

- 3 Select an action type, and specify the required parameters for the action.
- 4 Click **OK**.

The manual action executes.

Related Topics

[Action types](#) on page 443

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**.

Notification tray icons

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

Icon	Name	Description
	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 additional 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.
	Monitor ID	Shows the logical ID number assigned to your Security Desk monitor. Every individual monitor is assigned a unique ID number for the purpose of CCTV keyboard control, macros, and remote monitoring.

Icon	Name	Description
	Remote monitoring	Shows how many users are remotely controlling your Security Desk workstation. Click to view information about the users controlling your Security Desk, or kick out the users if you have the privileges to do so.
	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 (). 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 386.
	Hot actions	Click to open the <i>Hot actions</i> dialog box, and trigger a manual action or a hot action. Hot actions are actions you can trigger by pressing a function key on your keyboard. For more information, see Triggering hot actions on page 71.
	Joystick	Shows that a USB controller (for example, a joystick) is currently connected to your Security Desk workstation.
	CCTV Keyboard	Shows that a security keyboard is currently connected to your Security Desk workstation.
	Threat levels	Shows if there is a threat level set on your system. The icon turns red () when a threat level is currently activated. Click to open the <i>Threat levels</i> dialog box and activate or deactivate a threat level. For more information, see Responding to critical events through threat levels on page 373.
	Alarms	Shows the number of active alarms directed to you. The icon turns red () when you have active alarms in the system. Click to open the Alarm monitoring task and view the active alarms. For more information, see Acknowledging alarms on page 351.
	Inventory	Shows the number of MLPI offload files waiting to be reconciled. Click to open the Inventory management task and reconcile the reads. For more information, see Creating parking facility inventories on page 341.
	Task cycling	Click to turn task cycling on or off. For more information about how to adjust the time spent on each task, see Customizing task behaviour on page 51.
	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.

Icon	Name	Description
	Card requests	Shows the number of pending requests for credential cards to be printed (). Click to open the <i>Card requests</i> dialog box and respond to the request. For more information, see Responding to credential card requests on page 262.
	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, see Converting video files to ASF or MP4 format on page 188.

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**.

Remote monitoring

Using the *Remote* task, you can remotely monitor and control other Security Desks that are part of your system, using the *Monitoring* task and the *Alarm monitoring* task.

You can use the Remote task in the following two modes:

- **Simple mode:** Lets you control an individual Security Desk workstation.
- **Wall mode:** Lets you control a group of Security Desk monitors acting as a video wall. If you have physical video wall set up on your site, you can control all the monitors on that wall from your local Security Desk. Each monitor from the physical video wall is added as a separate remote Security Desk in the Remote task.

The actions you perform on the remote Security Desk are displayed locally in the Remote task, and on the remote Security Desk you are controlling. While remotely monitoring another Security Desk, you can still use all your local tasks.

IMPORTANT: You cannot remotely monitor Security Desks with an earlier version of Security Center installed. Backward compatibility is not supported for remote monitoring.

When connecting to a remote Security Desk, it is best practice to have the following:

- Your user privileges should be same as the user who is logged on to the remote Security Desk. If you have some user privileges that the remote user does not have, your connection is denied when you connect to the remote Security Desk.
- You should be a member of the same partitions as the user who is logged on to the remote Security Desk. If the partition settings do not match, your remote connection is also denied.

Connecting to remote Security Desks

To monitor and control Security Desks remotely, you must connect to one remote Security Desk workstation (*Simple mode*), or multiple remote Security Desk monitors (*Wall mode*).

Before you begin

When connecting to a remote Security Desk, make sure of the following:



- The remote Security Desk is running and connected to the same Security Center directory.
- You must have *Remote user control* of the Security Desks you want to connect to. Your system administrator needs to add each remote Security Desk workstation to the *Remote user control* list in the Security tab of your user in Config Tool (see the *Security Center Administrator Guide*).


What you should know

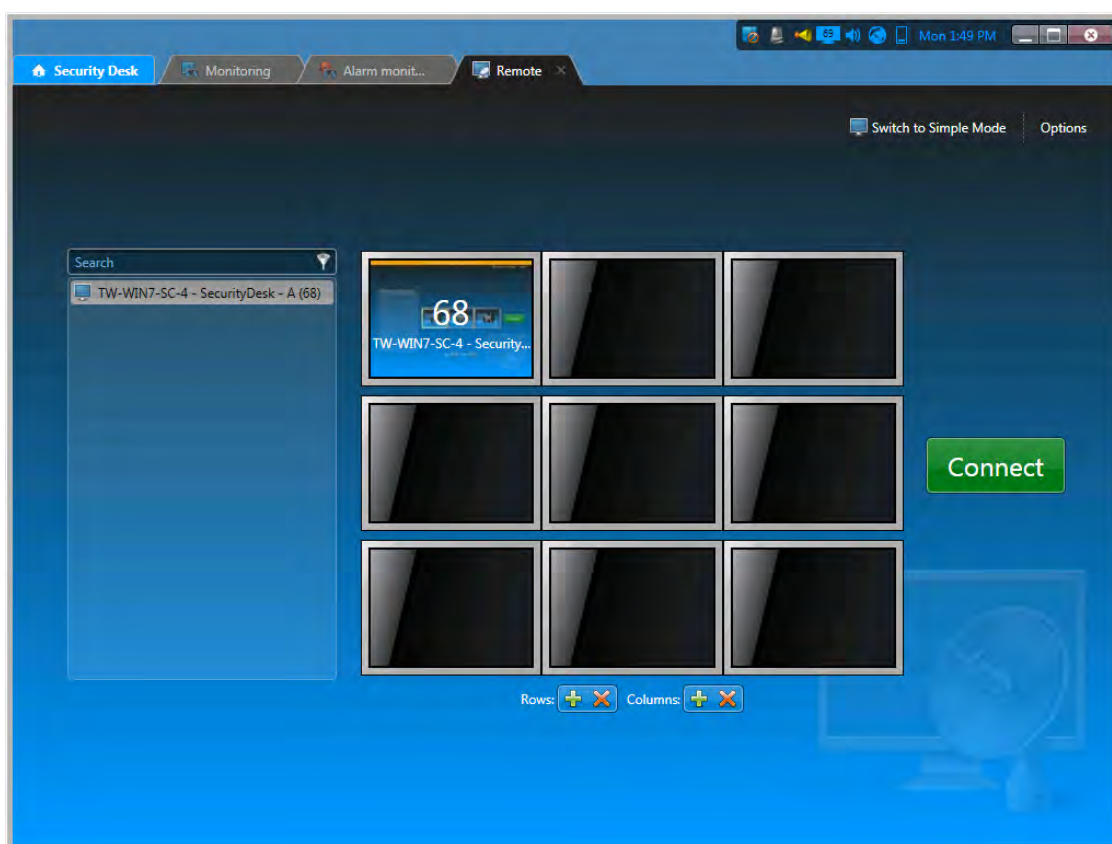
For information about the *Remote* task, see [Remote monitoring](#) on page 77.

IMPORTANT: You cannot remotely monitor Security Desks with an earlier version of Security Center installed. Backward compatibility is not supported for remote monitoring.

To connect to remote Security Desks:

- 1 From the home page, open the Remote task.
- 2 To connect to one remote Security Desk, select a remote Security Desk workstation from the drop-down list, or to connect to multiple remote Security Desk monitors, proceed as follows:
 - a) Click **Switch to Wall mode**.
 - b) To configure the layout of your wall, use the  and  buttons in the **Rows** and **Columns** sections.
 - c) From the drop-down list, double-click the remote Security Desk monitors you want to connect to.

The monitors you select populate the empty tiles. To remove a monitor from a tile, click  in the tile.



3 (Optional) Click **Options** and select one or both of the following:

- **Spy mode:** Allows you to connect to the Security Desk undetected. In this mode, you cannot perform any actions, you can only observe.
- **Low bandwidth:** Ensures that your bandwidth does not increase while remotely monitoring a Security Desk.

This option is helpful, because every command executed on the remote Security Desk is also executed on your local Security Desk, which might increase your bandwidth.

4 Click **Connect**.

You are connected to the remote Security Desk. If you are using Wall mode, the monitor that was placed in the first tile is displayed.

After you finish

Once you are connected, you can view the tasks that were already opened on the remote Security Desk. However, you can only use the *Monitoring* task and the *Alarm monitoring* task. For all other tasks, the following message is displayed: “This task cannot be remotely controlled”.

NOTE: On the remote Security Desk, the number of users that are remotely controlling it are indicated on the **Remote monitoring** icon in the notification tray (🖥️), unless those users are in spy mode. Click the **Remote monitoring** icon to view which users are remotely controlling your Security Desk, and which system they are on. If you have the user privilege, you can kick those users out of your Security Desk.

Related Topics

[Overview of the Remote task](#) on page 458

Monitoring events on remote Security Desks

In the *Monitoring* task on the remote Security Desk, you can use a subset of the actions available to you in a local *Monitoring* task. For example, you can only monitor video and access control and video entities (cameras, areas, doors, areas, elevators, intrusion detection areas, and so on).

Before you begin

[Connect to one or more Security Desks remotely.](#)

To monitor events on remote Security Desks:

- 1 Open the **Monitoring** task.

If the remote workstation does not have a **Monitoring** task open, proceed as follows:

- a) Right-click the **Home** tab, and click **New task** (+).
- b) Click **Monitoring**, and type a name for the task.
- c) Click **Create**.

- 2 Select which entities to monitor

This is done the same way as in a local *Monitoring* task.

- 3 To view an entity in a canvas tile, drag or double-click the entity from the area view.

The entity is displayed in your local Remote task, and on the remote workstation.

Related Topics

[Selecting entities to monitor](#) on page 65

Monitoring alarms on remote Security Desks

In the *Alarm monitoring* task on the remote Security Desk, you can acknowledge active alarms.

Before you begin

[Connect to one or more Security Desks remotely.](#)

To monitor alarms on remote Security Desks:

- 1 Open the **Alarm monitoring** task.
If the remote workstation does not have an **Alarm monitoring** task open, proceed as follows:
 - a) Right-click the **Home** tab and click **New task** (+).
 - b) Click **Alarm monitoring**, and then click **Create**.
- 2 Select an active alarm in the canvas, and acknowledge the alarm.

Related Topics

[Acknowledging alarms](#) on page 351

Actions you can perform on remote Security Desks

The following table lists what you can do while remotely monitoring a Security Desk from the *Remote* task.

All the commands listed are already described elsewhere in the *Security Desk User Guide*. If you want to find out more information about these commands, click the *See also* links.

Command	Description	Default keyboard shortcut	See also
Controlling cameras			
View live video	You can view video in the <i>Monitoring</i> task. NOTE: You cannot hear audio from the remote monitor on your local Security Desk.		Live and playback video modes on page 155
Change the stream selection	Change the video stream on the selected camera.		Changing the video stream on page 138
Switch to playback	Switch to playback video when you are currently viewing live video.	P	Live and playback video modes on page 155
Pause/play	Pause or play the video recording.	G	Live and playback video modes on page 155
Previous frame	When your playback video is paused, go to the previous video frame.	N	Camera widget on page 34
Next frame	When your playback video is paused, go to the next video frame.	M	Camera widget on page 34
Jump backward	Jump backwards in the recorded video according to the seek time specified in the Video options tab.	Ctrl+SHIFT+N	Camera widget on page 34
Jump forward	Jump forward in the recorded video according to the seek time specified in the Video options tab.	Ctrl+SHIFT+M	Camera widget on page 34
Go to specific date/time	Jump to a specific time in the video recording.		Switching between video modes on page 157
Switch to live	Switch to live video.	L	Switching between video modes on page 157
Controlling PTZ cameras			

Command	Description	Default keyboard shortcut	See also
PTZ pan left	Pan the PTZ camera image to the left.	LEFT ARROW	PTZ widget on page 39
PTZ pan right	Pan the PTZ camera image to the right.	RIGHT ARROW	
PTZ tilt down	Tilt the PTZ camera image down.	DOWN ARROW	
PTZ tilt up	Tilt the PTZ camera image up.	UP ARROW	
PTZ zoom in	Zoom in the PTZ camera image.	Hold the PLUS SIGN (+)	
PTZ zoom out	Zoom out the PTZ camera image.	Hold the HYPHEN (-) key	
Go to preset	Go to preset position.		
Rename preset/ pattern/ auxiliary	Rename a preset, pattern, or auxiliary.		
Save preset	Save preset position.		
Go to home position	Go to PTZ home (default) position.		
Adjust PTZ motor speed	Adjust the speed of the PTZ motor.		
Lock/unlock PTZ motor	Lock the PTZ controls from other users.		
Focus near/far	Manually focus the image near or far.		
Flip horizontally/ vertically	Flip the PTZ motor 180 degrees.		
Start PTZ pattern	Start a PTZ pattern. Click any preset of PTZ button to stop the pattern.		
Record new PTZ pattern	Record a new PTZ pattern.		
Set/clear auxiliary	Start or stop the PTZ auxiliary command.		

Command	Description	Default keyboard shortcut	See also
Controlling remote Security Desk layout			
Close all open tasks	Close all open tasks on the remote Security Desk workstation.		Opening tasks on page 45
Save the workspace	Save the task list so that it is automatically restored the next time same user logs on to the remote Security Desk.		Saving tasks on page 46
Start task cycling	Automatically switch between all loaded tasks in the Security Desk. By default, a 4 second dwell time for each task is used.		Opening tasks on page 45
Stop task cycling	Stop the task cycling rotation.		Opening tasks on page 45
Full screen	Toggle between displaying Security Desk in full screen and windows mode.		Opening tasks on page 45
Rename task	Rename the selected task.		Opening tasks on page 45
Change tile pattern	Change the tile pattern in the canvas.	Ctrl+P	<ul style="list-style-type: none"> • Changing tile patterns on page 27 • Customizing how tiles are displayed on page 29

Working with maps

This section includes the following topics:

- ["About Plan Manager"](#) on page 86
- ["Working with maps"](#) on page 87
- ["Differences between Monitoring and Maps tasks"](#) on page 89
- ["Supported map objects"](#) on page 91

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.

Working with maps

You can use either the [Maps](#) task or the [Monitoring](#) task to work with maps. While the Maps task is dedicated to working with maps, the Monitoring task is a generic task.

Once a map is loaded, the behavior of the map and the things you can do with it are exactly the same within both tasks. The differences have more to do with the specific workspace layout of each task.

Related Topics




[Overview of the Monitoring task on page 453](#)


[Overview of the Maps task on page 455](#)

Basic map commands

You can move your map by dragging it with the mouse, and interact with the security devices represented on the map by clicking on the devices. The shape of the mouse cursor indicates what action you can take.

The following table lists the basic commands you can use to interact with maps. Specific commands related to each type of [map objects](#) are described in [Supported map objects](#) on page 91.

To do this	Map command
Move the map	Drag.
Zoom in/out	Rotate the wheel upward/downward. Double-click/double-right-click.
Span the map across all monitors	(Maps task only) Click  Settings > Span map across all monitors in the task toolbar .
Switch to your default map	(Maps task only) Click  Default map in the task toolbar.
Switch to a different map	Click a map thumbnail. Click a map link (typically a colored semi-transparent polygon). (Maps task only) Click Select map or click a map name in the task toolbar. (Monitoring task only) Double-click a map () or drag it from the area view to the map tile.
Show the map object name	Point to the map object, or hold the Alt key to display the names of all map objects at once.

To do this	Map command
Select a map object	Click the map object. NOTE: If applicable, this action also: <ul style="list-style-type: none"> • Displays the related entity in a tile bubble • Displays the related widgets in the dashboard
Find entities on maps	(Maps task only) Click  Search in the task toolbar, and enter an entity name.
Display map object in the Monitoring task	(If applicable) Double-click the map object.
View multiple map objects in the Monitoring task (Lasso)	Click and drag while holding the ALT key to draw a lasso around the map objects you want to display in the Monitoring task.
Display all cameras that can see a specific location on the map in the Monitoring task (Smart click)	Click the location of interest on the map while holding the CTRL key. NOTE: All cameras that can see the clicked location are displayed in the Monitoring task. PTZ cameras that support <i>position feedback</i> will automatically turn to the location you clicked, if they are not obstructed by walls.


Showing or hiding information on your maps

You can choose the amount of information you want to show on your map by selecting the layers to display.

What you should know

A map is composed of a static background image with various information layered on top, called *map objects*. You can choose to show or hide any of these layers, thus, showing more or less information on your map.

To control the amount of information you want to see on your map:





- 1 Do one of the following:
 - Right-click anywhere on your map, and select **Layers**.
 - (Maps task only) Click  **Settings > Layers** in the [task toolbar](#).
- 2 In the dialog box that appears, select the layers (map objects) you want to show on your map.
- 3 Click **OK**.



NOTE: The option to cancel your changes is not available on this dialog.

Differences between Monitoring and Maps tasks

Both Monitoring and Maps tasks can be used to work with maps. The former is better suited when Security Desk is only controlling one monitor. The latter is better suited when Security Desk is controlling multiple monitors.

Once a map is loaded, the behavior of the map and the things you can do with it are exactly the same within both tasks. The differences have more to do with the specific workspace layout of each task.

Map feature	Monitoring task	Maps task
When to use	Only one monitor is controlled by your Security Desk workstation, and you need to see map and video side by side at all times.	Multiple monitors are controlled by your Security Desk workstation.
Multiple task instances	Yes.	Yes.
Map display area	Maps are displayed in tiles.	One map covers the entire workspace.
Multiple map display	Each tile can display a different map.	Displays one map at a time.
Span the map across all monitors	Not supported.	Click  Settings > Span map across all monitors in the task toolbar .
Click an entity on the map	Displays the entity in a tile bubble over the map.	Displays the entity in a tile bubble over the map.
Double-click an entity on the map	Displays the entity in a free tile in the canvas. When all tiles are filled, replaces the oldest displayed entity. May replace the map itself if it happens to be the oldest entity.	Displays the entity in a monitoring task if one is already open. If not, opens one.
Switch to a different map	Drag a different map (area) from the area view to the tile showing the current map.	Click a different map in the task toolbar.
Find entities on maps	Right-click an entity displayed in a tile and click Locate me .	Click  Search in the task toolbar, and enter an entity name..
Switch to your default map	Not supported.	Click  Default map in the task toolbar..
Switch to a favorite map	Not supported.	Click Select map in the task toolbar, and click a favorite.
Show alarm list	Type F9 and click Alarms .	Click  Alarms in the task toolbar.

Map feature	Monitoring task	Maps task
Show event list	Type F9 and click Events .	Click  Past events in the task toolbar.
Show/hide dashboard	Type F7 or click Hide dashboard .	Type F7 or click  Settings > Show dashboard in the task toolbar.








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.

The following map objects are supported.

Map object	Appearance on maps	Application and specific actions
Access control unit	<ul style="list-style-type: none"> •  - Access control unit • The color indicates the access control unit state: <i>Online</i>, <i>Offline</i>, or <i>Warning</i>. 	<ul style="list-style-type: none"> • Monitor the access control unit state.
Area	<ul style="list-style-type: none"> • 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). 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> •  - 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. 	<ul style="list-style-type: none"> • 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 and shunt the reader from the widget.

Map object	Appearance on maps	Application and specific actions
Camera	<ul style="list-style-type: none">  - Camera is not recording  - Camera is recording  - Camera detected motion (with green ripple effect)  - Camera is in maintenance mode Fixed cameras are shown with a blue FOV (field of view). PTZ cameras are shown with a green FOV. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none">  - Camera sequence 	<ul style="list-style-type: none"> Display multiple cameras at once. Point a number of PTZ cameras to a specific location. Double-click to display the camera sequence unpacked in a Monitoring task. <p>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.</p>
LPR camera	<ul style="list-style-type: none">  - Fixed LPR camera  - LPR camera is in maintenance mode Reads and hits are shown in notification bubbles. 	<ul style="list-style-type: none"> Monitor reads and hits from LPR cameras. Click to view live video from the associated context camera.
Alarm	<ul style="list-style-type: none">  - Alarm is inactive  - Alarm is active A map object that is linked to an active alarm is flagged with an alarm notification bubble. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Intrusion detection areas are represented as colored semi-transparent polygons. The color indicates the intrusion detection area state: <i>Perimeter armed, Master armed, Disarmed, or Unknown.</i> 	<ul style="list-style-type: none"> Monitor alarms and intrusion detection area state. Arm and disarm the intrusion detection area from the widget.
Zone	<ul style="list-style-type: none"> Hardware and virtual zones are represented as colored semi-transparent polygons. The color indicates the zone state: <i>Armed, Disarmed, or Unknown.</i> 	<ul style="list-style-type: none"> Monitor alarms and zone state. Arm and disarm the zone from the widget.
Input pin	<ul style="list-style-type: none">  - Input is active  - Input is inactive 	<ul style="list-style-type: none"> Monitor the input state.
Output relay	<ul style="list-style-type: none">  - Output relay (Normal)  - Output relay (Active) 	<ul style="list-style-type: none"> Trigger output behaviors on output relays directly from maps. Click to show a list of output behaviors you can trigger.
KML object	<ul style="list-style-type: none"> Can be anything displayed as transparent layer over a georeferenced map. 	<ul style="list-style-type: none"> Overlay useful information on maps, such as city boundaries, roads, and hydrographic features.
Macro	<ul style="list-style-type: none">  - Macro 	<ul style="list-style-type: none"> Execute macros directly from maps. Override the default execution context on maps. Click on a macro to run it.
Map link	<p>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.</p>	<ul style="list-style-type: none"> 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.

Map object	Appearance on maps	Application and specific actions
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.	A sample application could be to indicate the location of wall mounted scanners on a department store floor plan.
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 Genetec representative for information on Genetec Custom Solutions.

Advanced tasks

This section includes the following topics:

- ["Starting macros"](#) on page 96
- ["Finding out what changes were made to the system configuration"](#) on page 97
- ["Investigating user related activity on the system"](#) on page 98
- ["Viewing properties of units"](#) on page 101
- ["Monitoring your computer resources"](#) on page 103
- ["Shortcuts to external tools"](#) on page 107
- ["Customizing user logon options"](#) on page 109
- ["Customizing network options"](#) on page 111

Starting macros

You can start and stop a macro from the *System status* task.

Before you begin

You need the *Execute macros* privilege to start or stop macros.

What you should know

A macro is a type of entity that encapsulates a C# program that adds custom functionalities to Security Center. For more information about creating and configuring macros in Config Tool, see the *Security Center Administrator Guide*.

To start a macro:

- 1 From the home page, open the System status task.
- 2 From the **Monitor** drop-down list, select **Macros**.

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

- 3 Start a macro:
 - Select a macro in the report pane, and click **Start** (▶).
 - Click **Start** (▶), select a macro, and then click **Start**.
- 4 To stop an executing macro, select the macro in the report pane, and then click **Stop** (■).

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.

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 in Config Tool (see the *Security Center Administrator Guide*).

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 perimeter 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.
- 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.

Viewing properties of units

At a glance, you can view a list of all the 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.

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 has been 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.
- **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 will reject communication and the camera will go offline. For example, the Archiver expects the camera to be using digest authentication but suddenly the

camera wants 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 have been made visible to you when they were created or last configured.

Monitoring your computer resources

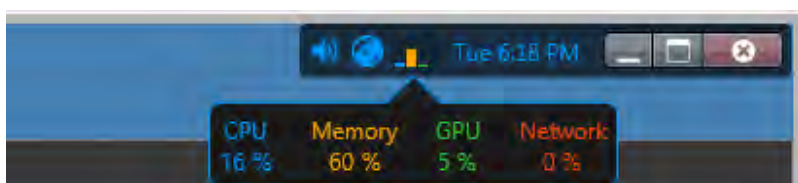
You can monitor the usage percentage of your computer resources by hovering the mouse pointer over the **Resources meter** icon in the notification tray. Click the same icon to view a summary of the hardware installed on your computer and their current use in a dialog box.

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.



The usage of your computer resources is shown in four categories:

- CPU (blue)
- Memory (orange)
- 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.

- 2 Click the **Resources meter** icon in the notification tray to view detailed information about your computer resources in the [Hardware information dialog box](#).

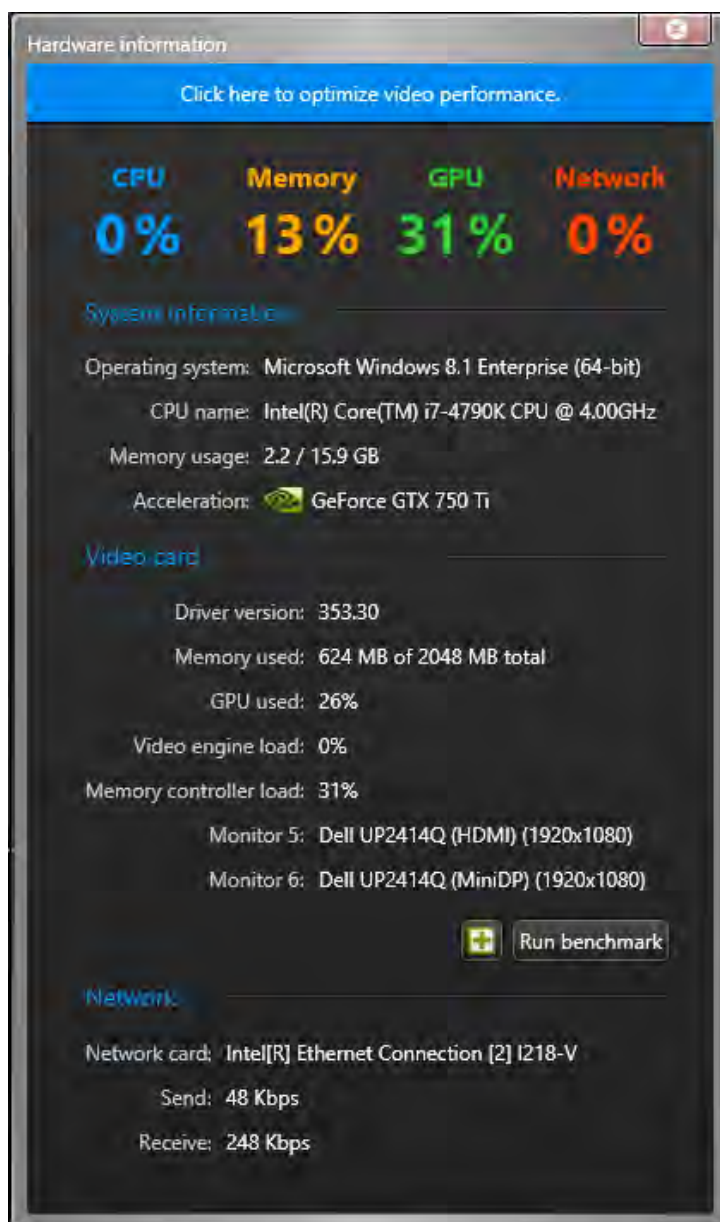
Related Topics

[Video options](#) on page 203

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.



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 more information about running the hardware benchmark tool, see [Using the hardware benchmark tool](#) on page 105.

Related Topics

[Video options](#) on page 203

[Troubleshooting: Hardware acceleration issues](#) on page 418

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.

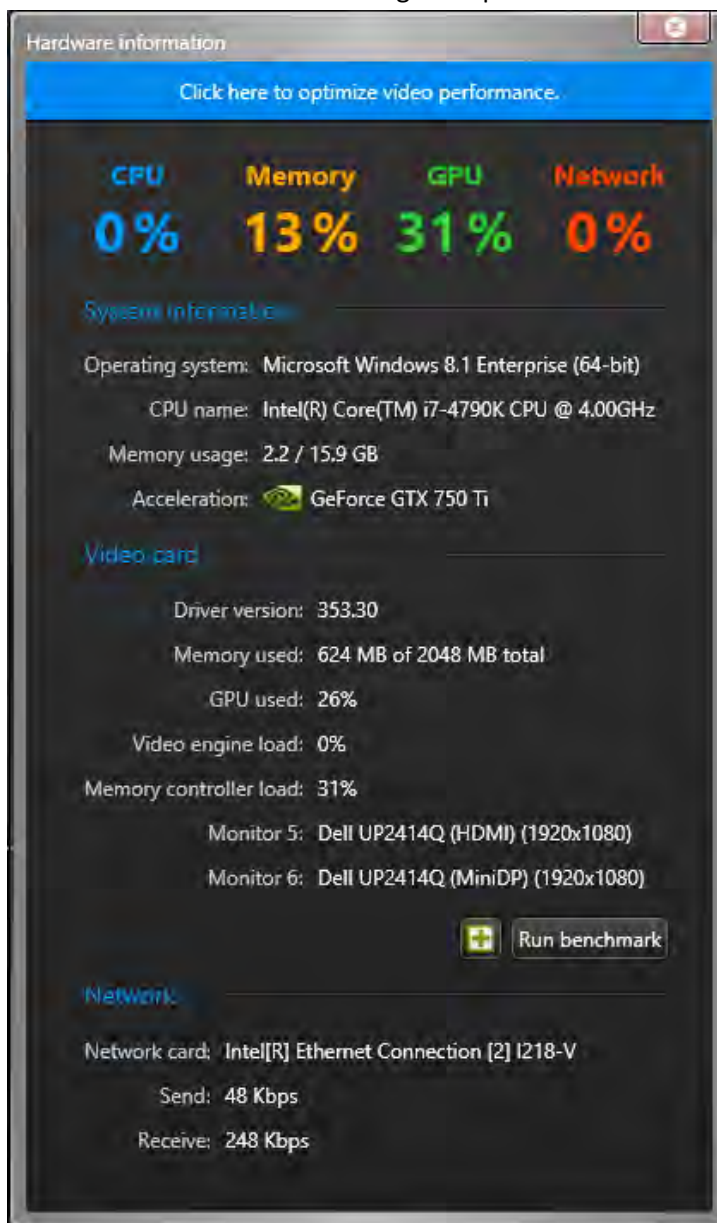
What you should know

- 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:

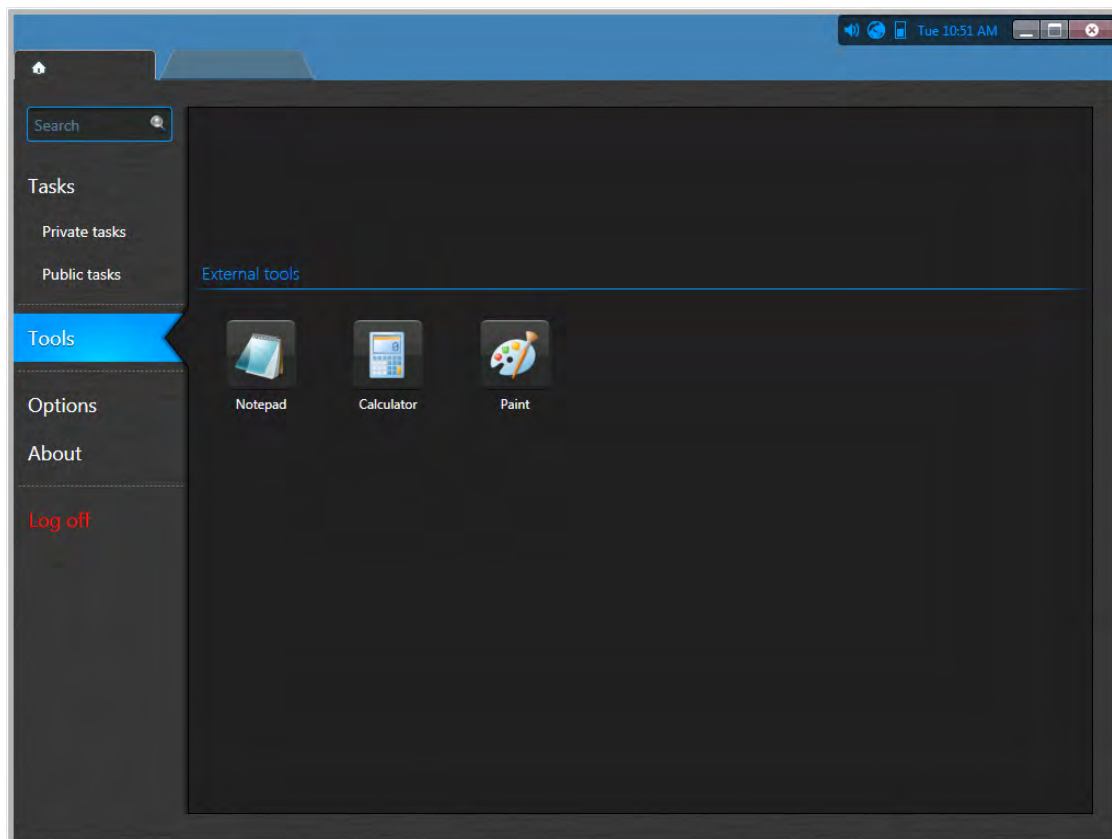


- 2 From the **Acceleration** drop-down list, select the video card you want to run the benchmark test on.
- 3 Click **Run benchmark**.
Once the benchmark test is complete, the **Frame rate** capability of the selected card is listed.
- 4 Click **Close**.

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>
```

Customizing user logon options

You can select how and when users are allowed to log on to Security Center.

What you should know

You must be an administrator to configure the logon options. 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.

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*. For more information about importing users from a corporate Active Directory, see the *Security Center Administrator Guide*.

- 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.



- 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 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.

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.

Keyboard shortcuts

This section includes the following topics:

- ["Default keyboard shortcuts"](#) on page 113
- ["Switching tasks using your keyboard"](#) on page 119
- ["Displaying cameras using your keyboard"](#) on page 120
- ["Customizing keyboard shortcuts"](#) on page 122

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		
Auto lock	Lock the workstation.	Ctrl+Shift+L
Cycle through canvas only, report only, and both	Show only the canvas, only the report pane, or both.	F9
Dashboard	Show/hide the dashboard.	F7
Exit application	Close the application.	Alt+F4
Full screen	Toggle between displaying the application in full screen and windows mode.	F11
Go to next content in cycle	When you are viewing a packed entity in a tile, switch to the next attached entity, or the next camera in the sequence.	Ctrl+Right arrow
Go to next content in cycle (all)	When you are viewing a packed entity in a tile, switch to the next attached entity, or the next camera in the sequence.	Ctrl+Shift+Right arrow
Go to next page	Switch to the next task tab.	Ctrl+Tab
Go to previous content in cycle	When you are viewing a packed entity in a tile, switch to the previous attached entity, or the next camera in the sequence.	Ctrl+Left arrow
Go to previous content in cycle (all)	When you are viewing a packed entity in a tile, switch to the previous attached entity, or the next camera in the sequence.	Ctrl+Shift+Left arrow
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 (`)
Hot action x	Execute hot actions 1-10, once you've configured them.	Ctrl+(F1-F10)
Options	Open the Options dialog box.	Ctrl+O

Command	Description	Shortcut
Select columns	Select which columns to show/hide in the report pane.	Ctrl+Shift+C
Selector	Show/hide the selector pane.	F6
Start cycling	Automatically switch between all loaded entities in Security Desk. By default, a 4 second dwell time for each entity is used.	Ctrl+Up arrow
Start cycling (all)	Automatically switch between all loaded entities in Security Desk. By default, a 4 second dwell time for each entity is used.	Ctrl+Shift+Up arrow
Tiles only	Show only the display tiles and task list. The selector pane, event pane, and dashboard are hidden. This is mainly used for the <i>Monitoring</i> task.	F10
Alarm commands		
Acknowledge (Default)	Acknowledge the selected alarm in the <i>Alarm report</i> task.	Spacebar
Acknowledge all (Default)	Acknowledge all alarms in the <i>Alarm report</i> task.	Ctrl+Shift+Spacebar
Show alarm page	Open the <i>Alarm monitoring</i> task.	Ctrl+A
Snooze alarm (all)	Put all alarms to sleep for 30 seconds. When an alarm is snoozing, it is temporarily removed from the canvas.	Atl+Ctrl+Shift+S
Snooze the alarm	Put the alarm to sleep for 30 seconds. When the alarm is snoozing, it is temporarily removed from the canvas.	S
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
Export video	Export video from the selected tile.	Ctrl+E
Export video from all tiles	Export video from all the tile in the canvas.	Ctrl+Shift+E
Forward	Forward the video playback.	Period (.)

Command	Description	Shortcut
Forward all	Forward the video playback of all cameras that are displayed in the canvas.	Ctrl+Shift+Period (.)
Instant replay	View an instant video replay in the selected tile.	I
Jump backward	Jump backwards in the recorded video according to the seek time specified in the Options dialog box.	Ctrl+Shift+N
Jump backward all	Jump backwards in the recorded video according to the seek time specified in the Options dialog box, for all cameras that are displayed in the canvas.	Alt+Ctrl+Shift+N
Jump forward	Jump forward in the recorded video according to the seek time specified in the Options dialog box.	Ctrl+Shift+M
Jump forward all	Jump forward in the recorded video according to the seek time specified in the Options dialog box, for all cameras that are displayed in the canvas.	Alt+Ctrl+Shift+M
Next frame	When your playback video is paused, go to the next video frame.	M
Next frame all	When your playback video is paused, go to the next video frame. This applies to all cameras that are displayed in the canvas.	Ctrl+Shift+J
Play/Pause	Pause or play the video recording.	G
Play/Pause all	Pause or play the video recording for all cameras that are displayed in the canvas.	Ctrl+Shift+G
Previous frame	When your playback video is paused, go to the previous video frame.	N
Previous frame all	When your playback video is paused, go to the previous video frame. This applies to all cameras that are displayed in the canvas.	Ctrl+Shift+H
Rewind	Rewind the video playback.	Comma (,)
Rewind all	Rewind the video playback for all cameras that are displayed in the canvas.	Ctrl+Shift+Comma (,)
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

Command	Description	Shortcut
Show video stream status	Show/hide the status summary of the video stream connectins and redirections in the selected tile.	Ctrl+Shift+R
Slow motion	Switch the playback to slow motion.	Shift+En dash (-)
Slow motion (all)	Switch the playback to slow motion for all cameras that are displayed in the canvas.	Ctrl+Shift+En dash (-)
Switch to live	Switch to live video.	L
Switch to live (all)	Switch to live video for all cameras that are displayed in the canvas.	Ctrl+Shift+V
Switch to playback	Switch to playback video.	P
Toggle recording	Start/stop recording video for the selected tile.	R
Toggle recording (all)	Start/stop recording video for all cameras that are displayed in the canvas.	Alt+Ctrl+Shift+R
Visual tracking	Enable/disable visual tracking for the selected tile.	Alt+F
Visual tracking (all)	Enable/disable visual tracking for all cameras that are displayed in the canvas.	Ctrl+Shift+F
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
Door commands		
Unlock	Unlock the selected door.	U
Unlock (all)	Unlock all the doors that are displayed in the canvas.	Ctrl+Shift+U
Task commands		
Rename task	Rename the selected task.	F2

Command	Description	Shortcut
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 <i>public tasks</i> page from the home page.	Ctrl+N
Tile commands		
Back	Switch to the previous tile content.	Alt+Left arrow
Change tile pattern	Change the tile pattern in the canvas.	Ctrl+P
Clear	Clear a specific tile in the canvas.	<Tile ID>+Backspace
Clear all	Clear all the tiles in the canvas.	Ctrl+Backspace
Cycle next pattern	Cycle to the next tile pattern.	W
Cycle previous pattern	Cycle to the previous tile pattern.	Q
Display camera sequence	Display a camera sequence in a specific tile.	<Camera sequence ID>+Ctrl+Enter
Display entity	Display an entity in a specific tile.	<Entity ID>+Enter
Forward	Switch to the next tile content.	Alt+Right arrow
Home	<ul style="list-style-type: none"> • Map mode: Jump to the home web page associated with the map. • Tile mode: Return to the first content you dragged into the tile. 	Alt+Home
Maximize tile	Maximize the selected tile to the whole canvas. Press E again to shrink the tile.	E
Maximize tile fullscreen	Maximize the selected tile to full screen mode. Press Alt+ENTER again to shrink the tile.	Alt+Enter
Monitor alarms	Enable/disable alarm monitoring for the selected tile. When alarm monitoring is enabled, alarms automatically appear in the tile.	Alt+A
Monitor all alarms	Enable/disable alarm monitoring for all tiles in the canvas. When alarm monitoring is enabled, alarms automatically appear in the tiles.	Alt+Ctrl+Shift+A

Command	Description	Shortcut
Monitor events	Enable/disable event monitoring for the selected tile. When event monitoring is enabled, events automatically appear in the tile.	Alt+T
Pack/unpack	Pack/unpack the area or camera sequence in the selected tile.	Alt+U
Refresh	Refresh the page, or reload the selected tile.	F5
Select next tile	Select the next tile in the canvas.	Y
Select previous tile	Select the previous tile in the canvas.	T
Start task cycling	Automatically switch between all loaded tasks in Security Desk. By default, a 4 second dwell time for each task is used.	Ctrl+Q
Stop task cycling	Stop the task cycling rotation.	ESC
Toggle monitoring (all)	Enable/disable event monitoring for all tiles in the canvas. When event monitoring is enabled, events automatically appear in the tiles.	Alt+Ctrl+Shift+T

Related Topics

[Customizing keyboard shortcuts](#) on page 122

Switching tasks using your keyboard

You can open a saved public task, or switch between public tasks on your local workstation using a keyboard shortcut sequence.

Before you begin

You need the logical ID of the public task. To find the logical ID of a task, check in the *System* task in Config Tool.

IMPORTANT: Multiple entities can use the same logical ID. If this is the case, then a camera or analog monitor entity with the same logical ID takes priority over the public task, and is displayed in the canvas instead of switching tasks.

To switch tasks using your keyboard:

- Type the task ID, and then press **ENTER**.

Example: <50><ENTER>.

Switching tasks on a remote monitor using your keyboard

If you are controlling a video wall or analog monitor, you can open a saved public task, or switch between public tasks on the remote workstation using a keyboard shortcut sequence.

Before you begin

You need the logical ID of the public task. To find the logical ID of a task, check in the *System* task in Config Tool.

IMPORTANT: Multiple entities can use the same logical ID. If this is the case, then a camera or analog monitor entity with the same logical ID takes priority over the public task, and is displayed in the canvas instead of switching tasks.

What you should know

As you type the shortcut, the monitor and task IDs are displayed at the top of your local Security Desk window beside the notification tray. This helps you keep track of what numbers you have entered.



To switch tasks on a remote monitor using your keyboard:

- 1 Type the remote Security Desk monitor ID, and then press the **PERIOD** (.) key.

TIP: The Security Desk monitor ID is shown in the notification tray (65). If it is not displayed, you can show the monitor ID icon from the Options dialog box.

- 2 Type the logical ID of the task, and then press **ENTER**.

Example: <65><PERIOD><50><ENTER>.

Related Topics

[Configuring the notification tray on page 73](#)

Displaying cameras using your keyboard

You can display a camera in a tile, or switch cameras on your local workstation using a keyboard shortcut.

What you should know

Tile IDs range from 1-26, depending on the tile pattern you are using. It is easier to select which camera to display when their logical IDs are shown in the area view. You can enable this option from the Options dialog box.

To display a camera using your keyboard:

- 1 Type the tile ID, and then press the **Period (.)** key.
- 2 Type the camera ID, and then press **Enter**.

Example: <2><Period><15><Enter>.

The camera is displayed in the tile you selected. If you did not select a tile, the camera is displayed in the first free tile.


Related Topics

[Customizing how entities are displayed in the canvas](#) on page 22

Displaying cameras on a remote monitor using your keyboard

If you are controlling a video wall or analog monitor, you can display a camera a tile or switch cameras on the remote workstation using a keyboard shortcut.

Before you begin

You must know the remote monitor ID. You can find the Security Desk monitor ID in the notification tray (). If it is not displayed, you can show the monitor ID icon from the Options dialog box.

What you should know

Tile IDs range from 1-26, depending on the tile pattern you are using. It is easier to select which camera to display when their logical IDs are shown in the area view. You can enable this option from the Options dialog box.

As you type the shortcut, the monitor, tile, and camera IDs are displayed at the top of your local Security Desk window beside the notification tray. This helps you keep track of what numbers you have entered.



To display a camera on a remote monitor using your keyboard:

- 1 Type the remote Security Desk monitor ID, and then press the **Period (.)** key.
- 2 Type the tile ID, and then press **Period**.
- 3 Type the camera ID, and then press **Enter**.

Example: <65><Period><3><Period><12><Enter>.

If you did not select a tile, the camera is displayed in the first free tile.

Related Topics

[Configuring the notification tray](#) on page 73

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 113

Part II

Video

This part includes the following chapters:

- Chapter 10, "[Video at a glance](#)" on page 124
- Chapter 11, "[Cameras](#)" on page 126
- Chapter 12, "[Video archives](#)" on page 154
- Chapter 13, "[Video export](#)" on page 174
- Chapter 14, "[Video options](#)" on page 198

Video at a glance

This section includes the following topics:

- ["About Omnicast"](#) on page 125

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

Cameras

This section includes the following topics:

- ["About cameras \(video encoders\)"](#) on page 127
- ["Viewing cameras in tiles"](#) on page 128
- ["On-tile video controls"](#) on page 129
- ["Controlling camera sequences"](#) on page 130
- ["How PTZ cameras are displayed in the canvas"](#) on page 131
- ["Controlling PTZ cameras"](#) on page 132
- ["Dewarping 360 degree camera lenses"](#) on page 133
- ["Viewing video on analog monitors"](#) on page 135
- ["Synchronizing video in tiles"](#) on page 137
- ["Changing the video stream"](#) on page 138
- ["Zooming in and out of video"](#) on page 139
- ["Creating digital zoom presets"](#) on page 140
- ["About visual tracking"](#) on page 141
- ["Adding bookmarks to video sequences"](#) on page 143
- ["Customizing snapshot options"](#) on page 145
- ["Taking snapshots of video"](#) on page 146
- ["Editing video snapshots"](#) on page 147
- ["Camera blocking"](#) on page 148
- ["Blocking users from viewing video"](#) on page 149
- ["How video is displayed if the Directory role disconnects"](#) on page 150
- ["Viewing camera settings"](#) on page 152

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.

Viewing cameras in tiles

From any video-related task in Security Desk, you can view cameras in the canvas.

To view a camera in a tile:

- Do one of the following:
 - Find a camera in the area view, and then double-click or drag it into a tile.
 - Drag a camera from the report pane into a tile.

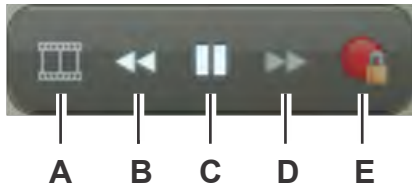
On-tile video controls

When viewing a camera in the canvas, a set of on-tile video controls appear on top of the video image when your mouse pointer hovers over the tile.

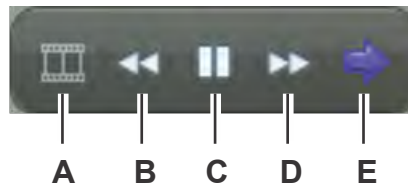
You can also hide the on-tile controls from the Options dialog box.

The following figures show the on-tile video controls when viewing live and playback video.

Live video:



Playback video:



A	Show/hide thumbnail images
B	Rewind (reverse playback)
C	Pause
D	Forward
E	<ul style="list-style-type: none"> • Live video: Recording state • Playback video: Switch to live video

Related Topics

[Camera widget](#) on page 34

[Customizing how tiles are displayed](#) on page 29

Controlling camera sequences

From any video-related task in Security Desk, you can control camera sequences that are displayed in the canvas.

What you should know

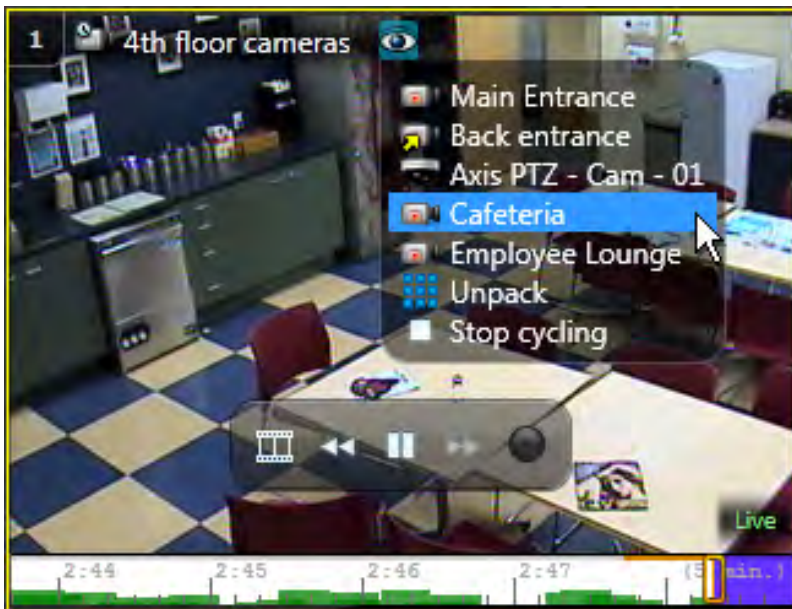
Camera sequences are groups of cameras that are saved as a single entity. They are represented in the area view by a camera icon with a clock overlay (🕒). If a camera in a sequence goes offline, you do not see the entity state change to red (offline), but the video stream is not available.

When a camera sequence is displayed in a tile, all the cameras in the sequence are displayed in rotation. If you add additional camera sequences to the canvas, the camera rotation is synchronized.

NOTE: If there is a PTZ camera in the sequence and you start controlling the PTZ, the rotation stops. You can click **Start cycling** again once you are done controlling the PTZ.

To control a camera sequence:

- 1 Display the camera sequence one of the following ways:
 - Find the camera sequence in the area view, and then double-click or drag it into a tile.
 - Drag the camera sequence from the report pane into a tile.
- 2 In the tile toolbar, click 🕒.



- 3 From the drop-down list of packed entities, do one of the following:
 - To pause the sequence and stay with the current camera, click **Stop cycling**.
 - To display all cameras simultaneously, click **Unpack**.
 - To force the sequence to display a specific stream, click the individual camera.

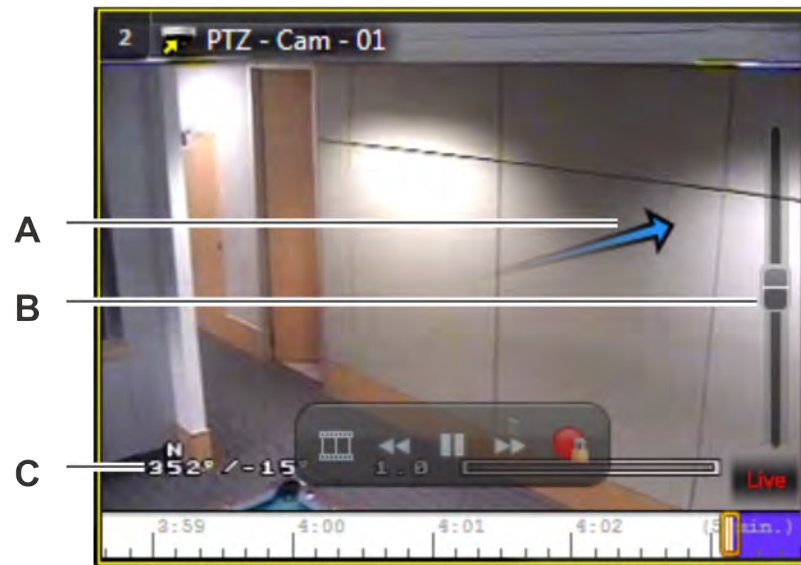
Related Topics

[Synchronizing video in tiles](#) on page 137

How PTZ cameras are displayed in the canvas

When a PTZ-enabled camera (👁️) is displayed in a tile, a zoom slider appears when the mouse pointer hovers over the video, which indicates that the PTZ controls are available.

The following illustration shows the different components of a tile when a PTZ camera is displayed.



-
- A** Direction that the PTZ motor is panning. The longer the arrow, the faster the motor moves. The shorter the arrow, the slower the motor moves.
-
- B** Slider that is used to zoom in and out.
-
- C** Current PTZ motor position and zoom value.
-

Controlling PTZ cameras

From any video-related task in Security Desk, you can control PTZ cameras that are displayed in the canvas.

What you should know

Some PTZ camera models support the following two additional PTZ controls:

- **Zoom box:** Zoom in on an area by drawing a box on the video image. 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.

To enable these commands, you must configure the PTZ for zoom box and center-on-click in Config Tool. For more information about configuring PTZ motors, see the *Security Center Administrator Guide*).

TIP: It is easier to use the PTZ controls when the on-tile video controls are hidden. You can hide the on-tile video controls from the Options dialog box.

You might be locked from controlling the PTZ if a user with a higher user level is currently controlling it. If you have the same user level as another user, the priority is decided on a first come first served basis.

To control a PTZ camera:

- 1 To display the PTZ camera, double-click or drag it from the area view or report pane into a canvas tile.
- 2 To expand the tile, double-click on the tile toolbar.
- 3 Zoom in and out one of the following ways:
 - Move your mouse pointer over the tile, and then move the zoom slider handle up to zoom in or down to zoom out.
TIP: You can also use your mouse wheel to zoom in and out.
 - If your PTZ camera supports the *Zoom box* feature, draw a box on the video image to zoom in.
- 4 To pan the PTZ motor, you can either:
 - a) click on the PTZ camera tile.
A white arrow appears.
 - b) Click on the white arrow once to change it to a blue arrow
A blue arrow indicates the direction of movement. The longer the arrow, the faster the motor moves. The shorter the arrow, the slower the motor moves.
 - c) Click your mouse pointer in the direction you want the PTZ motor to move.
 - a) Click once on the blue dot in the middle of the PTZ tile.
 - b) Click your mouse pointer in the direction you want the PTZ motor to move.
Blue arrows are following your movements.
- 5 If your PTZ camera supports the *Center-on-click* feature, click in the video image to center the image on that point.

Related Topics

[Customizing keyboard shortcuts](#) on page 122

Dewarping 360 degree camera lenses

To display a 360 degree fish-eye or panoramic camera lens image as a rectangular image in a Security Desk tile, you can dewarp, or flatten it by zooming into the camera image.

Before you begin

Configure the camera lens in Config Tool. For manufacturer-specific information about configuring 360 degree fish-eye or panoramic camera lenses, see the *Security Center Video Unit Configuration Guide*.

What you should know

The dewarping time varies, depending on your computer and the dewarped resolution. For example, the dewarping time will be four times longer using a 640x480 resolution instead of a 320x240 resolution.

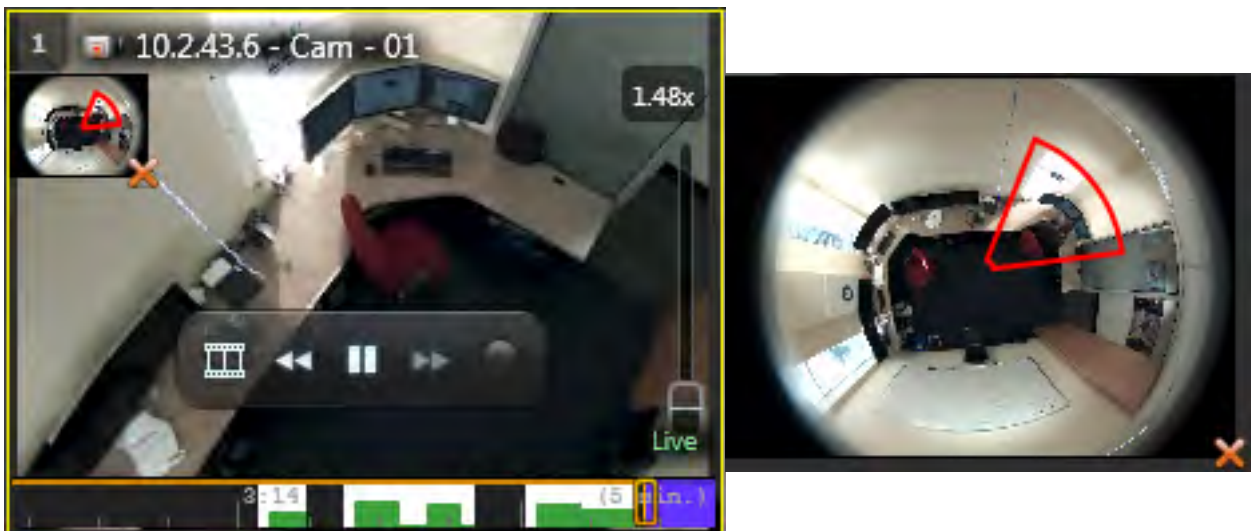
To dewarp a 360 degree camera lens:

- 1 Display a 360 degree fish-eye or panoramic camera in a tile.
- 2 To zoom in the image, use your mouse wheel, or draw a box on the region you want to zoom to.

NOTE: If you zoom using your mouse wheel, it zooms to the center of the image, not where your cursor is pointing.



- 3 To navigate the zoomed image, click the image thumbnail at the top-left of the tile.



- 4 To zoom out, use the mouse wheel, or the zoom slider on the right-side of the tile.

Viewing video on analog monitors

You can view live video on an analog monitor by displaying a camera or camera sequence in an analog monitor entity (📺) in the canvas. You can also receive alarms on an analog monitor if the analog monitor entity is a recipient of those alarms.

Before you begin

Your decoder unit needs to be connected to an analog monitor and it must be added in Security Center as a video decoding unit entity.

What you should know

If your decoder unit supports more than one analog monitor (for example, it is connected to multiple monitors on a video wall), each monitor is added as a separate analog monitor entity in Security Center. You can reproduce the physical layout of your video wall by adding the analog monitor entities to the canvas in a similar tile pattern. For more information about configuring analog monitors in Config Tool, see the *Security Center Administrator Guide*.

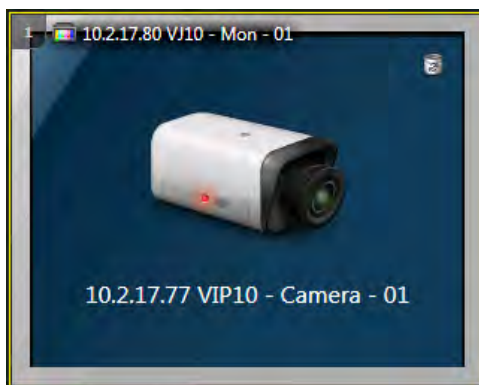
Omnicast 4.x federated cameras are not supported on analog monitors in Security Center.

To view video on an analog monitor:

- 1 Double-click or drag the analog monitor entity from the area view to a tile in the canvas.
- 2 Double-click or drag a supported camera or camera sequence into the tile that is displaying the analog monitor.

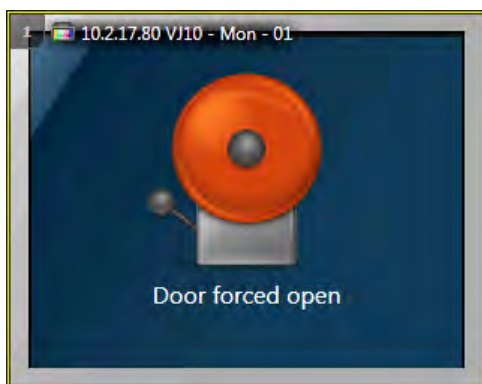
NOTE: Supported cameras must be from the same manufacturer as the video decoding unit and use the same video format.

The live video from the camera is displayed on the physical analog monitor. In Security Desk, only the camera name and camera icon are displayed.



- 3 To control the displayed cameras, use the widgets in the dashboard (for example, the camera or PTZ widget).
- 4 To remove the camera from the analog monitor, click 🗑️ in the tile.

If your analog monitor entity is a recipient of an alarm, you can receive alarms on your physical analog monitor. When you receive an alarm, the following is shown in the tile that is displaying the analog monitor.



5 To acknowledge the alarm, click **Acknowledge (Default)** (✓) in the alarm widget.

Related Topics


[Camera widget](#) on page 34

[PTZ widget](#) on page 39


Synchronizing video in tiles

You can force the live or playback video that is displayed in all the tiles to become synchronized in time.

To synchronize video displayed in tiles:

- 1 Select a tile.
- 2 At the bottom of the canvas, click **Synchronize video** ()

All the tiles are forced to display live or recorded video. The reference point is the currently selected tile. One of the following happens:

- If selected tile is displaying recorded video, synchronization forces all tiles to display playback video. All the playback videos display the same recording date and time, synchronized to the millisecond.
 - If the selected tile is displaying live video, synchronization forces all tiles to display live video. This is useful if you have multiple cameras with overlapping coverage. Forcing playback synchronization produces different perspectives of the same recorded event
- 3 To turn synchronization off, click **Stop synchronizing video** () at the bottom of the canvas.

Changing the video stream

You can change the video stream of a camera displaying live video in a tile.

Before you begin

If your camera supports multiple video streams, the streams must be enabled and configured in Config Tool before you can select the default video stream. For information about configuring video streams, see the *Security Center Administrator Guide*.

What you should know

Most *video encoders* and *IP cameras* supported by Security Center can generate multiple *streams* per individual camera. This is helpful when you want your live monitoring stream to be configured with a different video quality than the recorded stream. Additional streams can be configured for other needs, such as remote access (low bandwidth) or low resolution versus high resolution streams.

To change the video stream:

- 1 Right-click on the live video image in a tile.
- 2 Click **Camera > Select live stream**.
- 3 Select one of the following video streams to view:
 - **Live:** Default stream used for viewing live video.
 - **Recording:** Stream recorded by the Archiver for future investigation.
 - **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.
 - **Automatic:** Security Desk uses the *Low resolution* or *High resolution* stream, depending on the size of the tile.

Related Topics

[Tile menu commands](#) on page 20

Zooming in and out of video

To get a better view of the finer details of what you are monitoring, you can zoom in on the live or playback video that is displayed in a tile, regardless of whether you are using fixed cameras or PTZ cameras.

What you should know

If the default video stream of the camera is set to *Automatic*, the video stream switches to high resolution when you apply digital zoom.

To zoom in and out of tile content:

- 1 Select a tile that is displaying live or playback video.
- 2 Do one of the following:
 - Click and drag your mouse to create your desired zooming area (blue rectangle), and then release the mouse button. This method does not work with PTZ cameras.
 - Scroll your mouse wheel forwards to zoom in and backwards to zoom out. With PTZ cameras, this method only works once you apply the digital zoom.
 - In the camera widget, click **Toggle digital zoom** (🔍).
 - Right-click in the tile and click **Camera > Toggle digital zoom** (🔍).

A zoom thumbnail of the full image appears in the upper-left corner of the tile, and the zoom level is displayed in the tile.

- 3 In the zoom thumbnail, you can do the following:
 - Click and drag the red box to reposition the zoom area.
 - Click and drag the mouse cursor on the zoomed-in image to reposition the zoom area.
 - Use the slider to increase and decrease the zoom level.
- 4 To stop zooming, click **Toggle digital zoom** (✖) in the camera widget.

Related Topics

[Customizing video stream options](#) on page 202

[Video options](#) on page 203

Creating digital zoom presets

When you zoom into a camera image in a tile, you can create digital zoom presets for areas of interest in the image.

What you should know

You can create as many presets as you want. Digital zoom presets are not supported on PTZ cameras.

To create a digital zoom preset:

- 1 Apply a digital zoom method to an image displayed in a tile.
- 2 In the camera widget, click **Add** (+).
- 3 In the *Create preset* dialog box, type a name for the digital zoom preset and then click **Create**.

A preset is created for the current camera image position. You can now zoom to the preset by selecting it from the **Digital zoom presets** drop-down list in the camera widget.

- 4 If you move the camera image, you can click **Preset** (👁) to return to the preset position.
- 5 In the **Digital zoom presets** section, click the drop-down arrow beside **Preset** (👁) for the following additional preset options:
 - **Save:** Save the preset selected in the drop-down list, using the current PTZ position.
 - **Delete:** Delete the preset.
 - **Add preset:** Create a new digital zoom preset.

Related Topics

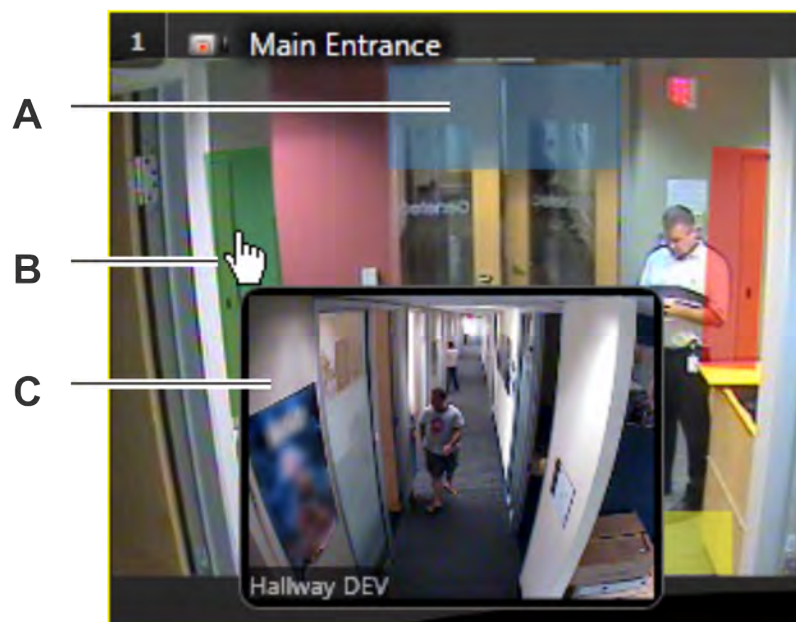
[Zooming in and out of video](#) on page 139

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.

Tracking moving targets

You can follow an individual or object that is moving across different cameras from the same canvas tile, using the visual tracking feature.

Before you begin

- Make sure that visual tracking is supported on all cameras using this feature.
- Configure visual tracking in Config Tool (see the *Security Center Administrator Guide*).

What you should know

Visual tracking works with both live and playback video.

To track a moving target:

- 1 Select a tile displaying video.
- 2 To enable visual tracking for that tile, do one of the following:
 - In the camera widget in the dashboard, click **Enable visual tracking** (👁️).
 - Right-click in the tile, and click **Camera > Enable visual tracking** (👁️).
 - On your keyboard, press **Alt+F**.
- 3 As the subject moves out of the camera's field of view, click the zone (colored overlay) representing a link to the next camera.

Hovering your mouse pointer over the zone gives you a preview of the image from the next camera.

Adding bookmarks to video sequences

If you see something worth noting, you can add a bookmark to the video you are viewing.

What you should know

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. If a camera is not currently recording, adding a bookmark forces it to begin recording.

To add a bookmark to a video sequence:

- 1 In the camera widget, click **Add a bookmark** (🔖).
- 2 (Optional) In the **Add a bookmark** dialog box, type a short text in the **Message** field.
The timestamp of the bookmark is fixed at the **Time** indicated in the dialog box.
- 3 (Optional) Protect the video sequence containing the bookmark against routine archive cleanup as follows:
NOTE: You can only protect the video sequence if the bookmark is added to a local (non federated) camera.
 - a) Select the **Protect video from deletion** option.
 - b) In the *Protect archives* dialog box, set the start time and end time of the video sequence to protect, and the duration.

By default, the protected sequence starts one minute before your bookmark and ends 4 minutes after. The default duration of the protection is 5 days.
 - c) Click **Protect**.
- 4 If you did not select the **Protect video from deletion** option, click **OK** to add the bookmark, or click **Cancel** to exit without adding a bookmark.

Leaving the **Message** field blank does not cancel the action.

Related Topics

[Overview of the Bookmarks task](#) on page 459

Viewing bookmarked videos

To view a sequence of video that was previously bookmarked, you can generate a report of the all the stored bookmarks in the *Bookmarks* task.

To view bookmarked video:

- 1 From the home page, open the Bookmarks 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 has been made visible to you when it was created or last configured.

- **Message:** Enter any text you want to find in the bookmark. A blank string finds all the bookmarks.
 - **Time range:** The time range for the report.
- 3 Click **Generate report**.
The bookmarks appear in the report pane. If your query does not generate a result, a warning message appears.
 - 4 To view the video associated with a bookmark, drag the bookmark from the report pane to a tile in the canvas.

Customizing snapshot options

Before taking snapshots of video, you can choose the file format and folder location of your saved snapshots.

What you should know

- The **Write camera name and timestamp** option is saved as part of your Security Center user profile. The other snapshot settings are saved locally for your Windows user profile.

IMPORTANT: Snapshots are saved in the same folder as exported video files. If you change the folder location, existing video and snapshots can no longer be viewed from the *Vault* tool.

- When you export a snapshot, the system can include additional file information (for example, camera name, creation date, camera coordinates) which can be useful during incident investigation. To view additional file information, right-click on a file in the *Vault* and select **Show properties**.

IMPORTANT: The system only includes this additional file information if an administrator enables the feature in your user settings.

To customize snapshot options:

- 1 From the home page, click **Options > Video**.
- 2 In the *Video options* page, set the following options:
 - **Location:** The windows folder path where exported video files and snapshots are saved. The default path (in Windows 7) is: *C:\Users\Username\AppData\Local\Genete Security Desk version#\Vault*.
 - **File format:** Choice of supported file formats: *.bmp, .jpg, .png, .gif*. The default format is **.png*.
 - **Write camera name and timestamp:** The date, time, and camera name is stamped on the snapshot image.
- 3 Click **Save**.

Taking snapshots of video

Whether you are viewing live or playback video in a tile, you can save the current video frame as an image file, and then organize and share all files using the *Vault* tool.

Before you begin



[Set your snapshot options.](#)

What you should know



- All snapshots are saved with the following naming convention: *CameraName (Date Time).png*. By default, snapshots are saved in *.png format in the following location: *C:\Users\Username\AppData\Local\Genete Security Desk version#\Vault*.
- When you export a snapshot, the system can include additional file information (for example, camera name, creation date, camera coordinates) which can be useful during incident investigation. To view additional file information, right-click on a file in the *Vault* and select **Show properties**.

IMPORTANT: The system only includes this additional file information if an administrator enables the feature in your user settings.

To take a snapshot of video in a tile:

- 1 Select the tile that is displaying the video image you want to save as a snapshot.
- 2 Do one of the following:
 - In the camera widget on the dashboard, click **Save a snapshot** (.
 - Right-click in the tile, and click **Camera > Save a snapshot** (.

A thumbnail preview is displayed in the upper-right corner of your Security Desk window for two seconds.

- 3 To open the Vault, from the home page, click **Tools > Vault**.
Thumbnails of all snapshots are displayed in the Vault.
- 4 To [edit a snapshot](#), do one of the following:
 - Select the snapshot and click **Edit** (.
 - Right-click the snapshot and click **Edit**.
- 5 To print a snapshot, do one of the following:
 - Select the snapshot and click **Print** (.
 - Right-click the snapshot and click **Print**.
- 6 To delete a snapshot, right-click the thumbnail and click **Delete**.
If you delete the snapshots, the image files are no longer available.
- 7 To rename a snapshot, right-click the thumbnail and click **Rename**.

Related Topics

[Editing video snapshots](#) on page 147

Editing video snapshots

To ensure privacy or to hide elements of a video snapshot, you can use the editing tools in the video snapshot image editor.

Before you begin

Take a video snapshot.

What you should know

- Snapshots are stored in the [Vault](#).
- All snapshots are saved with the following naming convention: *CameraName (Date Time).png*. By default, snapshots are saved in *.png format in the following location: `C:\Users\Username\AppData\Local\Genetec Security Desk version#\Vault`.

To edit a video snapshot:

- 1 To open the Vault, from the home page, click **Tools > Vault**.
- 2 To open the *Image editor*, do one of the following:
 - Select the snapshot and click **Edit** (✎).
 - Right-click the snapshot and click **Edit**.

- 3 Edit the snapshot.

The image editor provides the following standard set of editing tools:

- Mask
 - TIP:** Using the **Mask** tool, you can hide or blur elements of the image.
- Rotate
- Flip
- Crop
- Transparency

- 4 Click **Save as** and save the edited snapshot.

IMPORTANT: If you need to keep the original snapshot, you must save the edited snapshot with a different file name.

Related Topics

[Taking snapshots of video](#) on page 146

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 blocking is particularly targeted for installations that provide the general public with access to live video. In such cases, cameras might be streaming video that is not suitable for certain users. As a result, you can restrict users from viewing a segment or entire video capture by blocking the camera.

How it works

Camera blocking is based on a user attribute called the user level. The highest user level is 1 and the lowest user level is 254. If you block a camera, users with a lower user level than the one that you select cannot view video (live, playback, or cached) or export video for the amount of time that you set.

When blocking cameras, the following applies:

- A user can only block someone that has a lower user level. As a result, users with a user level equal to 254 cannot block anyone, and users with a user level equal to 1 cannot be blocked by anyone.
- A user cannot unblock or change the blocking level of a camera if the camera was blocked by someone with a higher user level.
- A user with a user level that is higher than the blocking level of a camera can unblock the camera or change its blocking level. To change the blocking level, it is not necessary to unblock the camera first.
- If there are more than one block settings applied to a camera at the same time, the user level that was specified for block setting that was created last is the active blocking level.

Example

You block a camera from 1 P.M. to 4 P.M, and set a user level of 20. Another user blocks the same camera from 3 P.M. to 5 P.M., and sets a user level of 100. From 3 to 5 P.M., the blocking level is 100.

Related Topics

[Blocking users from viewing video](#) on page 149

Blocking users from viewing video

If something critical occurs during a video capture and it must not be made accessible to certain users, you can restrict users from viewing a segment or entire video capture by blocking the camera.

Before you begin

Do the following:

- Make sure you have the *Block and Unblock video* user privilege.
- Make sure that the camera you want to block is not from a federated Omnicast system.

What you should know

You can block a camera that is displaying live or playback video in a tile from any Security Desk task. For example, you can block a camera that is displaying live video from the *Monitoring* task, or block a video archive that is displaying playback video from the *Archives* task. Users with a lower user level than the one that you select cannot view video (live, playback, or cached) or export video for the amount of time that you set. If they try to view video from that camera during the blocked period, **Blocked** is displayed in the tile.

NOTE: In the *System status* task, you can block and unblock cameras, and view the current block status of a camera.

To block users from viewing captured video:

- 1 Select a camera displayed in a tile.
- 2 Right-click in the tile, and click **Camera > Block** (🔒).
- 3 In the **Start** option, select the date and time to start blocking the video.
- 4 In the **End** option, select the duration of video to be blocked:
 - **Until:** The video is blocked from users until the selected date and time.
 - **For:** The video is blocked from users for the selected time (days, hours, minutes, or seconds).
 - **Indefinitely:** All video from the **Start** time onward (including new recordings) is blocked from users until you manually unblock the camera.
- 5 From the **User level** slider, select a minimum user level.

All users with a user level lower than the one you select are blocked from viewing the video. The highest user level is 1 and the lowest user level is 254.

- 6 Click **OK**.

The camera is blocked to users that have a lower user level than the one that you selected. Users that have a higher or equal user level can see that the camera is blocked because dashes appear on the tile's timeline.

- 7 To unblock the camera, right-click inside the tile and click **Camera > Unblock** (🔓).

Related Topics

[Tile menu commands](#) on page 20

[Camera blocking](#) on page 148

[Monitoring the status of your system](#) on page 392

How video is displayed if the Directory role disconnects

The Security Center *Directory* role manages your entire system and without it you cannot log on to the system. If the server's Directory role is disconnected from the rest of the system, Security Desk starts to operate in a degraded mode.

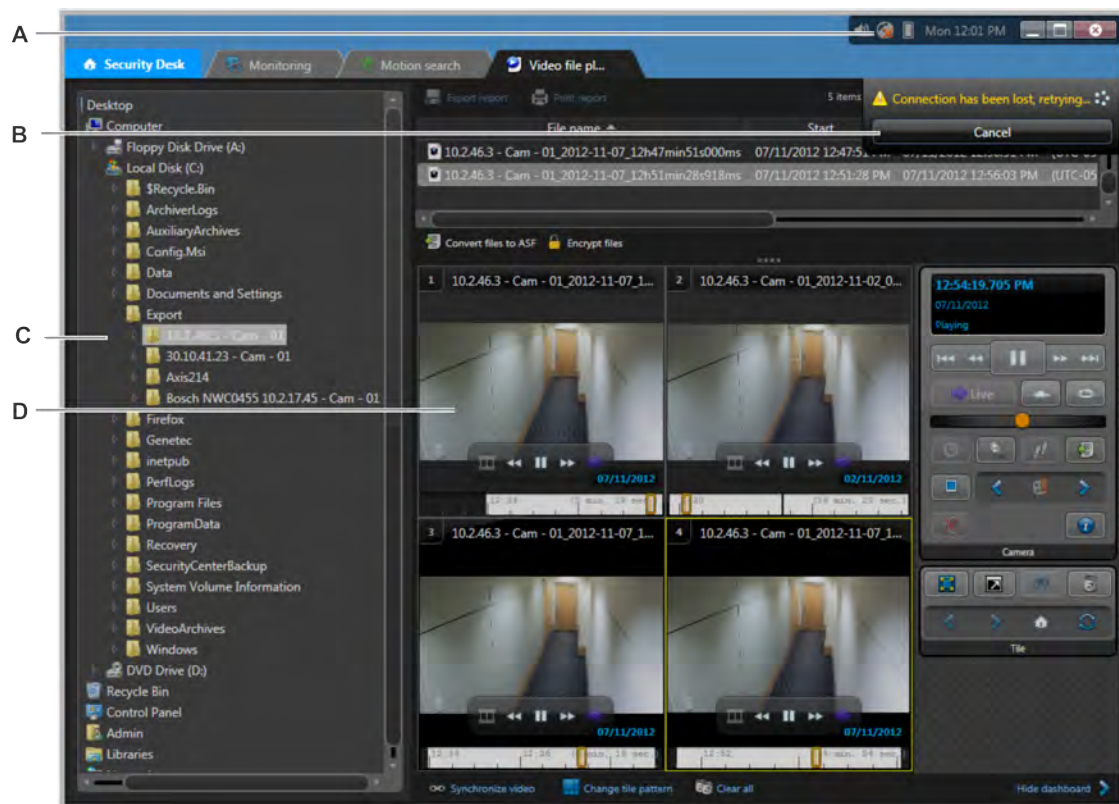
If you were viewing a camera, you remain connected to that camera's live video stream even after you are logged out of the system. You can also view playback video if the live video was cached to your local workstation. Cached video is indicated by the orange bar at the top of the timeline.

Video has not been cached

Video has been cached



Security Desk constantly attempts to reconnect to the Directory. Once reconnected, the operating mode reverts to normal. The following figure shows what the degraded mode looks like after a Directory failure.



A Connection state icon shows that you are disconnected

B Pop-up message appears indicating that the Security Desk is trying to reconnect

-
- C** The area view is unavailable
-
- D** Previously displayed cameras remain connected
-

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 has been 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.

Video archives

This section includes the following topics:

- ["Live and playback video modes"](#) on page 155
- ["Switching between video modes"](#) on page 157
- ["About the video timeline"](#) on page 159
- ["Creating a playback loop"](#) on page 160
- ["Viewing video archives"](#) on page 161
- ["Investigating Archiver events"](#) on page 163
- ["Searching video archives for motion events"](#) on page 164
- ["Searching video archives for camera events"](#) on page 167
- ["Preparing Bosch units to record video analytics events"](#) on page 168
- ["Searching for video analytics events stored on Bosch units"](#) on page 169
- ["Effects of Daylight Saving Time on video archives"](#) on page 171
- ["Changing the time zone to UTC"](#) on page 173

Live and playback video modes

When viewing a camera in the canvas, you can alternate between *live* and *playback* video modes from the timeline or from the camera widget in the dashboard.

The camera widget allows you to pause and rewind the video, or instantly replay the video if you missed something important. When you finish watching the replay, you can switch back to live video. When a camera is displayed, the current video mode is shown in the lower-right corner of the tile.

When you are viewing live video, the camera's current recording state is indicated:

- Red (**Live**) - The camera is currently recording.
- Green (**Live**) - The camera is currently not recording.

When you are viewing playback video, the date and time stamp of the recording is indicated. The date/time stamp can be displayed in absolute mode or relative mode. Click the date/time stamp to toggle between the two display modes.

- **Yesterday at 2:33 PM** Date/Time stamp overlay in *relative* mode.
- **28/08/2011 2:33:19.003 PM** Date/Time stamp overlay in *absolute* mode.

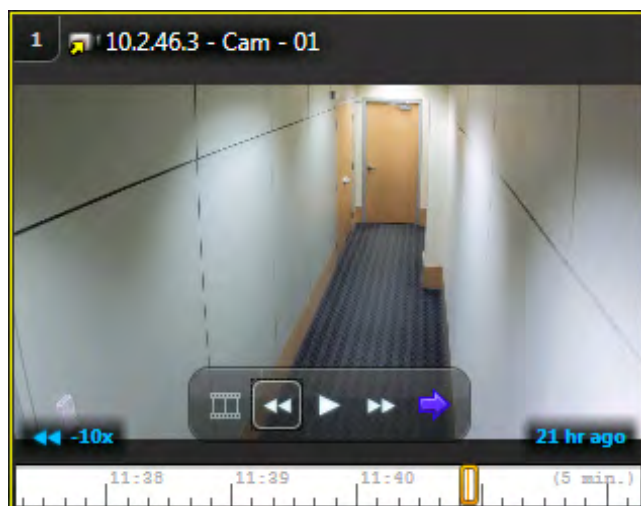
How the video mode is determined

If you decide to view another camera in the canvas, by default the video mode is inherited from the currently selected tile. For example, if the selected tile is displaying playback video, then when you add a camera into a new tile, it also displays playback video.





If the currently selected tile is not displaying a camera, the inherited video mode depends on the task type. The default video mode for *Monitoring* tasks is live video. The default video mode for investigation tasks is playback video.

Video playback states

When you are viewing playback video in a state other than normal playback (1x), a blue overlay appears on the lower-left corner of the image. In the following figure, the playback video is reversing at 10 times (10x) the normal speed.



Possible playback states

	Pause
	Slow motion playback
	Fast forward playback (2x, 4x, 6x, 8x, 10x, 20x, 40x, or 100x)
	Reverse playback (-2x, -4x, -6x, -8x, -10x, -20x, -40x, or -100x)

Related Topics

[Switching between video modes](#) on page 157

Switching between video modes

You can alternate between *live* and *playback* video modes from the timeline or from the camera widget in the dashboard.

What you should know

If the camera is not currently recording (indicated with the green **Live** overlay), the Archiver might not be available. However, even if the camera is not recording on the Archiver, the orange bar at the top of the timeline indicates the video that has been buffered locally on your hard drive. Locally buffered video is available for playback.

To switch video modes:

1 Switch to *playback* video mode one of the following ways:

- On the timeline, click and drag the playback cursor to the left.

TIP: The timeline scale can be adjusted by scrolling your mouse wheel while hovering your mouse pointer over it.

- To begin reverse playback, click **Rewind** (⏮) in the camera widget.

Successive clicks adjust the playback speed from -1x to -100x.

- To jump backwards in 15-second increments, click **Jump backward** (⏮) in the camera widget.

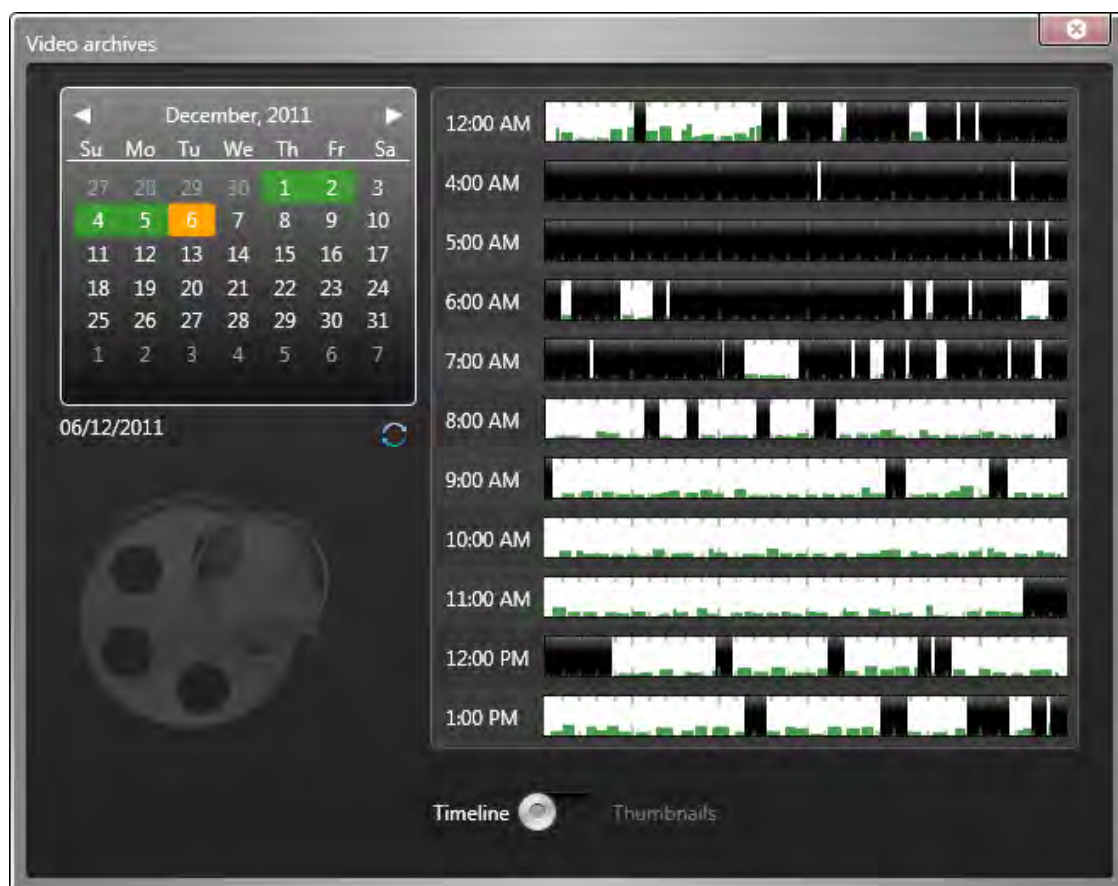
The seek value is 15 seconds by default. You can change this value in the Options dialog box.

- To jump to a specific time in the video playback, do the following:

1 In the camera widget, click **Go to specific time** (🕒).

2 In the *Video archives* dialog box, use the calendar to navigate through the months and years, and select a date.

The hours in the day that video archives are available on are shown on the right in a timeline and are indicated by a white background.



- 3 (Optional) Switch between Timeline and Thumbnails view.
 - 4 Click a position in the timeline to jump to that hour in the video recording.
- 2 Switch to *live* video mode one of the following ways:
- In the on-tile video controls, click **Camera > Switch to live** (➡).
 - In the camera widget, click **Switch to live** (➡ Live).

Related Topics

[Live and playback video modes](#) on page 155

[Video options](#) on page 203

About the video timeline

The timeline appears below the video image in canvas tiles.

With the video timeline you can do the following:

- Move the timeline window to the left or to the right by clicking on the timeline itself and dragging it either left or right.
- Shrink or widen the timeline by hovering your mouse pointer over the timeline and turning your mouse wheel.



A	White background indicates that a recording is present.
B	Black background indicates that no recording was made at that time.
C	Green motion-bars. The bigger the bar, the more motion is present.
D	Orange ribbon icon indicates the presence of a bookmark. Mousing over the bookmark displays the associated text and time stamp.
E	Orange bar at the top of the timeline indicates video that has been cached (buffered) on your workstation's hard drive.
F	Playback cursor. Drag cursor to playback a different point on the timeline.
G	Playback timestamp. Click to toggle between relative and absolute time.
H	Timeline duration/scale. Hover your mouse pointer and scroll the mouse wheel to zoom in or out on the scale of the timeline.
I	Purple background indicates the future.

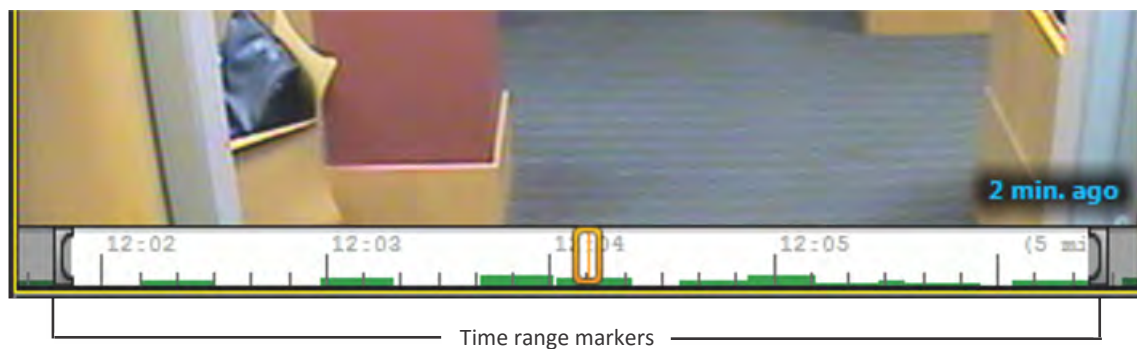
Creating a playback loop

To play the same sequence of video repeatedly, you can create a playback loop in the video timeline.

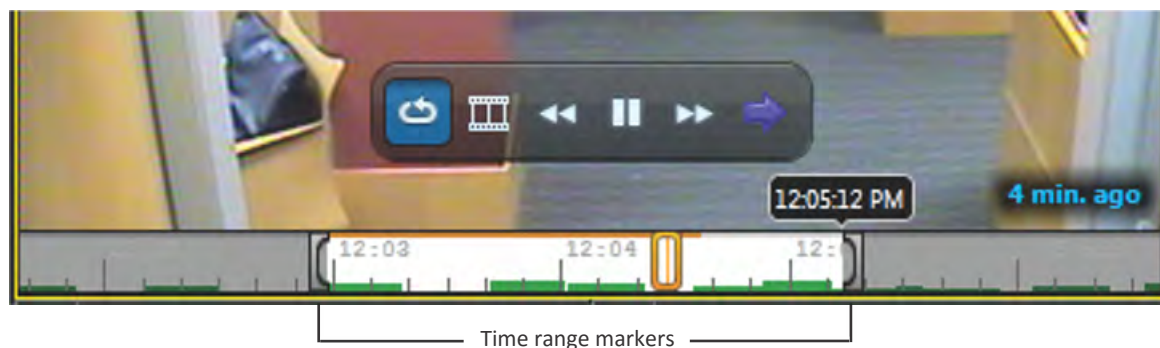
Do one of the following:

- In the camera widget, click **Loop playback** (↺).
- Right-click in the timeline.

Two time range markers appear on each end of the timeline.



Drag the markers to their desired positions. While you are holding a marker with your mouse, the exact time position of the marker is shown.



The playback loop starts instantly. While you are in a playback loop, all the playback controls remain available.

To cancel the playback loop, click **Loop playback** (↺) in the on-tile video controls or the camera widget.

Viewing video archives

You can find and view available *video archives* on your system by camera and time range, using the *Archives* report.

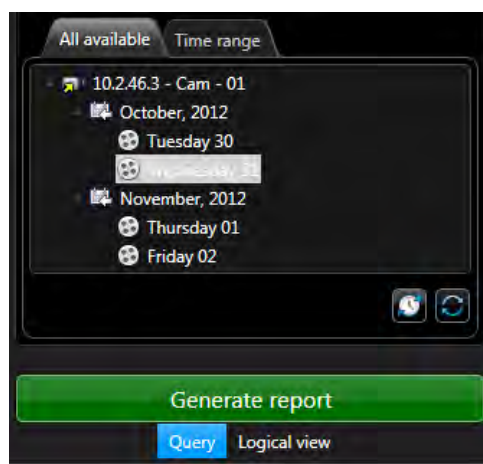
What you should know


In the Archives report, you can search for archived video sequences within a given time range or for a specific *camera* on a given date. For example, if an important security event occurs, you can search through the video archives to review the video recording, and then export it to share with colleagues or law enforcement.

If a Mobile app streamed live video to a Security Center camera that was recorded by an Archiver, you can view the playback video from that mobile stream by selecting the Archiver and the time range. For more information about streaming video to Security Center from Mobile apps, see the *Security Center Mobile Installation and Administration Guide*.

To view a video archive:

- 1 From the home page, open the **Archives** task.
- 2 In the *Filters* tab, do one of the following:
 - To search for archives by date:
 - 1 Click the **All available** tab, and then select a camera that you want to investigate. All days that include video archives for the selected camera are listed by month and day.



- 2 To show the time range for each day that video archives are found on, click .
- 3 Select a date.
- To search for archives by time range:
 - 1 In the **Cameras** filter, select the camera to investigate.
 - 2 Click the **Time range** tab, and set the time range.
- 3 Click **Generate report**.

The related video recordings are listed in the report pane, one of the following ways:

- If you searched by date, the hours in the selected day that video is available on are listed.
- If you searched by time range, only cameras with video archives are listed. The length of the listed video sequences corresponds to the specified time range.

The **Preview** column shows where video is available within the sequence for each camera.

- 4 To view the video sequence in a tile, double-click or drag an item from the report pane to the canvas.

The selected sequence immediately starts playing.

NOTE: If you get the message *No video available at this time*, verify the following:

- That you have a valid certificate if the video stream is encrypted.
 - That you have the right to see that particular camera. The camera can be blocked and require a special privilege to see its archives.
- 5 To control the video recording, use the camera widget.
 - 6 To export an important video archive, select the item in the report pane, and then click **Export** (📄).

Related Topics

[Exporting video](#) on page 179

[Camera widget](#) on page 34

[Overview of the Archives task](#) on page 461

Report pane columns for the Archives 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 have been made visible to you when they were created or last configured.
- **End time:** End of the time range, playback sequence, or video sequence.
- **Preview:** Timeline showing where video is available during the selected time range.
- **Start time:** Beginning of the time range, playback sequence, or video sequence.
- **Thumbnails:** Thumbnail images of the recorded video during the selected time range.

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 a time range of a 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 Archivars 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 has been 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 have been 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.

Searching video archives for motion events

You can search the video archives for *video sequences* that detect motion in specific areas of a camera's field of view, using the *Motion search* report.

To search the video archives for motion events:

- 1 From the home page, open the Motion search task.
- 2 In the *Filters* tab, select a camera from the drop-down list.

When a camera is selected, a preview image based on the default time range appears. If the selected camera does not support motion search, the message "Motion search not available for this camera" is displayed instead of the preview image.
- 3 To refresh the preview image based on the new time range, click .
- 4 To view a video instead of a still image, click .
- 5 Set the time range for the motion search.
- 6 To define a motion detection zone over the preview image, draw motion detection blocks (blue rectangles) on areas where motion is meaningful for the search, using the following tools:
 - 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.
- 7 To influence the speed and accuracy of the motion query, configure the motion detection criteria options as follows:
 - **Motion threshold:** Sets the minimum number of blocks that must be activated for a motion detection result to show up in the query. The total number of blocks in the motion detection zone is indicated as the maximum value allowed for the threshold. A value of zero means any motion detected in the defined zone would qualify for the search.
 - **Consecutive frame hits:** Applies the motion threshold to a specified number of video frames. This setting helps to avoid false-positive motion detection (for example, video noise in a single frame). It ensures that motion is detected when the threshold is met over a specified number of consecutive frames, not in a single frame.
 - **Minimum time between frames:** Controls the sampling rate for the search by telling the system not to examine every single video frame. The *higher* the value, the more frames the system skips during the search, thus performing the search faster. To examine every frame, set the value to 33 ms or less. The highest archiving frame rate is 30 frames/sec. At this rate, the time between two consecutive frames is only 33 ms.
- 8 Click **Generate report**.

The motion events are listed in the report pane.
- 9 To show the corresponding video of a motion event in a tile, double-click or drag an item from the report pane to the canvas.

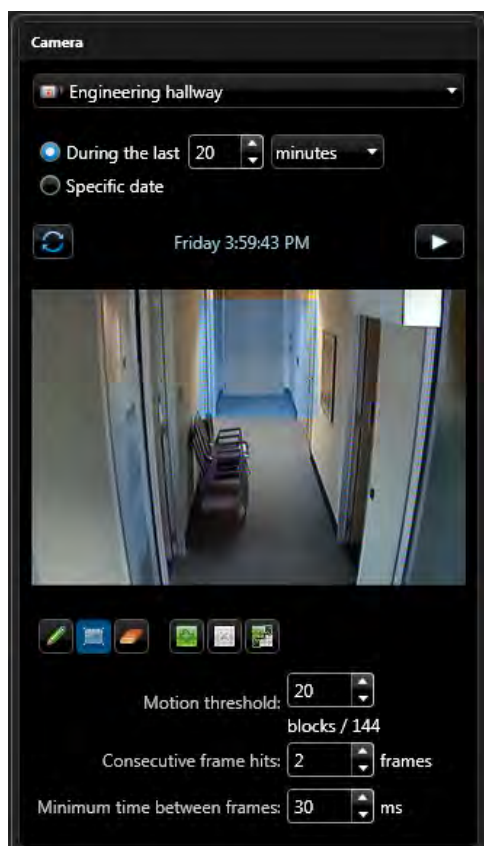
The selected sequence immediately starts playing.

10 To control the video recording, use the camera widget.

11 To export an important video archive, select the item in the report pane, and then click **Export** (📁).

Example

If you want to see the activity that happened around a specific door, you can search for motion using the camera that points at the door. In the following figure, a motion detection zone is defined by the entrance door. As a result, the search is targeted at the door and motion created by people walking farther down the hallway is ignored.



Related Topics

[Exporting video](#) on page 179

[Selecting date and time ranges for reports](#) on page 55

[Camera widget](#) on page 34

[Overview of the Motion search task](#) on page 462

Report pane columns for the Motion search 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 have been made visible to you when they were created or last configured.

- **End time:** End of the time range, playback sequence, or video sequence.
- **Source (entity):** The name of the system the camera belongs to.
- **Start time:** Beginning of the time range, playback sequence, or video sequence.

Searching video archives for camera events

You can find events related to selected cameras that were recorded by an Archiver, using the *Camera events* report.

What you should know

This report is helpful if you already know the name of the camera that you are looking for. You can see what events have been triggered from that camera. You can also investigate specific events. For example, recording that was started due to an alarm.

To receive results in your report, the video and analytic metadata must be recorded by an Archiver.

To search the video archives for camera events:

- 1 From the home page, open the **Camera events** 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 has been 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 camera events are listed in the report pane.
- 4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.
- 5 To control the video recording, use the camera widget.

Related Topics

[Camera widget](#) on page 34

Report pane columns for the Camera 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.

- **Archiver:** Archiver role name.
- **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 have been 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.

Preparing Bosch units to record video analytics events

Before you can search for video analytics events that were recorded on Bosch units using the Forensic search report, the units must be configured to record video locally, and the Bosch Video SDK must be installed on Security Desk workstations.

What you should know

For more information about installing or configuring Bosch video units, see the manufacturer documentation.

To prepare a Bosch unit to record video analytics events:

- 1 Install your Bosch video units on the network.
They must be devices that support Bosch IVA video analytics.
- 2 Use the unit's web interface to configure it to record locally on the device itself or on an iSCSI network drive.
- 3 Use the unit's web interface to configure the *Bosch IVA* video analytics.

NOTE: Bosch video units that support IVA analytics record both video images and raw, unprocessed metadata. This means that the analytic configuration can be changed at any time and used for historical searches. For example, if you initially configure your analytics for the event "*line crossed*" and you later decide to change the analytic configuration for the event "*loitering*", you can still search for the new analytic event.

- 4 Install the *Bosch Video SDK* on all Security Desk workstations that use the Forensic search task.
The installation files can be found in the `\Tools` folder of your Security Center installation package.
- 5 Add your Bosch video units (IP cameras or video encoders) in Security Center.
The Archiver must be connected to the device to send command and control signals to the video unit. However, since the unit records by itself, the Archiver only provides duplicate video recordings, and a perhaps a longer retention period for the archives. You can only search for video analytic events on video recordings that are stored on the camera. For information about adding video units in Security Center, see the *Security Center Administrator Guide*.

After you finish

[Search for video analytics events stored on Bosch units.](#)

Searching for video analytics events stored on Bosch units

You can search for video analytics events that are recorded locally on Bosch video units, using the *Forensic search* report.

Before you begin

[Prepare your Bosch units to record video analytics](#) so that the events are searchable using the Forensic search task.




What you should know

To receive results in your report, the video analytics must be performed by the video unit itself, and the video and analytic metadata must be recorded locally on the unit (Internal hard drive, USB hard drive, Compact Flash memory, or iSCSI connected drive).

To use the Forensic search report, you require the *Forensic search* license option. At this time, only Bosch video units running Bosch IVA analytics are supported with this report.

NOTE: To search for video analytics events that were recorded by an Archiver, then use the *Camera events* report instead

To search the archives for a video analytics event stored on a Bosch unit:

- 1 Open Security Desk on a workstation that has the *Bosch Video SDK* installed.
- 2 From the home page, open the **Forensic Search** task.
- 3 In the **Filters** tab, set the **Cameras** query filter to select a camera to investigate.
When a camera is selected, a live video preview is displayed.
- 4 To reset the forensic configuration, click .
- 5 To display or edit the forensic configuration, click .
- 6 Set the **Time range** query filter to select a time range for the report.
- 7 Click **Generate report**.
The video analytics events are listed in the report pane.
- 8 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.
- 9 To control the video recording, use the camera widget.
- 10 To export an important video archive, select the item in the report pane, and then click **Export** (.

Related Topics

[Exporting video](#) on page 179

[Selecting date and time ranges for reports](#) on page 55

[Camera widget](#) on page 34

Report pane columns for the Forensic search 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.

- **Algorithm ID:** Bosch forensic value. For more information, see the manufacturer documentation.

- **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 have been made visible to you when they were created or last configured.
- **End time:** End of the time range, playback sequence, or video sequence.
- **Event:** Event name.
- **Event type:** Bosch forensic value. For more information, see the manufacturer documentation.
- **Start time:** Beginning of the time range, playback sequence, or video sequence.
- **Track ID:** Bosch forensic value. For more information, see the manufacturer documentation.

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.

Video export

This section includes the following topics:

- ["Video export formats"](#) on page 175
- ["Configuring settings for exporting video"](#) on page 177
- ["Exporting video"](#) on page 179
- ["The Export video dialog box"](#) on page 182
- ["Viewing exported video files"](#) on page 184
- ["Sharing exported video files"](#) on page 187
- ["Converting video files to ASF or MP4 format"](#) on page 188
- ["Re-exporting G64 and G64x video files"](#) on page 190
- ["Viewing the properties of video files"](#) on page 192
- ["Protecting video files from being deleted"](#) on page 195
- ["Encrypting exported video files"](#) on page 197

Video export formats

The video export formats that are available in Security Desk determine the media player that is used to view the exported video files. You can export video in G64, G64x, ASF, and MP4.

G64x and G64 formats

The G64x and G64 formats are Security Center formats that support bookmarks, motion indicators, metadata overlays, and audio and date-time information. All event markers are included, except metadata markers. These formats also support variable frame rate and variable image resolution. G64x format also supports *watermarking*.

When you export multiple video sequences from the canvas simultaneously, they can be combined into a single G64x file. G64x files are also created when you export an incident package using incident recording in a tile. Depending on how you export the video, the video sequences are either played back in the same tiles that they were playing in when they were exported, or played back within a single tile, in the order that they were recorded.

NOTE: Federated Omnicast cameras cannot be exported in G64x format. If you select G64x format, the video sequences from federated Omnicast cameras are exported in multiple G64 files instead of the packaged G64x file.

You need Security Desk or the Genetec Video Player to view G64x and G64 files.

ASF format

Advanced Systems Format (ASF) is a Microsoft proprietary data format. This format supports audio information and variable frame rate, but not metadata associated with the video sequence. Date and time information is also not supported, but it can be overlaid on the video images during the exporting process.

If the video sequence that you want to export uses multiple image resolutions (CIF, 2CIF, 4CIF, and so on), the exported video sequence follows the image resolution of the first frame rate in the source video sequence. In addition, metadata that is associated with the video sequence is not exported. You can use this format if you need to make a copy of a video recording to share with law enforcement, your legal department, or other members of your security team.

When you export multiple ASF video sequences from the canvas simultaneously, a single ASX file is produced so you can view the ASF files in the order they were recorded.

You need Windows Media Player to view ASF video files.

MP4 format

MP4 is a standard format that stores audio and video and can be played back on many media players such as Windows Media Player and QuickTime.

When you export multiple MP4 video sequences from the canvas simultaneously, an ASX file is produced so you can view the MP4 files in the order they were recorded.

Exporting to MP4 supports H.264 and MPEG-4 video, and AAC audio formats. Fusion stream encryption and overlays are not currently supported.

Related Topics

[Exporting video](#) on page 179

[Configuring settings for exporting video](#) on page 177

Watermarks with exported video files

Video sequences in Security Desk that are exported in G64x format are automatically watermarked if the original video was watermarked, which preserves the digital signature of the video file. When a video file's authenticity is protected through watermarking, it is eligible in court as proof of evidence.

Within a single video file, the watermarking must remain the same. If the watermarking changes in the middle of a sequence that is being exported, Security Desk closes the current video file that it is writing to and creates a new file to store the remainder of the video sequence.

In the Export dialog box, each broken section of the sequence indicates *Partial export*, and the last part of the sequence indicates *Successful*. Each new section that is created is inserted after the last one that was created for the same camera.

NOTE: G64, ASF, and MP4 formats do not support watermarking. However, watermarking is supported when exporting video from federated Omnicast cameras.

Configuring settings for exporting video

Before exporting video in Security Desk, you must choose where to save the exported video files and configure the settings for each export format.

What you should know

- When you export a G64x video, the system can include additional file information (for example, camera name, creation date, camera coordinates) which can be useful in incident investigation. To view additional file information, right-click on a file in the *Vault* and select **Show properties**.
- **IMPORTANT:** The system only includes this additional file information if an administrator enables the feature in your user settings.
- **IMPORTANT:** Exported video files are saved in the same folder as snapshots, and are available from the *Vault* tool. If you change the folder location, existing video and snapshots can no longer be viewed from the Vault.

To set default settings for exporting video:

- 1 From the home page, click **Options > Video**.
- 2 In the **Vault** section, select a location from the following field:
 - **Location:** The windows folder path where exported video files and snapshots are saved. The default path (in Windows 7) is: `C:\Users\Username\AppData\Local\Genete Security Desk version#\Vault`.
- 3 In the **Export** section, select a **Default File format** for exporting video:
 - **G64:** A Security Center format that can be played back in Security Desk or the Genetec Video Player.
 - **G64x:** A file that contains multiple G64 files that can be played back in Security Desk or the Genetec Video Player.
 - **ASF (Advanced Systems Format):** A Microsoft proprietary data format that can be played back in Windows Media Player.
 - **MP4:** A standard format that stores audio and video and can be played back on multiple media players such as Windows Media Player and QuickTime.
- 4 Click Advanced (⊕) and set the following options:

The options vary depending on the file format you choose.

Option	Description	Format
Encrypt files	Turn this option on to set a password on the exported video files. Specify a password in the Encryption key field. Turning this option on converts the exported video files into GEK format, which you must decrypt before viewing.	G64x, G64

Option	Description	Format
Use following profile	Select the compression profile. The bit rate (shown in brackets) indicates the quality of the exported video. The higher the bit rate, the better the quality and the larger the file size. The Description under the profile provides useful information to guide your choice.	ASF
Export audio	Turn this option on to include audio information in ASF and MP4 files.	ASF, MP4
Display date and time on video	Turn this option on to have the date and time overlaid on the exported video image.	ASF
Delete intermediary files	Turn this option on if you want to delete the original files after they are converted into ASF, MP4, or GEK (encrypted) files.	ASF, MP4

5 Click **Save**.

Related Topics

[Video export formats](#) on page 175

Exporting video

To create stand-alone *video files* in Security Desk that can be played without being connected to the Security Center *Directory*, you can export video from any task in Security Desk that is displaying a playback video sequence in the canvas.

Before you begin

- [Configure the settings for each export format.](#)
- Make sure that you have the *Export video* user privilege.

What you should know

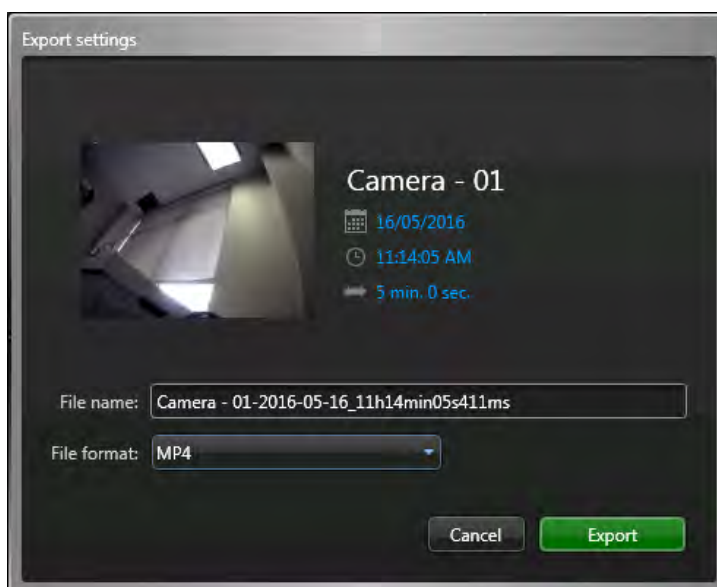
- Video export formats determine the media player that is used to view the exported video files. You can export video in the following formats:
 - G64x
 - G64
 - ASF
 - MP4
- If another export process is currently running, your export is queued and starts when the current export has finished.
- When you export a G64x video, the system can include additional file information (for example, camera name, creation date, camera coordinates) which can be useful in incident investigation. To view additional file information, right-click on a file in the *Vault* and select **Show properties**.

NOTE: The system only includes this additional file information if an administrator enables the feature in your user settings.



To export video:

- 1 Display playback video in the canvas.
- 2 Do one of the following:
 - Select an item in the report pane, and then at the bottom of the report pane, click **Export** (📄).
 - Right-click inside a tile, and then click **Camera > Export video**.
 - In the camera widget, click **Export** (📄).


When you click **Export** from the camera widget, you have the the option of exporting video from the selected tile or from all tiles.



- 3 To set the date, time, and duration of the selected video sequences, do the following:
 - a) Click the date, time, or duration setting.
 - b) In the timeline, drag the time range markers (⏮ ⏭) to the desired length of time.
 - c) To set the date and time range, click the date-time widget.
- 4 (Optional) In the **File name** field, type a name for the video file.
By default, the file name includes the camera name, the date, and the duration of the video sequence.
- 5 From the **File format** drop-down list, select one of the following export formats:
 - **G64**: A Security Center format that can be played back in Security Desk or the Genetec Video Player.
 - **G64x**: A file that contains multiple G64 files that can be played back in Security Desk or the Genetec Video Player.
 - **ASF (Advanced Systems Format)**: A Microsoft proprietary data format that can be played back in Windows Media Player.
 - **MP4**: A standard format that stores audio and video and can be played back on multiple media players such as Windows Media Player and QuickTime.
- 6 (Optional) If you selected the G64x format you can enter a **Description** for the exported video. The **Description** is listed when generating an Audit trails report, as well as when you right-click on the file in the Vault and select the **Show properties** option.
NOTE: The **Description** field is only available if the **Include additional properties on export/snapshot** option is enabled on the **Advanced** tab for a user in Config Tool.
- 7 (Optional) If you are exporting video from all tiles (G64x, ASF, and MP4), do the following:
 - a) (G64x only) Select a **Playback mode**.
 - **All at once**: Play back the sequences in the same tiles that they were displayed in when they were exported.
 - **Sequential**: Play back the video in sequence within a single tile.

b) To change the play back order of the video sequences, select a video sequence, and use the  and  buttons.

8 Click **Export**.

The export progress is shown in the notification tray (). To view the current progress or troubleshoot exporting errors, click **More** or **Show details** to open the *Export* dialog box.

When the export is complete, the video files are created in the export folder that you specified, and the files are available in the Vault.

After you finish

Do one of the following:

- [Play your exported G64 and G64x video files on your local computer.](#)
- [Copy the exported video files so that you can share them on another computer.](#)

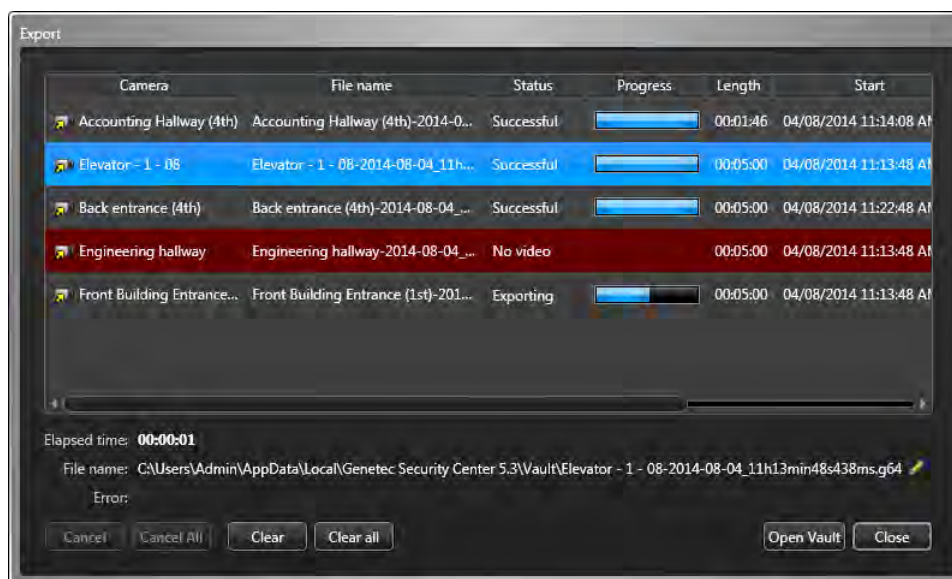
Related Topics

[Video export formats](#) on page 175

The Export video dialog box

The Export video dialog box opens when you are exporting video from any task in Security Desk that is displaying a playback video sequence in the canvas.

The figure that follows shows the Export video dialog box during the exporting video process.



The Export dialog box displays the following information about the export progress:

- **Camera:** Camera name.
- **File name:** Name of the file being exported.
- **Status:** The export status, which can be one of the following:
 - **Queued:** The export operation is queued, but has not started.
 - **Exporting:** The export is in progress. The progress is indicated by the number of bytes transferred.
 - **Converting:** If you chose to encrypt the video file or export in ASF format, this step comes after the **Exporting** step. The progress is indicated by the percentage of work completed.
 - **No video:** There is no recorded video from that camera for the selected time period.
 - **Partial export:** The export has to be aborted due to some unexpected problem. Click on the sequence to see a description of the problem in the Status field found at the bottom of the dialog box. When this happens, the remainder of the video is exported to a separate video file.
 - **Archiver server not running:** The Archiver that manages the selected video sequence is not running.
 - **Cancelled:** The export operation has been cancelled by the user.
 - **Successful:** The complete video sequence has been exported successfully.
 - **Error occurred:** The export operation failed. Click the sequence to see why the export failed in the Error field found at the bottom of the dialog box.
- **Progress:** The export progress
- **Length:** Total length of the video file.
- **Start:** Start time of the video sequence contained in the file.

- **End:** End time of the video sequence contained in the file.
- **Source:** The archiving source of the video sequence.
- **Elapsed time:** The total elapsed time since the export operation started.
- **File name:** Name of the file being exported. You can click **Rename** (✎) to edit the filename.
- **Error:** The error message explaining why the selected export failed or was aborted (partial export).
- **Cancel:** Interrupt the export before it completes. If the operation already started, the partial sequences that were already exported are saved as video files.
- **Cancel all:** Interrupt the export of all remaining video files. The sequences that were already exported (marked as *Successful*) are saved as video files.

Viewing exported video files

You can use the Vault tool in Security Desk to play back your exported video files on your local computer.

What you should know

- If you exported multiple video sequences simultaneously as a G64x file, they are either played back in the same tiles that they were displayed in when they were exported, or played back sequentially within a single tile.
- If you changed the save location of exported video files, files that were exported to the original location can no longer be viewed from the Vault. You cannot drag a video file from Windows into the Vault.
- ASF files can only be viewed in Windows Media Player.
- MP4 files can be viewed in many media players such as Windows Media Player and QuickTime.
NOTE: Some media players require a specific codec to be installed in order to play the file correctly.
- When you export a G64x video, the system can include additional file information (for example, camera name, creation date, camera coordinates) which can be useful in incident investigation. To view additional file information, right-click on a file in the *Vault* and select **Show properties**.
IMPORTANT: The system only includes this additional file information if an administrator enables the feature in your user settings.

To view an exported video file from the Vault:

- 1 From the home page, click **Tools > Vault**.
The Vault displays all exported files.
- 2 If you want to view an encrypted GEK file, you must first decrypt it as follows:
 - a) Select the encrypted video file, and click **Decrypt file** (🔓).
 - b) In the **Destination** field, use the default path if you want to be able to access the file from the Vault.
 - c) In the **Encryption key** field, type the password that was specified when the file was encrypted or exported, and then click **Decrypt**.
- 3 Do one of the following:
 - To view a video file in the Security Desk canvas, drag the file into the canvas.
The video starts playing. You can control the playback using the camera widget.
 - To view a video file in the Genetec Video Player, double-click the file.
 - To view an ASF or MP4 file, double-click the file.
The file opens in the media player you have installed on your system.

To view exported video files from the Genetec Video Player:

- 1 From the home page, click **Tools > Genetec Video Player**.
- 2 Do one of the following:
 - Drag the video file you want to view into the Genetec Video Player.
 - Click **File > Open file**, and then select the video file to view.

The video starts playing. You can control the playback using the commands at the bottom of the window.

Related Topics

[Camera widget](#) on page 34

Viewing exported files in the Video file explorer

Using the *Video file explorer* task, you can search for and play exported G64 and G64x *video files* and check whether they are authentic.

What you should know

You do not have to be logged on to Security Center to use the Video file explorer task. This is helpful if you need to view an important video file but cannot log on.

TIP: Double-clicking an exported file in Windows Explorer automatically opens a new *Video file explorer* task in Security Desk. You can also drag a file from Windows Explorer directly to a tile in Security Desk.

To view an exported video file in the Video file explorer:

- 1 From the home page, open the Video file explorer task.
- 2 In the *Selector*, select a folder.

If the folder contains video files, they are listed in the report pane with the following information:

- **File name:** Name of the video file.
 - **Camera:** Name of camera the video was taken from.
 - **Start:** Start time of the video sequence contained in the file.
 - **End:** End time of the video sequence contained in the file.
 - **Time zone:** Time zone of the camera.
 - **Length:** Length of the video sequence (**End time** minus **Start time**).
 - **File size:** Size of the video file.
 - **Watermark:** Indicates whether the video file is watermarked.
 - **Encryption:** Indicates whether the video file is encrypted. If the file is encrypted, you must decrypt it before you can view it.
- 3 Double-click or drag a video file from the report pane to the canvas.

The selected sequence starts playing immediately, and the file name and playback timestamp are displayed. The time in the timeline always represents the local time of the recorded video.

NOTE: You cannot switch to live video when you are viewing an exported file, because Security Desk does not know which camera the file is associated with.



Related Topics

[Overview of the Video file explorer task on page 464](#)

Sharing exported video files

To share your exported G64 and G64x video files with someone who does not have Security Desk installed, you can package the files with the Genetec Video Player, and then copy them to a CD, DVD, or USB.

What you should know

To share ASF or MP4 files, you copy the files onto a CD or DVD.

To share an exported video file:

- 1 From the home page, click **Tools > Vault**.
- 2 Select the video file, and click **Package with Genetec Video Player** (🌐).
- 3 In the **Destination** field, select where to save the files and the *Genetec Video Player.exe*.
- 4 Click **Package**.
- 5 Navigate to the folder where you saved the files, and then copy all the files onto a CD, DVD or USB.

Converting video files to ASF or MP4 format

Security Desk enables you to convert previously exported G64 or G64x video files to ASF or MP4 format so they can be viewed using Windows media players.


Before you begin

[Configure your video export settings](#)

What you should know


Video files exported in *ASF* or *MP4* format can be viewed using software such as Windows Media Player. You do not need Security Desk installed. This is helpful if you need to make a copy of a video recording to share with law enforcement, your legal department, or other members of your security team.

To convert a video file to ASF or MP4 format:

- 1 From the home page, do one of the following:
 - Click **Tools > Vault**.
 - Open the **Video file explorer** task, and select the folder that contains the video file to convert.
- 2 Select the video file, and click the **Save as** button (.

NOTE: To select multiple video files, hold the **CTRL** or **SHIFT** keys.

- 3 In the **Save as** dialog box, you can type a new **File name**, or leave the existing one.
- 4 From the **File format** field, choose **ASF** or **MP4**.
- 5 Click **Save** to start the conversion.


TIP: You can check the progress of the conversion at any time by double-clicking the **Video conversion** () icon in the notification tray.

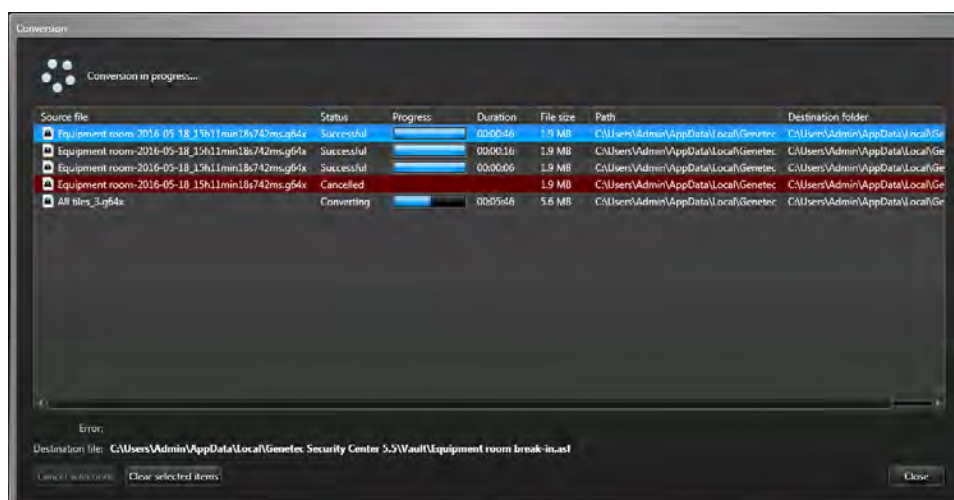
Related Topics

[Video export formats](#) on page 175

Conversion dialog box

In Security Desk, you can monitor the conversion status of G64 and G64x video files to ASF or MP4 formats from the *Conversion* dialog box.

You can open the **Conversion** dialog box by double-clicking the **Video conversion** () icon in the notification tray.



The dialog box shows both the conversion queue (files waiting to be converted) and the conversion log (files that have already been converted). Each file is identified by its **File name**, the conversion **Status**, a **Progress** indicator, the **Duration** of the conversion, the original **File size**, the file **Path**, and the **Destination folder** for the converted file. The converted file keeps the name of the original file, but uses the **ASF** extension.

The possible conversion statuses are the following:

- **Queued:** The file is waiting to be converted.
- **Converting:** The conversion is in progress. The progress of the conversion is indicated in the **Progress** column.
- **Successful:** The conversion has been completed successfully. The time the conversion took is indicated in the **Duration** column.
- **Error occurred:** The conversion failed. Select the file to see the reason of the failure in the **Error** field below.
- **Cancelled:** The conversion has been cancelled by the user. If the conversion was cancelled after it started, the conversion time is indicated in the **Duration**.

The action buttons found in the dialog box are the following:

- **Clear selected items:** Deletes the selected items from the conversion log. Only conversions that are **Successful**, **Failed**, and **Cancelled** can be removed from the log. The conversion log is lost when you exit Security Desk.
- **Cancel selections:** Cancels the selected items from the conversion queue. Only conversions that are **Queued** or **Converting** can be cancelled. When you cancel a conversion that has already started, the portion that has already been converted is saved.
- **Close:** Closes the conversion monitoring dialog box. The conversion process continues in the background. Closing this dialog box allows you to add more files to the conversion.

Re-exporting G64 and G64x video files

Previously exported G64 and G64x files can be re-exported to create new files in Security Desk. This is useful when you want to focus on a specific segment of the previously exported video, because you can define a start and end time for the new export. You might also want to save the file in a different format. You can re-export a video file from a Security Desk tile or from the Vault.

Before you begin

- [Configure the settings for each export format.](#)
- Make sure that you have the *Export video* user privilege.

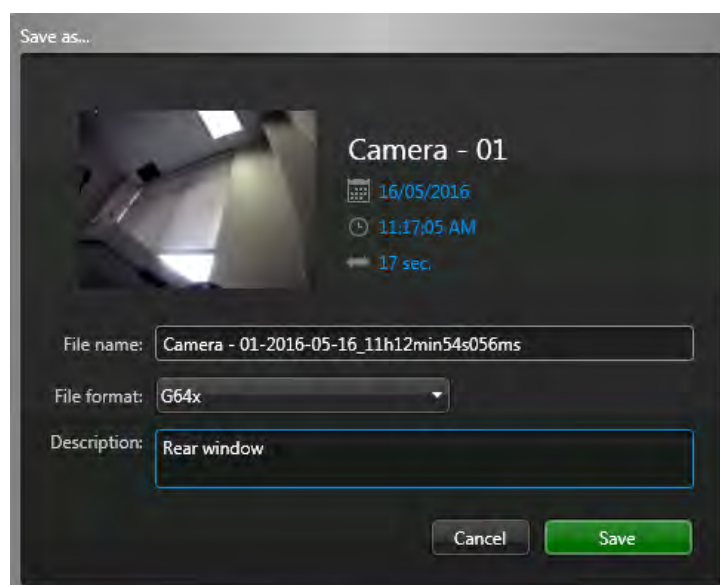
What you should know

- If another export process is currently running, your re-export is queued and starts when the current export has finished.


To re-export video:

- 1 Do one of the following:
 - Open a previously exported video file in a Monitoring task tile.
 - Open the Vault tool and select the file you want to re-export.
- 2 If you are re-exporting the file in a Monitoring task tile, do one of the following:
 - Right-click inside the tile, and then click **Camera > Save as**.
 - In the camera widget, click **Save as** (📁).
- 3 If you are re-exporting the file from the Vault, select the file and click **Save as** (📁).
- 4 In the **Save as** dialog box, do the following:
 - a) Click either the date, time, or duration setting.

NOTE: These settings appear in blue.



- b) In the timeline that appears, drag the time range markers (⏮ ⏭) to the desired length of time.

- c) To set the date and time range, click the date-time widget.
- 5 (Optional) In the **File name** field, type a name for the video file.
By default the file name includes the camera name, the date, and the duration of the video sequence.
- 6 From the **File format** field, select one of the following export formats:
- NOTE:** G64x files cannot be re-exported to the G64 format.
- **G64:** A Security Center format that can be played back in Security Desk or the Genetec Video Player.
 - **G64x:** A file that contains multiple G64 files that can be played back in Security Desk or the Genetec Video Player.
 - **ASF (Advanced Systems Format):** A Microsoft proprietary data format that can be played back in Windows Media Player.
 - **MP4:** A standard format that stores audio and video and can be played back on multiple media players such as Windows Media Player and QuickTime.
- 7 (Optional) If you selected the G64x format you can enter a **Description** for the exported video. The **Description** is listed when generating an Audit trails report, as well as when you right-click on the file in the Vault and select the **Show properties** option.
- NOTE:** The **Description** field is only available if the **Include additional properties on export/snapshot** option is enabled on the **Advanced** tab for a user in Config Tool.
- 8 Click **Save**.
- The progress of the export is shown in the **Video conversion**  icon in the notification tray.
Once the export is complete, the file is available in the Vault.

After you finish

Do one of the following:

- [Play your exported G64 and G64x video files on your local computer.](#)
- [Copy the exported video files so that you can share them on another computer.](#)

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 has been 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 195

[Overview of the Archive storage details task](#) on page 466

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 have been 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.

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. For information about monitoring the disk space available for video files, see the *Security Center Administrator Guide*.

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.



- 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 information about archive storage, see the *Security Center Administrator Guide*.

- **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.

Encrypting exported video files

To protect your exported video files, you can encrypt them by setting a password. Selecting this option converts the exported video files into GEK format, which must then be decrypted before viewing.

What you should know

To view an exported video file that was encrypted, you must decrypt the file from the *Video file explorer* task. After decrypting a file, you can then view it in a tile and open it from the export file.

To encrypt an exported video file:

- 1 From the home page, do one of the following:
 - Click **Tools > Vault**.
 - Open the **Video file explorer** task, and select the folder that contains the unencrypted G64 video file.
- 2 Select the video file, and click **Encrypt files** (🔒).

NOTE: To select multiple video files, hold the **CTRL** or **SHIFT** keys.

- 3 In the *Encryption settings* dialog box, select a **Destination** folder.
- 4 In the **Encryption key** field, type a password and then click **Encrypt**.

A GEK video file is created, indicating that the video file is encrypted. In the Vault, the file is shown as encrypted.

Decrypting exported video files

To view exported video files in Security Desk or the Genetec Video Player that are encrypted (GEK files), you must decrypt them.

What you should know

If you try to open a GEK file from the Vault tool or from Windows file explorer, you are required to enter a password before viewing the video.

To decrypt an encrypted video file:

- 1 From the home page, do one of the following:
 - Click **Tools > Vault**.
 - Open the **Video file explorer** task, and select the folder that contains the encrypted GEK video file.
- 2 Navigate to the folder that contains the encrypted GEK video file, and select it from the report pane.
- 3 Select the encrypted video file, and click **Decrypt file** (🔓).
- 4 In the **Encryption key** field, type the password that was specified when the file was encrypted or exported, and then click **Decrypt**.

The video file is converted into a G64 or G64xfile. The video file can now be viewed in a Security Desk tile or the Genetec Video Player.

Video options

This section includes the following topics:

- ["Configuring joysticks"](#) on page 199
- ["Configuring CCTV keyboards"](#) on page 201
- ["Customizing video stream options"](#) on page 202
- ["Video options"](#) on page 203

Configuring joysticks

You can configure any joystick (or any game controller supporting at least one axis) attached to your computer, so you can control the camera display in Security Desk.

Before you begin

Connect a joystick to your computer.

BEST PRACTICE: Do not connect two joysticks of the same model. They are listed with the same name, and you might not know which one to select. Furthermore, you can only have one joystick active at a time.


What you should know

You can associate two different Security Desk commands to each button, one for the button down event, and another for the button up event. The *Up command* is optional. The number of buttons you can configure depends on the type of joystick that you have.

The **Joystick dead zone** option value determines the percentage of movement required on the joystick before the PTZ camera starts moving. When you bring the joystick back into the home position, this value determines how close to the home position the joystick needs to be for the PTZ to stop moving.

The joystick settings apply to the local Security Desk workstation for all users.



To configure a joystick:

- 1 From the home page, click **Options > Peripherals**.
- 2 Click the **Joystick** tab.
- 3 From the **Active joystick** drop-down list, select the brand and model name of your joystick.
You can click  at any time to refresh the list.

All axes supported by your joystick are listed below.

- 4 (Optional) To import a previously saved joystick configuration from a disk, click **Import**.
- 5 To map the joystick axis commands to the PTZ commands of your choice, do the following:
 - a) Select an **Axis** from the list.
 - b) From the drop-down list in the **Commands** column, select a PTZ command.
 - c) To invert the command, select the option in the **Invert** column.

Example: If you mapped the *Tilt* command to the Y axis, inverting the commands causes the camera to move up when you pull the joystick towards you, and down when you push the joystick away from you.

- d) To erase the selected command mapping, click **Clear** .
- 6 To map the joystick buttons to the Security Desk commands of your choice, do the following:
 - a) Select a *Button* in the list.
 - b) To associate a command to a button down event, select a command from the drop-down list in the *Down command* column.
 - c) To associate a command to a button up event, select a command from the drop-down list in the *Up command* column.
 - d) If the selected command requires an argument, such as selecting a PTZ preset, then enter it in the *Args* column field.
- 7 To erase the selected command mappings and start over, click **Clear** .

- 8 To set the threshold for registered movement in relation to the home position (idle zone), select a percentage value in the **Joystick dead zone** option.
- 9 To save the joystick configuration to disk, click **Export**.
- 10 Click **Save**.

Configuring CCTV keyboards

You can configure any CCTV keyboard (for example, the Axis T8310 Video Surveillance Control Board) attached to your computer, so you can control the camera display in Security Desk.

Before you begin

Connect a CCTV keyboard to your computer.

What you should know

After you connect to a CCTV keyboard, you can control PTZ monitors, switch between cameras, control playback, and so on, using the keyboard instead of your mouse.

The CCTV keyboard settings apply to the local Security Desk workstation for all users.

To configure a CCTV keyboard:

- 1 From the home page, click **Options > Peripherals**.
- 2 Click the **Keyboard** tab.
- 3 From the **Keyboard protocol** drop-down list, select the make and model of your CCTV keyboard.
- 4 In the **Serial port** section, configure the characteristics of the serial port where the CCTV keyboard is connected.

This section is only required for some CCTV keyboards. Follow the specifications of the keyboard manufacturer.

- 5 To automatically connect to the CCTV keyboard every time Security Desk starts up, select the **Connect to keyboard automatically** option.

If you clear this option, you'll have to connect the keyboard manually every time you want to use it.

- 6 Click **Connect**.

For some CCTV keyboards, the connection status is displayed in the **Keyboard status** section.

- 7 To disconnect the CCTV keyboard, from the home page, click **Options > Peripherals > Keyboard > Disconnect**.

Customizing video stream options

You can customize video stream options, such as the default video stream for viewing live video in the canvas, the default archiving source for viewing playback video, and when to receive messages about video streams, from the *Options* dialog box.

What you should know

The **Live stream** and **Playback source** options apply to the local Security Desk workstation for all users. The **Display a warning when stream selection is not automatic** option is saved as part of your user profile.

To customize video stream options:

- 1 From the home page, click **Options > Video**.
- 2 From the **Live stream** drop-down list, select the default video stream for live video.
 - **Live:** Default stream used for viewing live video.
 - **Recording:** Stream recorded by the Archiver for future investigation.
 - **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.
 - **Automatic:** Security Desk uses the *Low resolution* or *High resolution* stream, depending on the size of the tile.
- 3 From the **Playback source** drop-down list, select the default archiving source to view playback video from.
 - **Archiver:** Video that was recorded by the Archiver.
 - **Auxiliary Archiver:** Video that was recorded by the Auxiliary Archiver.
 - **Federation:** Video that was recorded on a federated system.
 - **Edge playback:** Video that was recorded on an edge recording unit.
- 4 Click the **User interaction** tab.
- 5 If you want to receive a warning message when the resolution of a displayed video image is too big for the tile, and the video stream selection is not *Automatic*, select the **Display a warning when stream selection is not automatic** option.

The message that appears says you should change the video stream to *Automatic*.
- 6 Click **Save**.

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.

Seek time options

Select the default values when seeking for live and playback video. These settings are saved as part of your user profile.

- **Playback offset:** When you view an event in a tile, this value determines how many seconds of video is played before the event occurred. The default playback offset value is 15 seconds. You can set the value from 0 to 90 seconds.

NOTE: If the *Time to record before an event* option in Config Tool has a lower value than the seek time, you might not receive any video. Ask your administrator for the *Time to record before an event* value. For more information, see the *Security Center Administrator Guide*.

- **Playback duration:** When you view an event in a tile, this value determines how many seconds of video is played. If you export the event, this value determines the length of the exported video sequence.
- **Jump backward/forward:** Determines the amount of time that a playback video recording jumps backwards or forwards when you click **Jump backward** (⏮) or **Jump forward** (⏭) in the camera widget.

Default options

Select the default values when playing video. These settings apply to the local Security Desk workstation for all users.

- **Live stream:** Video stream to request when playing live video.
- **Playback source:** The video source to prioritize when requesting playback video.
- **Show overlays:** Turn this option on to show video overlays by default.

Video cache options

The video cache is used to cache playback video streams received by Security Desk. Playback video is buffered before playback starts so that a sufficient length of video plays. The cache helps to reduce re-transmission of video, allows faster access to playback video, provides smoother reverse playback and additional playback speeds. The cache is emptied when you close Security Desk or logoff.

These settings apply to the local Security Desk workstation for all users.

- **Cache location:** Select the location where you want the cache to be stored. You can use the default folder provided by Windows or specify your own.
- **Maximum size:** Set a size for your cache.
- **Live video caching:** Live video streams are cached separately from playback video. When the cache location is unavailable, the live video is not affected.
- **Clear cache at logoff:** Turn this option on to clear the cache when you log off Security Desk.
- **Clear cache now:** Click to clear the cache now.

Advanced video settings

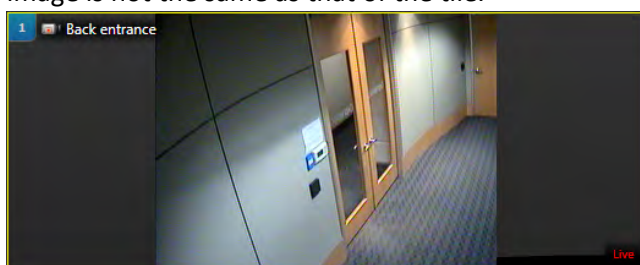
The advanced video settings apply to the local workstation and affect Security Desk and Config Tool for all users.

NOTE: After changing the Advanced setting options, you must restart Security Desk.

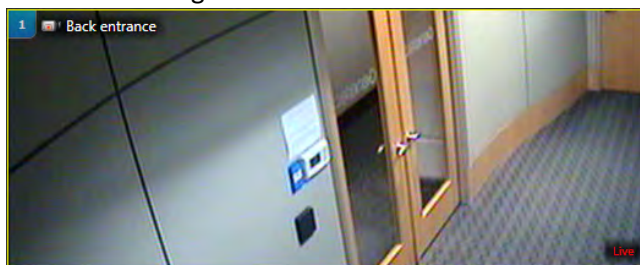
- **Jitter buffer delay:** The Jitter buffer prevents rendering issues with the video stream rendering issues caused by network latency variations, and provides smoother video in the event of irregular frame transmission from the source. It is recommended that the buffer size be kept at to a minimum to avoid side effects such as a time lag in PTZ manipulation or an increased delay when you start to view a video stream.
- **Enable deinterlacing:** Select this option to help reduce the jagged effect around straight lines during movement in interlaced video streams.
- **Enable video quality degradation:** Select this option to prevent Security Desk from using too much CPU on your computer by lowering the frame rate of the video displayed. When the CPU is above 90%, Security Desk lowers the frame rate of the video displayed in the canvas, starting from tile number 1. MJPEG video streams are reduced to 5 fps or lower, while video streams using other types compression are reduced by showing only key frames. The video tiles affected by this option are indicated with a flashing icon (🔴). To restore a video to its normal frame rate, clear the tile and restore its content (from the tile widget, click 🗑️ and click ↩️).

NOTE: Whenever you change the content displayed in the canvas, Security Desk restarts lowering the video frame rate from tile #1.

- **Camera tile:** Select how cameras are displayed in tiles.
 - **Display full image (boxed):** Black strips might appear around the image if the aspect ratio of the image is not the same as that of the tile.



- **Fill the tile (cropped):** The video image fills the tile. The image might be cropped if the aspect ratio of the image is not the same as that of the tile.



- **Audio mode:** Select the audio mode.
 - **Full-duplex:** Allows you to talk and listen at the same time.
 - **Half-duplex (push-to-talk):** Requires you to switch between talking and listening. When you click the *Talk* (🗨️) button in the camera widget, the *Listen* (👂) button is disabled until you release the Talk button. Half-duplex mode is necessary when two units are connected, or when audio must be controlled through digital inputs.

- **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](#).

Part III

Access control

This part includes the following chapters:

- Chapter 15, "[Access control at a glance](#)" on page 207
- Chapter 16, "[Cardholders and visitors](#)" on page 211
- Chapter 17, "[Credentials](#)" on page 250
- Chapter 18, "[Areas, doors, and elevators](#)" on page 271
- Chapter 19, "[Access control units](#)" on page 286

Access control at a glance

This section includes the following topics:

- ["About Synergis"](#) on page 208
- ["How access events are displayed in tiles"](#) on page 210

About Synergis

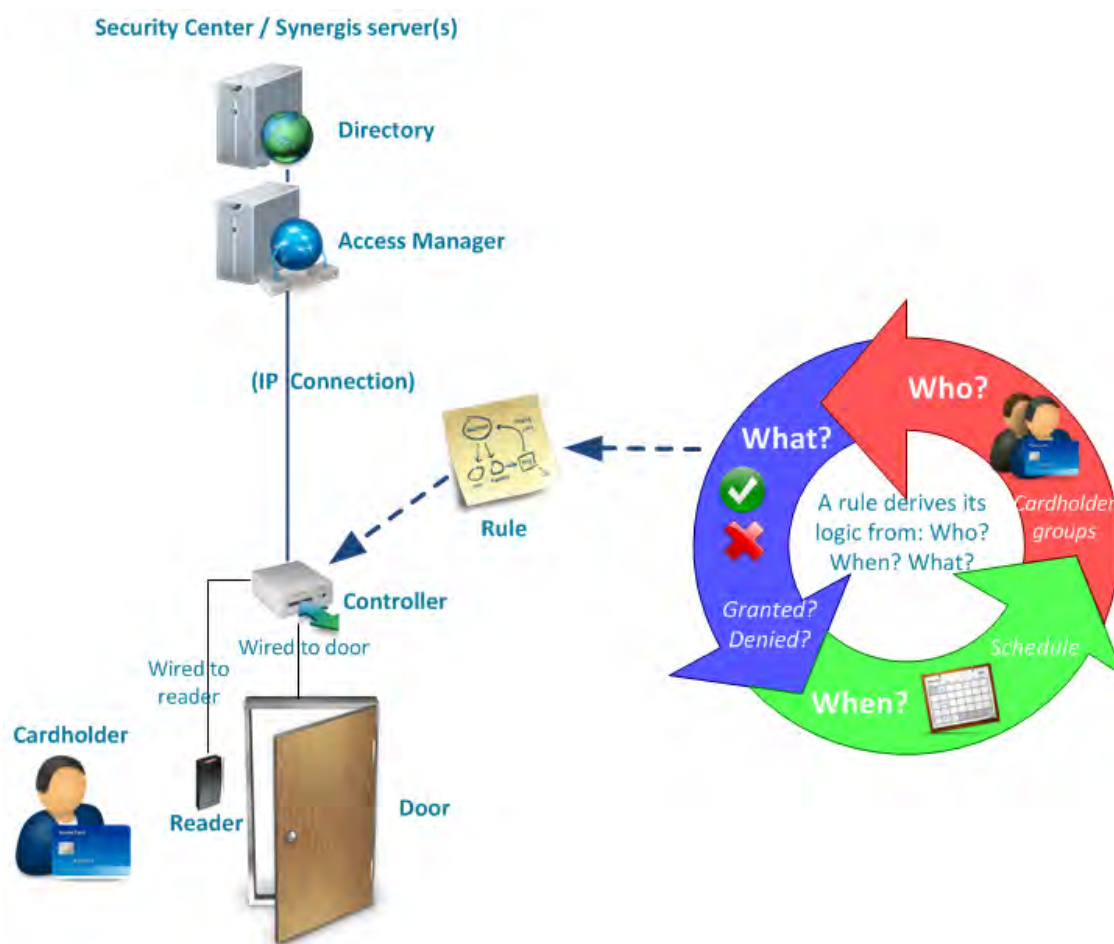
Synergis is the IP access control system of the Security Center designed to offer end-to-end IP connectivity, from access control reader to client workstation. Synergis seamlessly integrates a variety of access control capabilities including, but not limited to, badge design, visitor management, elevator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

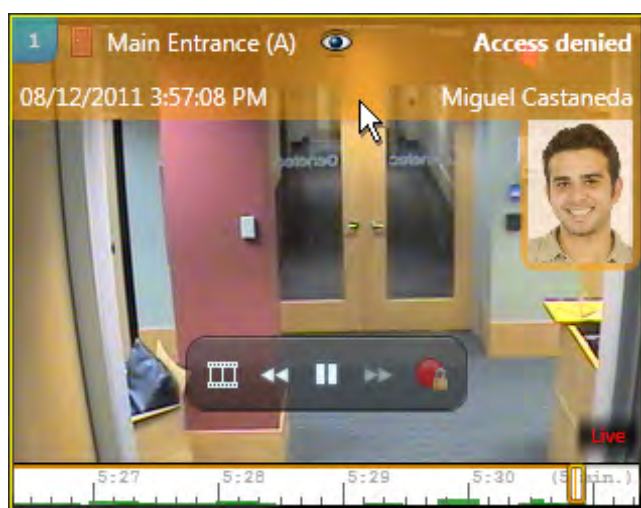
- The Directory pushes configurations to the Access Manager.
- Access Manager communicates directly with the physical door controllers, called access control units, over TCP/IP.
- Access Manager pushes schedules, cardholder information, and access rules to the door controllers.
- When a cardholder presents 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.

How access events are displayed in tiles

An access event (*Access granted* or *Access denied: Invalid PIN*, and so on) is any event involving an [access point](#). When an access event occurs on an entity you are monitoring, information about the event is displayed in a tile in the *Monitoring* task.

The following figure is an example of an Access denied event that has occurred. The event description is displayed at the top of the tile as a colored overlay. Additional information, such as the event timestamp and the cardholder name is displayed when you place the cursor over the colored overlay. Also, you can expand the cardholder picture by placing the cursor over the picture. This might be helpful when comparing the cardholder picture to the face you see in the video.



How antipassback works

An *antipassback violation* occurs when a cardholder enters an area that they never exited, or when they exit an area that they never entered. This can occur when an authorized cardholder unlocks a door, and while entering, passes their card back to somebody else.

The Security Center administrator can configure the system to deny access to that cardholder. When this happens, you must click the **Forgive antipassback violation** (👉) button to let the cardholder in or out. For information about applying antipassback to areas, see the *Security Center Administrator Guide*.

Cardholders and visitors

This section includes the following topics:

- ["About cardholders"](#) on page 212
- ["How cardholders are displayed in the Security Desk canvas"](#) on page 213
- ["Creating cardholders"](#) on page 214
- ["Checking in new visitors"](#) on page 218
- ["Cropping pictures"](#) on page 221
- ["Applying transparent backgrounds to pictures"](#) on page 222
- ["Assigning credentials"](#) on page 223
- ["Assigning temporary cards"](#) on page 227
- ["Using signature pads"](#) on page 229
- ["Checking out visitors"](#) on page 230
- ["Investigating cardholder events"](#) on page 231
- ["Investigating visitor events"](#) on page 233
- ["People counting"](#) on page 235
- ["Tracking cardholders present in an area"](#) on page 236
- ["Tracking attendance in an area"](#) on page 238
- ["Tracking the duration of a visitor's stay"](#) on page 239
- ["Viewing properties of cardholder group members"](#) on page 241
- ["The modify cardholder dialog box"](#) on page 243
- ["The modify visitor dialog box"](#) on page 245
- ["Searching for cardholders and visitors"](#) on page 247

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.

How cardholders are displayed in the Security Desk canvas

Cardholders represent people, such as employees, who can enter and exit secured areas using access cards, and whose activities can be tracked.

To view cardholder information in the canvas, drag a cardholder-related event from the report pane in the Cardholder access rights or Cardholder configuration tasks, to a tile.



-
- | | |
|----------|---|
| A | Cardholder name. |
| B | Displays additional cardholder details. |
| C | Cardholder picture. |
| D | Cardholder details. |
-

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 in Config Tool (see the *Security Center Administrator Guide*).
- If you require different groups of cardholders with different access rights, create cardholder groups in Config Tool (see the *Security Center Administrator Guide*).

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 their status to *Active* or *Inactive*. For their credential to work, and for them to 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.

To learn more about configuring areas and doors using the extended grant time and antipassback rules, see the *Security Center Administrator Guide*.

- 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 221

[Applying transparent backgrounds to pictures](#) on page 222

[Overview of the Cardholder management task](#) on page 468

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 in Config Tool (see the *Security Center Administrator Guide*).

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.

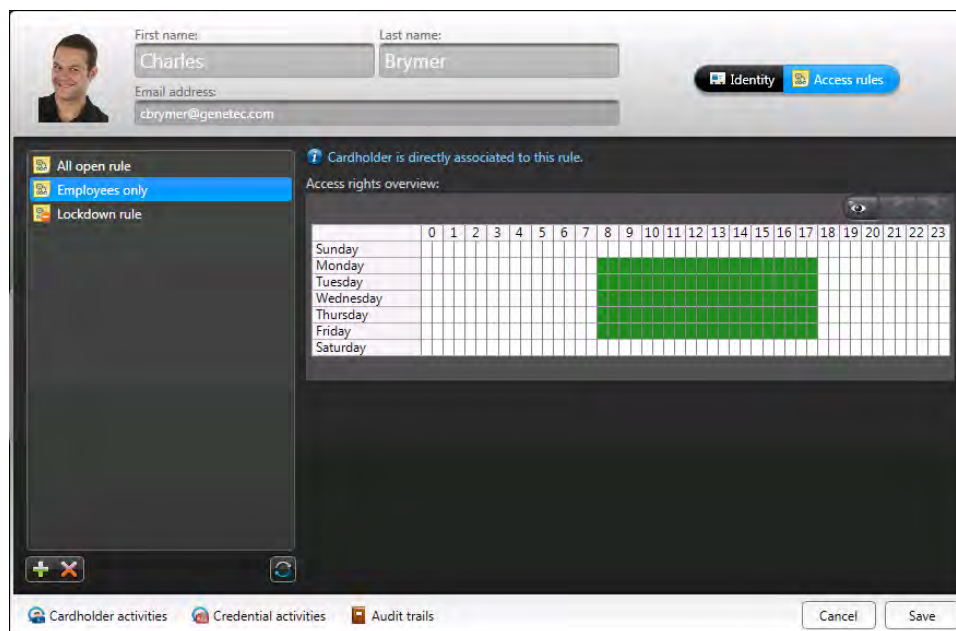
To assign access rules to a cardholder:

- 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.



- 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.](#)

Checking in new visitors

To ensure that a visitor's activities can be monitored throughout their visit, you must check in visitors, using the *Visitor management* task.

Before you begin

Access rules cannot be directly associated to visitors. Therefore, to grant [access rights](#) to a visitor, you must create a cardholder group that is reserved for visitors in Config Tool, and assign access rules to the group. For more information about creating cardholder groups, see the *Security Center Administrator Guide*.

To check in a new visitor:

- 1 From the home page, open the **Visitor management** task.
- 2 Click **Check-in** (👤).
- 3 At the top of the dialog box, enter the visitor's first name, last name, and e-mail address.
- 4 To assign a picture to the visitor, 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.
- 5 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.
- 6 In the *Status* section, set the following:

NOTE: The *Activation* time is not the same as the check-in time. *Activation time* indicates when the visitor's credentials are activated. *Check-in time* indicates when the visitor profile was created. You can set the activation time to a date in the future, which allows you to create visitor profiles in advance.

 - **Status:** Set their status to *Active* or *Inactive*. For their credential to work, and for them to 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.
- 7 [Assign a credential](#) to the visitor so that their movement can be tracked in the system.

NOTE: You can assign a credential now or later.

8 Assign the visitor to a *cardholder group*.

Cardholder groups defines which access rules apply to the visitor.

- a) To assign the first cardholder group, click the **Cardholder group** drop-down list and select a cardholder group.

NOTE: Only cardholder groups configured for visitors appear in this list. A visitor can belong to more than one 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**.

9 Enter the visitor's e-mail address.

10 (Optional) Assign a host (or an escort) to the visitor, as follows:

For more information about the visitor escort rule, see the *Security Center Administrator Guide*.

- a) Click the **Visitor host** drop-down list and select a cardholder or a cardholder group as the visitor's host.
- b) Select the option **Escort required** if the visitor is not allowed to access certain areas unless their escort also present their credential after them within a certain delay.

11 (Optional) If custom fields are defined for visitors, enter the additional visitor information.

12 (Optional) In the *Advanced* section, configure the following visitor properties:

NOTE: Some of these properties can be inherited from the parent cardholder groups. When a specific value is configured for the visitor, 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 visitor has been assigned a credential, grant access privileges to the visitor.

- **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.

To learn more about configuring areas and doors using the extended grant time and antipassback rules, see the *Security Center Administrator Guide*.

- b) In the **Security clearance** field, enter the visitor'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 new name for the visitor entity, if you do not want to use the visitor's first and last name.

By default, the **Entity name** uses the **First name** and **Last name** fields.

- d) (Optional) In the **Description** field, type a description for the visitor.

- e) Assign the visitor 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 visitor.

13 Click **Save**.

Related Topics

[Overview of the Visitor management task](#) on page 470

Checking in returning visitors

If a visitor returns to your site, you can check in the visitor without having to re-enter their information, because all checked-out visitors are saved in the database.

What you should know

If the visitor was previously assigned a credential, you must assign a new credential after the visitor is checked in.

To check in a returning visitor:

- 1 In the **Visitor management** task, click **Check-in** (👤🟢).
- 2 At the top of the dialog box, enter the visitor's first name or last name.
If a match is found in the visitor database, a green button showing the number of potential matches appears (👤🟢).
- 3 Click the green button.
A **Visitors** dialog box appears, listing all potential matches found in the database.
- 4 (Optional) To filter the visitor list, do one of the following:
 - Type a visitor's first name or last name, and then click **Search**.
 - Select the visitor's activation or expiration date, and then click **Search**.
 - Click **Click to edit**, select a visitor custom field, click **OK**, and then click **Search**.
- 5 Select a visitor, and then click **Select**.
The information of the selected visitor is loaded into the visitor dialog box.
- 6 Modify the visitor information as necessary, and then click **Save and close**.

After you finish

If the visitor requires a credential, [assign one](#).

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.



- 5 To revert the picture to its original state, click **Reset**.
- 6 Click **Apply**.

Applying transparent backgrounds to pictures

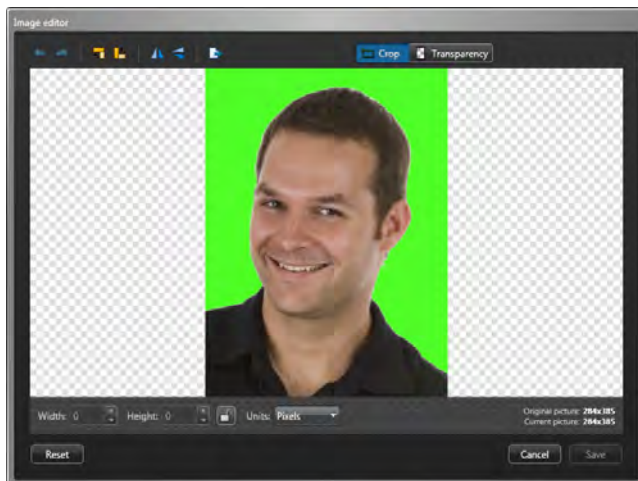
If a cardholder or visitor's picture was taken in front of a chroma key screen, you can make the picture background transparent. This is helpful if you create a badge template that has an image in the background.

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).



- 4 Using the **Tolerance** slider, adjust the transparency percentage.



- 5 To revert the picture to its original state, click **Reset**.
- 6 Click **Save**.

Assigning credentials

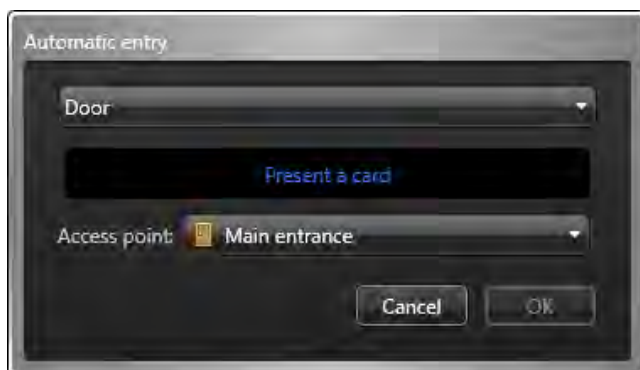
To grant cardholders or visitors access to secured areas, you must assign them credentials.

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.



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.

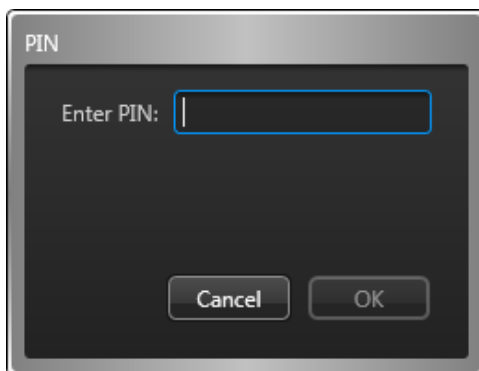
- 5 If you select **Manual entry**, then select a card format, enter the required data fields, and click **OK**.



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:



- 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**.

Badge templates are created in Config Tool. For information, see the *Security Center Administrator Guide*.

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.

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.

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. Badge templates are created in Config Tool. For information, see the *Security Center Administrator Guide*.

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** (🔔) icon appears in the notification tray.

Related Topics

[Responding to credential card requests](#) on page 262

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.

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.

For information about creating badge templates, see the *Security Center Administrator Guide*.

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**.

Assigning temporary cards

If a cardholder or visitor's card credential is reported as lost or stolen, you can replace it with a temporary card and mark the original card as lost.

Before you begin

Make sure that you have the following:

- A card reader nearby.
- A stack of pre-enrolled spare cards. You can [enroll a large quantity of cards](#) at once using the Credential management task.

To assign a temporary card to a cardholder or visitor:

- 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 **Assign temporary card**.
- 3 From the drop-down list, select a card reader near you.

The card reader can be a **USB Reader** connected to your computer, or you can use an **Access point** (door).
- 4 Present a spare card that is pre-enrolled.
- 5 Set the number of days the temporary card is to remain active, and click **Assign temporary card**.
- 6 Click **Save**.

After this operation, the original card is marked as **Lost**, but remains assigned to the cardholder. The temporary card is activated for the specified number of days, and assigned to the same cardholder. The cardholder now has at least two cards. A permanent one that is lost, and a temporary one that is active.

Restoring original cards to cardholders and visitors

When a lost card is found, you can restore the original card and remove the temporary card assignment.

Before you begin

Make sure you have a card reader nearby.

What you should know

To restore the original card, the cardholder or visitor must return both the original and the temporary card.

CAUTION: When a cardholder has more than one temporary card, returning the temp card restores the original card to the cardholder. The return temporary card functionality can be used only once per cardholder.

To restore an original card to a cardholder or visitor:

- 1 In the **Cardholder management** or **Visitor management** task, click **Return card** (👉).
- 2 From the drop-down list, select a card reader near you.
The card reader can be a **USB Reader** connected to your computer, or you can use an **Access point** (door).
- 3 Present both the original and the temporary cards; the order is not important.
- 4 If both cards match the same cardholder, click **Restore original card** to restore the status of the original card to **Active**, and deactivate the temporary card.
The temporary card can now be assigned to someone else.

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**.

Checking out visitors

You must check-out visitors when they leave.

To check out a visitor:

- 1 In the **Visitor management** task, select the visitor from the visitor list.
If the visitor list is long, use the search features to locate the visitor name.
- 2 Click **Check-out** (👤).

The checked-out visitor is removed from the visitor list, but remains available for investigation reports. The visitor's information is also saved in the database, and can be used if the visitor returns.

If the visitor was assigned a credential, the credential status switches to *Unassigned*, and can be assigned to another visitor or cardholder. The credential is also removed from all access controllers it was synchronized with. This might take a few seconds.

Related Topics

[Investigating visitor events](#) on page 233

[Overview of the Visitor management task](#) on page 470

Investigating cardholder events

You can investigate events related to cardholders (Access denied: Invalid PIN , First person in, Last person out, Antipassback violation, and so on), using the *Cardholder activities* report.

What you should know

For example, if you want to see which areas, doors, and elevators the cardholder has access in the last day or week, you can search for that specific cardholder, and set a time range for your report. If there has been suspicious activity on your site in the last day, you can investigate which cardholders were denied access to an area by selecting the area, and the *Access denied* event.

To investigate cardholder events:

- 1 From the home page, open the **Cardholder activities** task.
- 2 Set up the query filters for the report. Choose from one or more of the following filters:
 - **Cardholders:** Restrict the search to certain cardholders.

NOTE: If you only select the *All cardholders* cardholder group, federated cardholders are not included. This is because *All cardholders* is a local cardholder group that only covers local cardholders.
 - **Credentials:** Restrict the search to specific credentials.
 - **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 has been made visible to you when it was created or last configured.
 - **Doors - Areas - Elevators:** Restrict the search to activities that took place at certain doors, areas, and elevators.
 - **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 cardholder events are listed in the report pane.
- 4 Show the corresponding video of an event in a tile by double-clicking or dragging the item from the report pane to the canvas.

If there is no camera attached to the entity, the door, elevator, or area icon is displayed, depending on the type of cardholder event.
- 5 Control the tiles using widgets in the dashboard.

Report pane columns for the Cardholder activities 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).
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.

- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.
- **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 have been 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.).
- **Email address:** Cardholder or visitor's email address.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **First name:** Cardholder or visitor's first name.
- **IP address:** IP address of the unit or computer that generated the event.
- **Last name:** Cardholder or visitor's last name.
- **Location:** Location (area) where the activity took place.
- **Occurrence period:** Period when the event occurred.
- **Picture:** Cardholder or visitor's picture.
- **Product type:** Model of the unit involved.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door or elevator.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, intrusion detection, or LPR unit involved.


Investigating visitor events

You can investigate events related to visitors (access denied, first person in, last person out, antipassback violation, and so on), using the *Visitor activities* report.

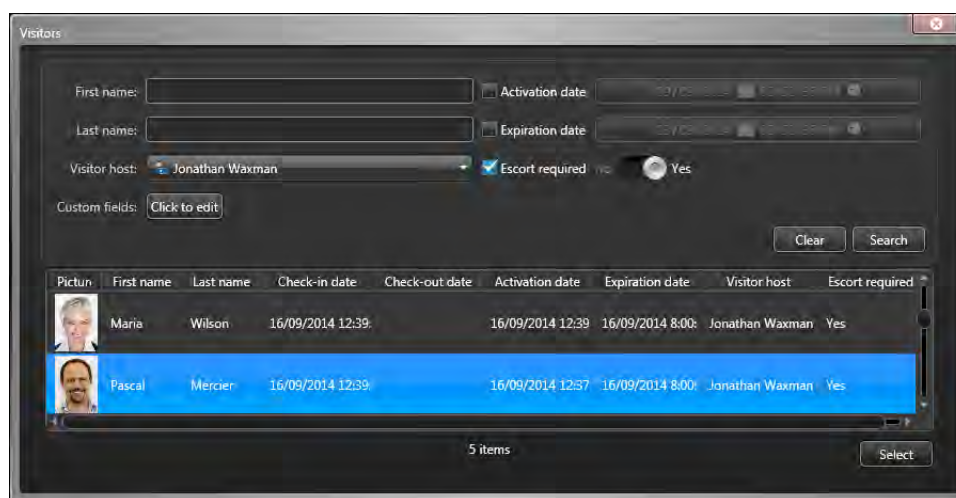
What you should know

For example, if you want to see all the areas and doors the visitor accessed during their stay, you investigate on just that visitor. If you want to see if there were any critical events that occurred on your site in the last day in relation to visitors, you can set a time range for the report.

To investigate visitor events:

- 1 From the home page, open the **Visitor activities** task.
- 2 In the **Visitor** query filter in the *Filters* tab, click .
- 3 In the **Visitors** dialog box, filter the visitor list one of the following ways:
 - Type a visitor's first name or last name, and then click **Search**.
 - Select the visitor's activation or expiration date, and then click **Search**.
 - Select the visitor's host or escort, and then click **Search**.
 - Click **Click to edit**, select a visitor custom field, click **OK**, and then click **Search**.
- 4 Select a visitor to investigate.

You can only specify one visitor at a time.



- 5 Click **Select**.
- 6 Set up the other 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 has been made visible to you when it was created or last configured.
 - **Doors - Areas - Elevators:** Restrict the search to activities that took place at certain doors, areas, and elevators.
 - **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.
- 7 Click **Generate report**.
The visitor events are listed in the report pane.
 - 8 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If there is no camera attached to the entity, the door, elevator, or area icons are displayed, depending on the type of visitor event.
 - 9 To control the tiles, use the widgets in the dashboard.

Report pane columns for the Visitor activities 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).
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.
- **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 have been 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.).
- **Email address:** Cardholder or visitor's email address.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **First name:** Cardholder or visitor's first name.
- **IP address:** IP address of the unit or computer that generated the event.
- **Last name:** Cardholder or visitor's last name.
- **Location:** Location (area) where the activity took place.
- **Occurrence period:** Period when the event occurred.
- **Picture:** Cardholder or visitor's picture.
- **Product type:** Model of the unit involved.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door or elevator.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, intrusion detection, or LPR unit involved.

People counting

You can view the number of cardholders that are currently in secured areas on your system, using the *People counting* task.

What you should know

The number of cardholders present in a selected area is updated live as people move in and out of the area.

For the report to be accurate, the selected area must be fully secured, meaning that people should not be allowed to enter or exit the area without swiping their card. Readers should be installed on both sides of a door (no *REX's*), and cardholders must pass through the door one by one (no *tailgating*). Turnstiles are often used for this purpose.

To count the number of cardholders in an area:

- 1 From the home page, open the **People counting** task.
- 2 In the *Selector*, select an area.

The cardholders present in that area are listed on the right.

- 3 To launch an investigation report on a selected cardholder, click **Investigate** (🔍).
- 4 To reset the people count to zero for the selected area, click **Clear all** (🗑️).

Example

If you see suspicious activity while monitoring a live video feed, you can use people counting to see the cardholders that currently are in that area. If there is a fire in your building, you can use people counting to see if there is anyone left in an area of the building.

Tracking cardholders present in an area

You can see how many cardholders and visitors are currently present in a selected area, and how long they have been there, using the *Area presence* report.

What you should know

For the report to be accurate, the selected area must be fully secured, meaning that people should not be allowed to enter or exit the area without swiping their card. Readers should be installed on both sides of a door (no *REX's*), and cardholders must pass through the door one by one (no *tailgating*). Turnstiles are often used for this purpose.

To track which cardholders are present in an area:

- 1 From the home page, open the **Area presence** task.
- 2 Set up the query filters for the report. Choose one or more of the following filters:
 - **Areas:** Select the areas to investigate.
 - NOTE:** You must select a fully secured area.
 - **Cardholders:** Restrict the search to certain cardholders.
 - **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 has been made visible to you when it was created or last configured.
- 3 Click **Generate report**.

The cardholders and visitors currently in the selected area are listed in the report pane.
- 4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If the area is not associated to a URL or a map file through a tile plugin, the area icon is displayed.
- 5 To control the areas, use the [area widget](#).

Report pane columns for the Area presence 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.

- **Area:** Area name.
- **Cardholder:** Cardholder entity name.
- **Cardholder group:** Cardholder groups that the user belongs to.
- **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 have been 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 access:** Time the cardholder entered the area.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.

- **Visitor host:** The visitor's host (or escort).

Tracking attendance in an area

Find out which cardholders and visitors have been inside a selected area, and the total duration of their stay within a given date range, using the *Time and attendance* report.

What you should know

This report displays the total time spent in the selected area by each selected cardholder and visitor, for each day covered by the date range. For example, if something happened in an area two days ago, you can find out who was in that area during that day by selecting the area and the date range.

For the report to be accurate, the selected area must be fully secured, meaning that people should not be allowed to enter or exit the area without swiping their card. Readers should be installed on both sides of a door (no *REX's*), and cardholders must pass through the door one by one (no *tailgating*). Turnstiles are often used for this purpose.

To investigate the duration of a cardholder or visitor's stay:

- 1 From the home page, open the **Time and attendance** task.
- 2 Set up the query filters for the report. Choose from one or more of the following filters:
 - **Areas:** Select the areas to investigate.

NOTE: You must select a fully secured area.
 - **Cardholders:** Restrict the search to certain cardholders.
 - **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 has been made visible to you when it was created or last configured.
 - **Time range:** The date range for the report.
- 3 Click **Generate report**.

The total time spent in the selected area by each selected cardholder and visitor, for each day covered in the selected date range, are listed in the report pane.

Report pane columns for the Time and attendance 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.

- **Area:** Area 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 have been made visible to you when they were created or last configured.
- **Date:** The date.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **Total time:** Total time spent in that area on that date by the cardholder.
- **Weekday:** Weekday corresponding to the date.


Tracking the duration of a visitor's stay

You can investigate the stay (check-in and check-out time) of current and past visitors, using the *Visit details* report.

What you should know

For example, if you want to know if a visitor checked-out before they left at the end of the day, you can investigate that visitor, and see if the *Check-out date* column in the report pane is filled out. You can also see which visitors were added or removed from the system in the last week.

To track the duration of a visitor's stay:

- 1 From the home page, open the **Visit details** 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.
 - **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 has been made visible to you when it was created or last configured.
 - **Expiration date:** Specify a time range for when the cardholder or visitor's profile expired.
 - **First name:** Cardholder or visitor's first name.
 - **Last name:** Cardholder or visitor's last name.
 - **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 visitor events are listed in the report pane.
- 4 To show a visitor's picture, name, and custom fields in a tile, double-click or drag an item from the report pane to the canvas.
- 5 To display additional visitor information in a tile, click .

Report pane columns for the Visit 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.

- **Activation date:** Time the cardholder or visitor's profile was activated.
- **Check-in date:** Time the visitor was checked in (can correspond to the arrival time).
- **Check-out date:** Time the visitor was checked out (can correspond to the departure time).
- **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 have been made visible to you when they were created or last configured.
- **Expiration date:** Time the cardholder or visitor's profile expired.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.

- **Picture:** Cardholder or visitor's picture.

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 has been 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

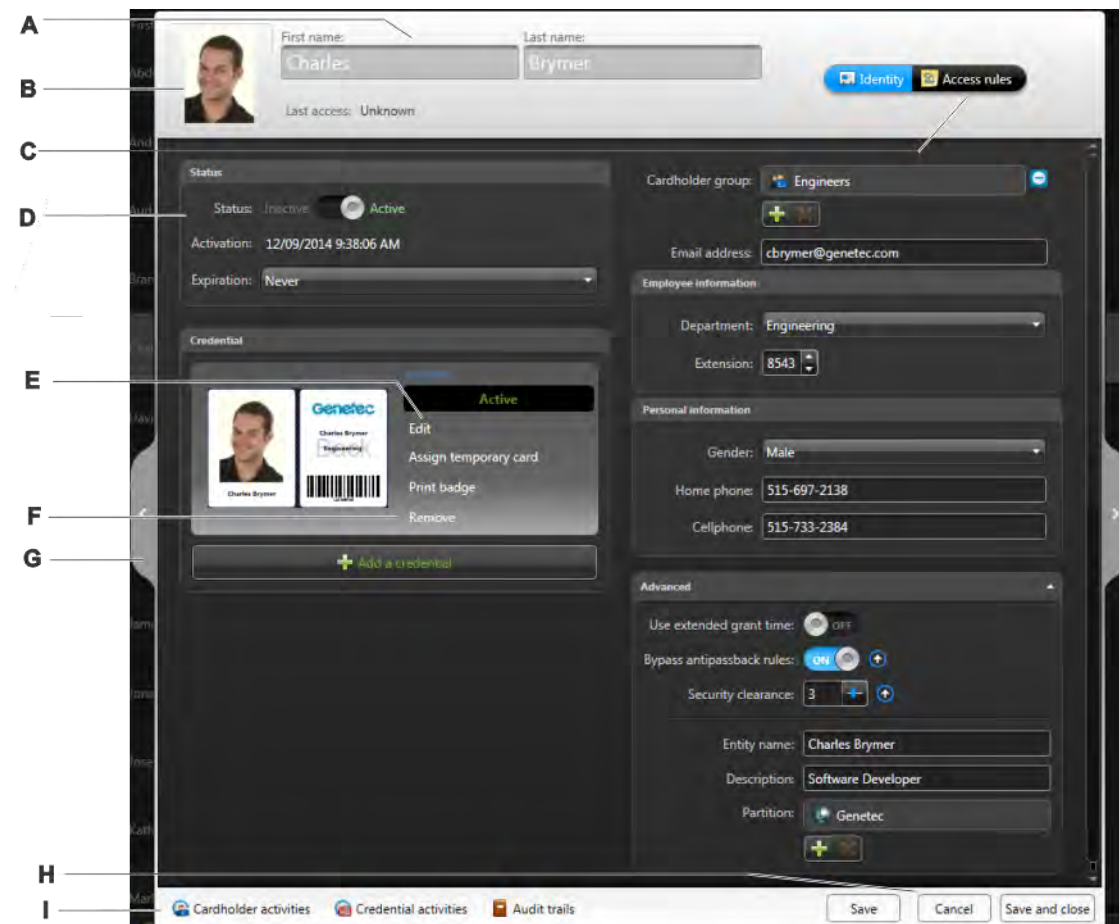
After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **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 have been 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.

The modify cardholder dialog box

Once you have created a cardholder, you can always go back and modify their properties, credentials, and access rights, by selecting the cardholder in the *Cardholder management* task, and then clicking *Modify* (✎).

The properties you can edit depend on your *user privileges*. The following figure shows the cardholder modification dialog box.






A Cardholder's basic properties. The cardholder properties are described in [Creating cardholders](#) on page 214.

B Edit the cardholder's picture (see [Cropping pictures](#) on page 221 and [Applying transparent backgrounds to pictures](#) on page 222).

To remove the cardholder's picture, right-click, and then click **Clear the picture**.

C Assign additional access rights to the cardholder from the *Access rules* tab (see [Assigning credentials](#) on page 223).

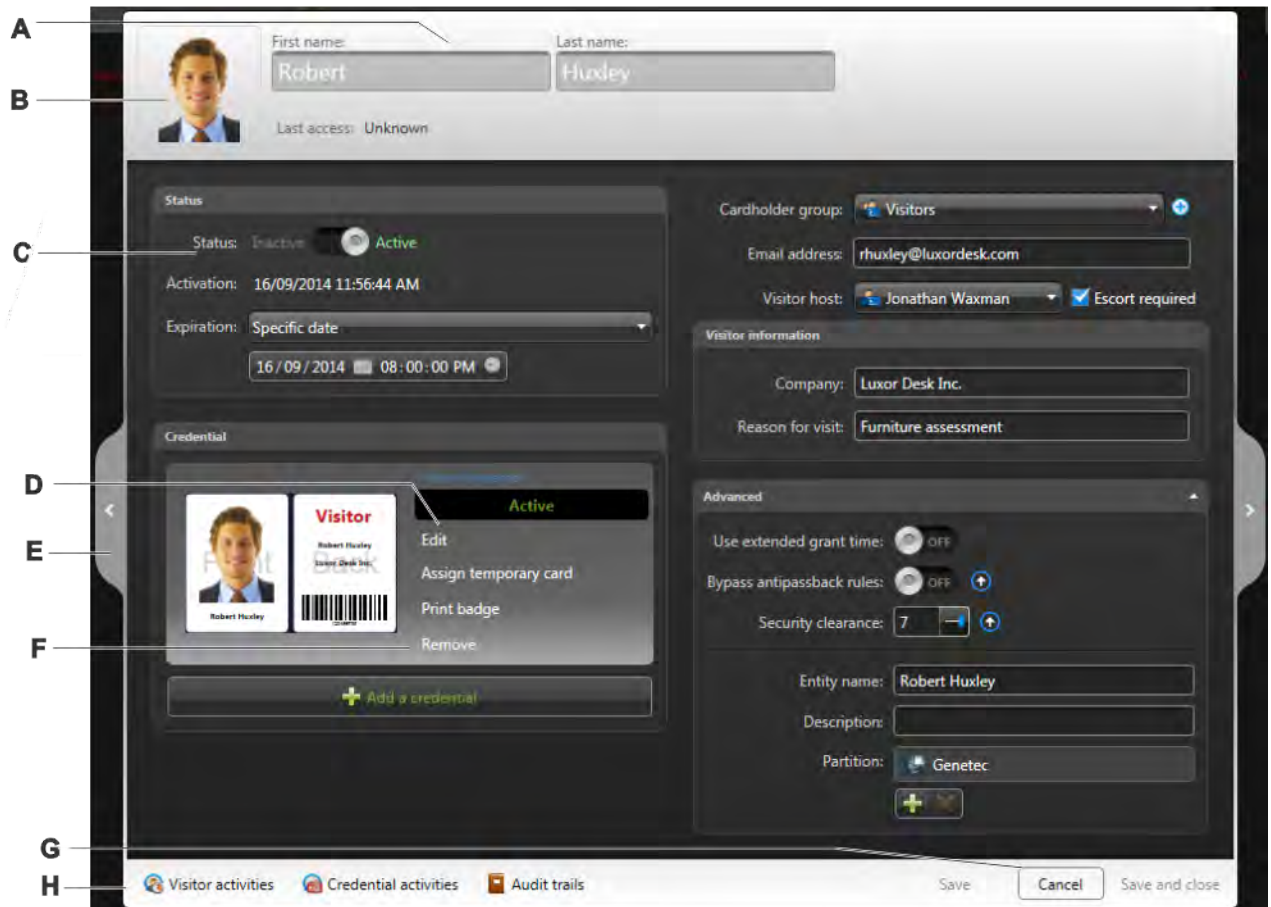
D Additional cardholder information. The properties are described in [Creating cardholders](#) on page 214.

-
- E** Edit the cardholder's credential. The credential properties are described in [Assigning credentials](#) on page 223.
-
- F** Remove the cardholder's credential.
-
- G** Switch between cardholders.
-
- H** Save or cancel your changes.
-
- I**
-  - Report on the cardholder (see [Investigating cardholder events](#) on page 231).
 -  - Report on the cardholder's credential (see [Investigating credential events](#) on page 265).
 -  - Report on the changes made to the cardholder (see [Finding out what changes were made to the system configuration](#) on page 97).
-

The modify visitor dialog box

Once you have checked-in a visitor, you can always go back and modify their properties by selecting the visitor in the *Visitor management* task, and then clicking *Modify* (✎).

The properties you can edit depend on your *user privileges*. The following figure shows the visitor modification dialog box.



A Visitor's basic properties. The visitor properties are described in [Checking in new visitors](#) on page 218.

B Edit the visitor's picture (see [Cropping pictures](#) on page 221 and [Applying transparent backgrounds to pictures](#) on page 222).

To remove the visitor's picture, right-click, and then click **Clear the picture**.




C Additional visitor information. The properties are described in [Checking in new visitors](#) on page 218.

D Edit the visitor's credential. The credential properties are described in [Assigning credentials](#) on page 223.

E Switch between visitors.

F Remove the visitor's credential.

G Save or cancel your changes.

- H**
-  - Report on the visitor (see [Investigating visitor events](#) on page 233).
 -  - Report on the visitor's credential (see [Investigating credential events](#) on page 265).
 -  - Report on the changes made to the visitor (see [Finding out what changes were made to the system configuration](#) on page 97).
-

Searching for cardholders and visitors

If you have a large access control system and cannot find a cardholder or visitor, you can search for them by name, or use the advanced search by applying a combination of filters.

To search for a cardholder or visitor:

1 From the home page, do one of the following:

- Open the **Cardholder management** task.
- Open the **Visitor management** task.

2 To search by an entity name, type the name in the **Search** (🔍) box.

All entities with names that match the text you entered are listed.

3 To search for the entity using the advanced search:

a) In the left pane, click **Advanced search**.

b) Set up the query filters for the report. Not all query filters are available for each task. Choose from one or more of the following, according to your task:

- **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.
- **Check-in date:** Time the visitor was checked in (can correspond to the arrival time).
- **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.
- **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.
- **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 has been made visible to you when it was created or last configured.
- **Escort required:** Specify that an escort is required.
- **Visitor host:** Select the visitor's host (or escort).

c) Click **Search**.

The cardholders or visitors that match your search criteria are displayed on screen.

Example

Let's assume that the cardholder or visitor you are searching for has a card that was activated less than a week ago. In the **Activation date** filter, enter *7 days* in the *During the last* box.

Report pane columns for the Cardholder management and Visitor management tasks

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.

NOTE: Not all report pane columns are available for both the **Cardholder management** task and the **Visitor management** task.

- **Activation date:** Time the cardholder or visitor's profile was activated.
- **Cardholder:** Cardholder entity name.
- **Cardholder status:** The cardholder's profile status.
- **Check-in date:** Time the visitor was checked in (can correspond to the arrival time).
- **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 have been made visible to you when they were created or last configured.
- **Description:** Description of the event, activity, entity, or incident.
- **Email address:** Cardholder or visitor's email address.
- **Escort required:** Indicates whether an escort is required.
- **Expiration date:** Time the cardholder or visitor's profile expired.
- **First name:** Cardholder or visitor's first name.
- **Last access:** Time and details of the last access event involving the cardholder or the credential.
- **Last name:** Cardholder or visitor's last name.
- **Member of:** All groups the cardholder belongs to.
- **Picture:** Cardholder or visitor's picture.
- **Role:** Role type that manages the selected entity.
- **Security clearance:** The cardholder's security clearance level.
- **Status:** The visitor's profile status.
- **Visitor host:** The visitor's host (or escort).


Searching for cardholders and visitors using their credential

If you have an unidentifiable card, you can find the cardholder or visitor it belongs to by presenting the card at a USB reader or door.

Before you begin

Make sure that you have a USB reader connected to your computer, or that there is a door you can present the card at.

To search for a cardholder or visitor by using their credential:

- 1 From the home page, open one of the following tasks:
 - For cardholders, click **Cardholder management**.
 - For visitors, click **Visitor management**.
- 2 At the top of the task window, click .
- 3 From the drop-down list in the search window, select one of the following:
 - **USB Reader:** A USB reader that is connected to your computer.
 - **Door:** An access point close by.
- 4 Present the card to the device selected in the previous step.

If the card is assigned to a cardholder or visitor, the search dialog box closes and the corresponding person is selected in the cardholder or visitor list. If the card is not assigned to a cardholder or visitor, the reason that the card is rejected is displayed in the search dialog box. You can present another card, or click **Cancel** to stop the operation.

Example

If you found a card in the office or parking lot and it has no name or picture on it, you can identify who it belongs to.

Credentials

This section includes the following topics:

- ["About credentials"](#) on page 251
- ["Credential enrollment methods"](#) on page 254
- ["Enrolling multiple credentials automatically"](#) on page 255
- ["Enrolling multiple credentials manually"](#) on page 257
- ["Creating credentials"](#) on page 259
- ["Responding to credential card requests"](#) on page 262
- ["Investigating request history of credential cards"](#) on page 263
- ["Investigating credential events"](#) on page 265
- ["Viewing credential properties of cardholders"](#) on page 267
- ["Searching for credentials"](#) on page 269

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. This table describes the standard card formats supported by Security Center, with the valid number range for the facility code and card 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 (also known as “Card ID Numbers”)
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 (also known as “Company ID Code”)	0 to 1 048 575 (also known as “Card ID Numbers”)

¹If 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.

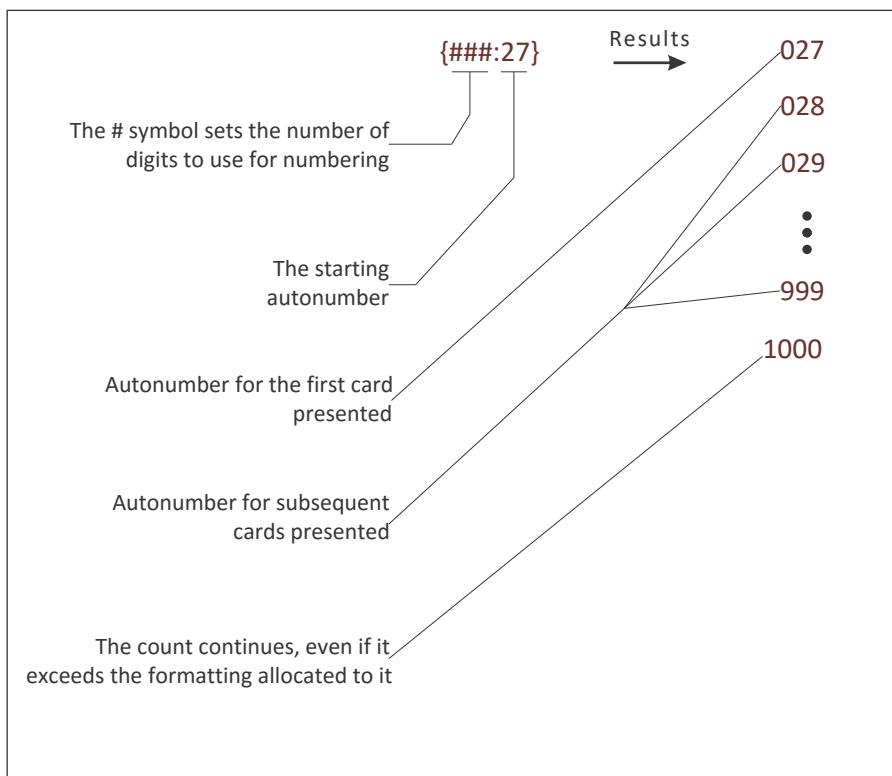
. Custom card formats are also supported if they are predefined in your system. To learn about creating custom card formats, see the *Security Center Administrator Guide*.

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.



The following are examples for the autonumber format.

Credential prefix	Credential sequence generated	Comments
Credential_	Credential_0 Credential_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 a 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 types 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*. For more information about importing credentials using the *Import tool*, see the *Security Center Administrator Guide*.

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.

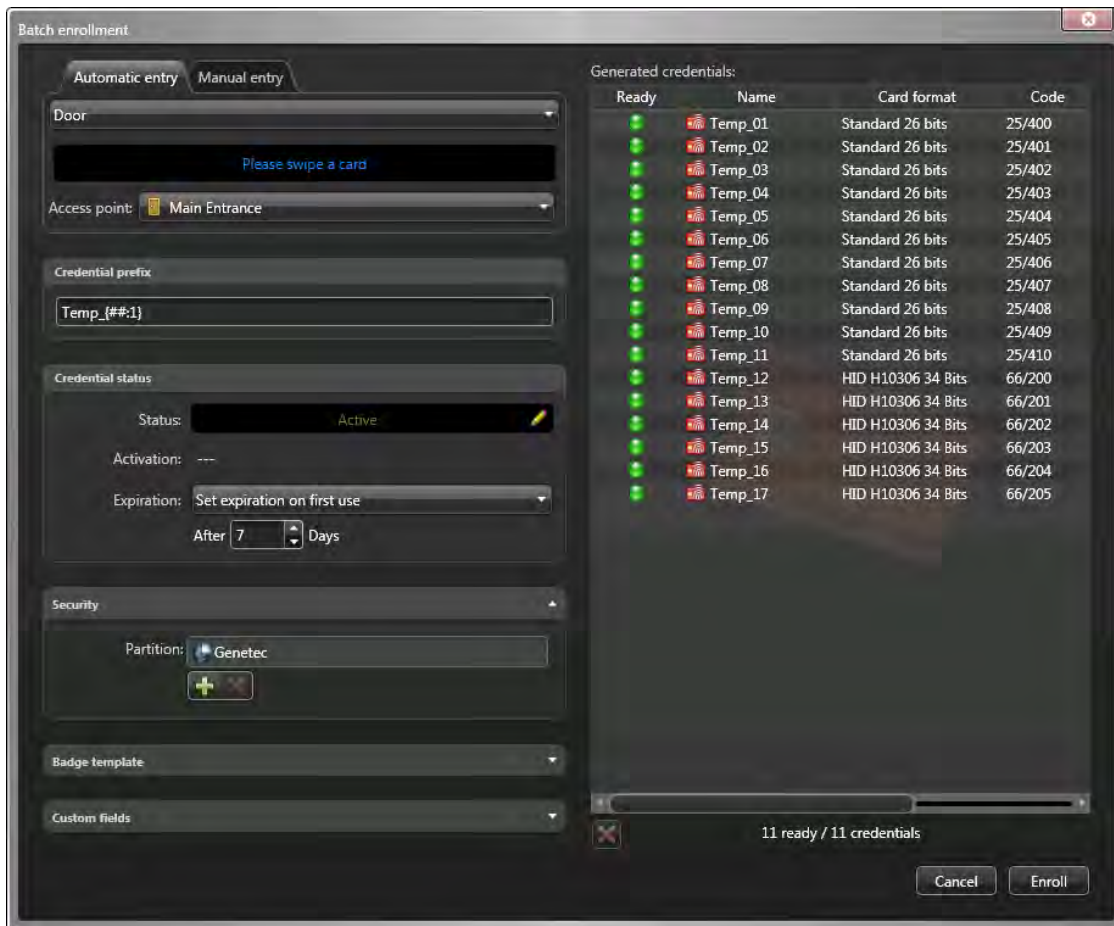
What you should know

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** (X).
- 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.



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

[About credentials](#) on page 251

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.

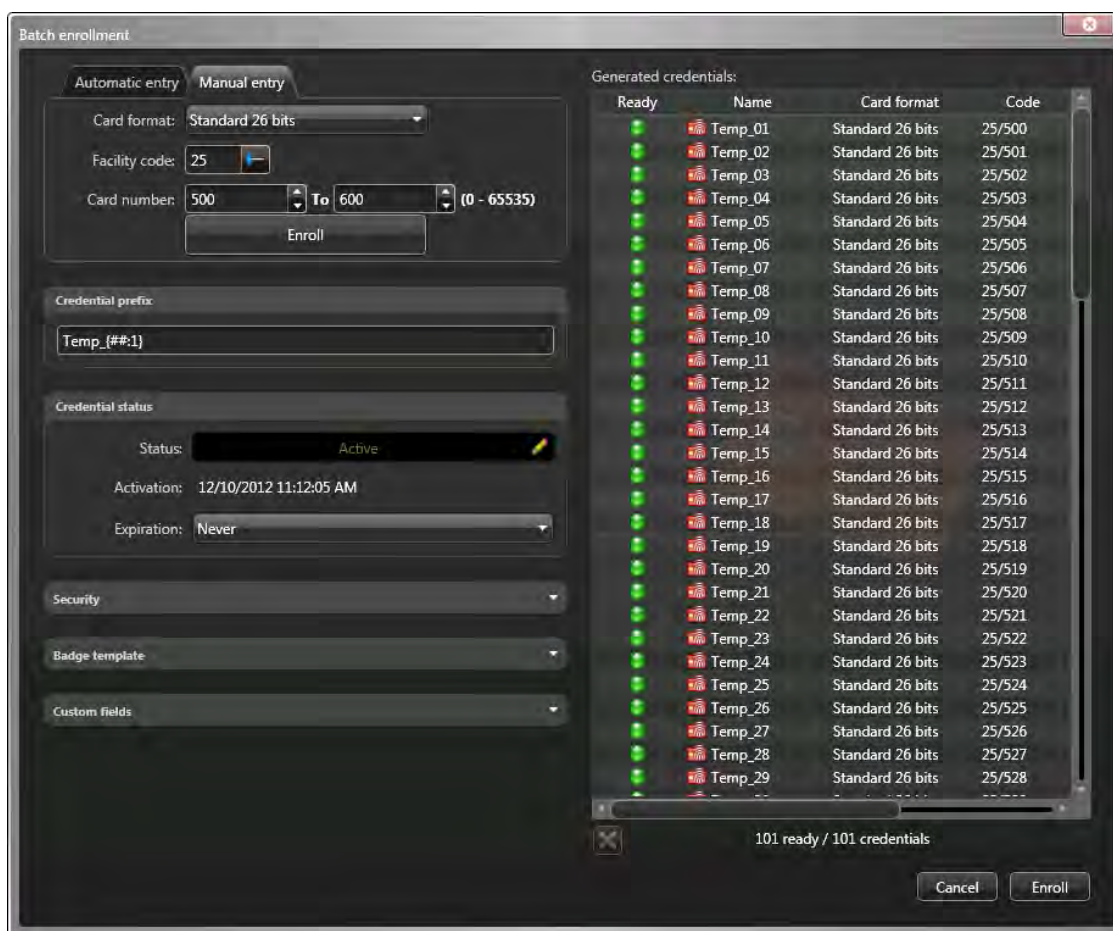
NOTE: If the specified **Card number** range contains more than 5000 values, the end value is automatically adjusted to be the start value plus 5000.

- 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 (X)**.
- 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.



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 **X**.
- 12 Click **Enroll**.

After you finish

[Assign the credentials to your cardholders.](#)

Related Topics

[About credentials](#) on page 251

Creating credentials

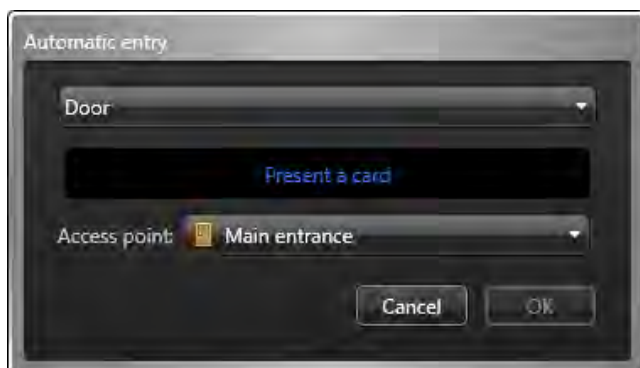
You can create a new credential, configure its properties, and assign it to a cardholder or visitor, using the *Credential management* task.

What you should know

Instead of creating credentials manually, you can import them from a CSV file, or from your company's Active Directory. For more information, see the *Security Center Administrator Guide*).

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.



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.

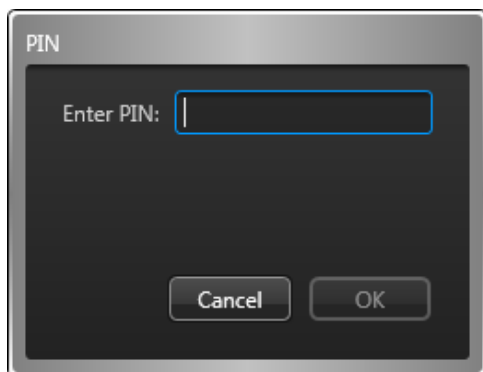
- 4 If you select **Manual entry**, then select a card format, enter the required data fields, and click **OK**.



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.

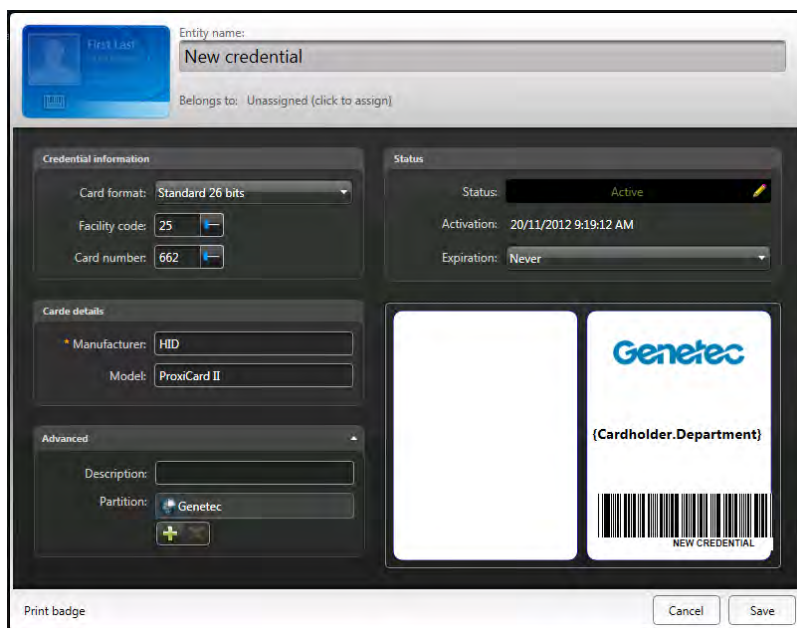
NOTE: The numeric value corresponding to the PIN cannot exceed 65535.

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.



- 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. For information, see the *Security Center Administrator Guide*.

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

[Assigning credentials](#) on page 223


[Requesting credential cards](#) on page 225

[Overview of the Credential management task](#) on page 472

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

[Creating credentials](#) on page 259

[Requesting credential cards](#) on page 225

Investigating request history of credential cards

You can see which users requested, cancelled, and printed credential cards, using the *Credential request history* report.

Before you begin

To receive results in the Credential request history report, you must already be monitoring credential request user activities. For information about how to select which activities to monitor and record in the database from the System task in Config Tool, see the *Security Center Administrator Guide*.

What you should know

Credential badges are usually requested if there is no printer located on the site. If you create a report of the badges that were printed in the last month, the report results can be used as billing information.

To investigate the request history of credential badges:

- 1 From the home page, open the **Credential request history** task.
- 2 Set up the query filters for your report. Choose one or more of the following filters:
 - **Activities:**
Select which badge printing activities to investigate.
 - **Credential request:** When a user requests a badge printing job.
 - **Credential request cancelled:** When a user cancels a badge printing job.
 - **Credential request completed:** When a user prints a badge from the queue.
 - **Cardholders:** Restrict the search to certain cardholders.
 - **Credentials:** Restrict the search to specific credentials.
 - **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 has been made visible to you when it was created or last configured.
 - **Printing users:** Restrict the search to specific users that printed a badge.
 - **Requesting users:** Restrict the search to specific users that requested to print a badge.
- 3 Click **Generate report**.
The credential badge printing events are listed in the report pane.

Related Topics

[Requesting credential cards](#) on page 225

Report pane columns for the Credential request 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.

- **Activity name:** Type of activity.

- **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 have been made visible to you when they were created or last configured.
- **Credential:** Credential name used by the cardholder.
- **Date/time queued:** The date and time that the badge printing job was requested.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **Request reason:** Reason why the new credential was requested.
- **Requester email:** Email address of the user who requested the badge printing job.
- **User:** Name of the user who triggered the event. The user name is empty if the event was not triggered from Security Desk.

Investigating credential events

You can investigate events related to credentials (Access denied: Expired credential, Access denied: Inactive credential, Access denied: Stolen credential, and so on), using the *Credential activities* report.

What you should know

In the *Credential activities*, you can investigate areas a cardholder accessed by selecting the credential, and the time range. You also can search by critical credential events. For example, if an *Access denied: Stolen credential* event occurred, you can see who tried to use the stolen credential by reviewing the video associated with the event.

To investigate credential events:

- 1 From the home page, open the **Credential activities** task.
- 2 Set up the query filters for your report. Choose one or more of the following filters:
 - **Credentials:** Restrict the search to specific credentials.
 - **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 has been made visible to you when it was created or last configured.
 - **Doors - Areas - Elevators:** Restrict the search to activities that took place at certain doors, areas, and elevators.
 - **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 credential events are listed in the report pane.
- 4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If there is no camera attached to the entity, the door, elevator, or area icon is displayed, depending on the type of credential event.
- 5 To control the tiles, use the widgets in the dashboard.

Report pane columns for the Credential activities 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).
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.

- **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 have been 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.).
- **Email address:** Cardholder or visitor's email address.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **First name:** Cardholder or visitor's first name.
- **IP address:** IP address of the unit or computer that generated the event.
- **Last name:** Cardholder or visitor's last name.
- **Location:** Location (area) where the activity took place.
- **Occurrence period:** Period when the event occurred.
- **Picture:** Cardholder or visitor's picture.
- **Product type:** Model of the unit involved.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, intrusion detection, or LPR unit involved.

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 has been 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 .

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 have been 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.

Searching for credentials

If you have a large access control system and cannot find a credential, you can search for it by name, or use the advanced search by applying a combination of filters.

To search for a credential:

- 1 From the home page, open the **Credential management** task.
- 2 To search by an entity name, type the name in the *Search* (🔍) box.

All entities with names that match the text you entered are listed.

- 3 To search for the entity using the advanced search:

a) In the left pane, click **Advanced search**.

b) Set up the query filters for the report. Choose from one or more of the following filters:

- **Cardholders:** Restrict the search to certain cardholders.
- **Credential:** Specify whether or not the credential is assigned.
- **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 has been made visible to you when it was created or last configured.
- **Description:** Restrict the search to entries that contain this text string.
- **Expiration date:** Specify a time range for when the credential will expire.
- **Partition:** Partition that the entity is a member of.
- **Status:** The status of the cardholder or visitor's profile: Active; Expired; Inactive; Lost; Stolen. Not all statuses are available for every task.

c) Click **Search**.

The credentials that match your search criteria are displayed on screen.

Report pane columns for the Credential management 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.

- **Activation date:** Time the credential was activated.
- **Card format:** Credential card format.
- **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.
- **Credential:** Credential name used by the cardholder.
- **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 have been made visible to you when they were created or last configured.
- **Description:** Description of the event, activity, entity, or incident.

- **Email address:** Cardholder or visitor's email address.
- **Expiration date:** Time the credential expired.
- **First name:** Cardholder or visitor's first name.
- **Last access:** Time and details of the last access event involving the cardholder or the credential.
- **Last name:** Cardholder or visitor's last name.
- **PIN:** Credential PIN.
- **Role:** Role type that manages the selected entity.

Areas, doors, and elevators

This section includes the following topics:

- ["How areas are displayed in the canvas"](#) on page 272
- ["How doors are displayed in the Security Desk canvas"](#) on page 273
- ["Allowing access through doors"](#) on page 274
- ["Preventing access through doors"](#) on page 276
- ["Investigating area events"](#) on page 277
- ["Investigating door events"](#) on page 279
- ["Investigating elevator events"](#) on page 281
- ["Identifying who is granted/denied access at access points"](#) on page 283
- ["Identifying who is granted access to doors and elevators"](#) on page 284
- ["Identifying which entities are affected by access rules"](#) on page 285

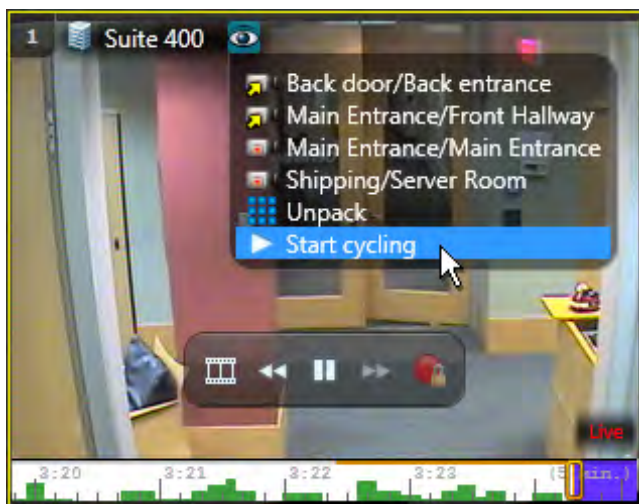
How areas are displayed in the canvas

When you display an *area* (🏠) or a *secured area* (🔒) in a canvas tile, the area widget appears in the dashboard so you can control the area.

Areas usually have multiple cameras attached to them. When you view an area, the first camera associated to that area is displayed.




By clicking the eye (👁️) icon in the tile toolbar, you can select which attached entity to view, or you can *unpack* the area, which displays all the attached entities in separate tiles. You can also start *entity cycling*, which rotates the entities displayed in the tile.

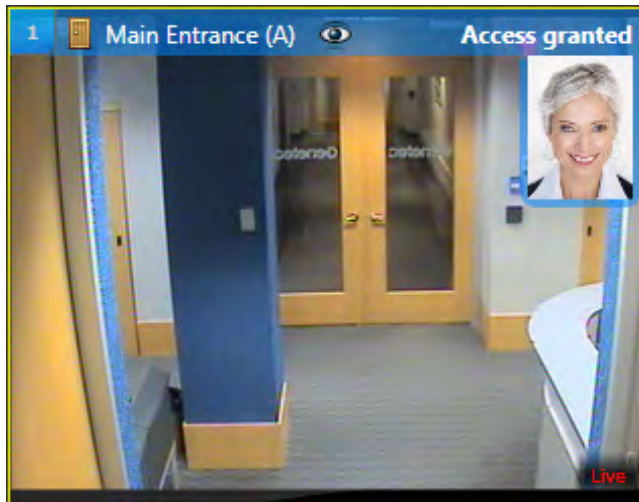


If no camera is associated to the area, only the area icon is shown.

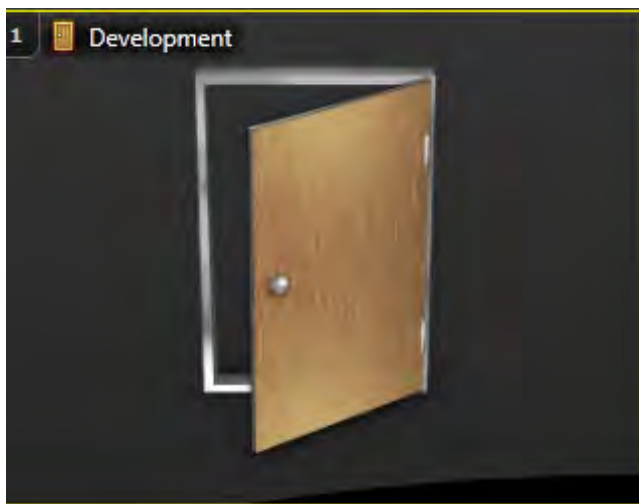
How doors are displayed in the Security Desk canvas

When you display a *door* () in a canvas tile, the door widget appears in the dashboard so you can control the door.

If the door is linked to a camera, then the video stream of the camera is shown in the tile.



If the door is not linked to a camera, only the door icon is shown. The door image is static. It always remains open.



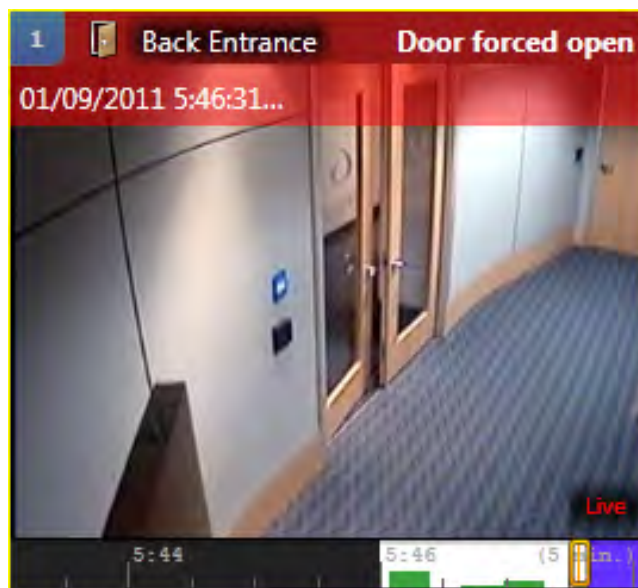
Allowing access through doors

To unlock a door or override locking and unlocking schedules, you can use the *Door* widget to control access through doors. The door widget is enabled when a door entity is displayed in the selected canvas tile.

What you should know

Access controlled doors are locked by default, unless an unlock schedule is being used. Only cardholders with the correct credentials can open them. When a door is displayed in a canvas tile, the door entity icon in the tile toolbar changes in real time to reflect whether the door is physically open (🚪) or closed (🚪).

If no camera is associated to the door, a static open door image is displayed in the canvas tile. The following figure shows an open door and its corresponding door icon.



To allow access through a door:

- 1 From the **Monitoring** task, select a tile that is displaying a door.

The *Door* widget is displayed in the dashboard.

- 2 In the door widget, do one of the following:

- To unlock the door and temporarily grant access, click **Unlock** (🚪).

The duration of the grant time is configured by the system administrator. The widget shows that the door is open and unlocked.

- To override the door's unlock schedule, click **Override unlock schedules** (🚪), and select one the following:
 - **Unlock for maintenance:** Unlock the door indefinitely for maintenance purposes. To cancel this override, click 🚫 in the door widget.
 - **Temporarily override unlock schedule:** Lock or unlock the door for the time specified in the *From* and *To* fields. With this option, the door returns to its normal state after the time expires.

Example

When setting unlock schedules for a door, a Security Center administrator can program a door to grant access to everyone during certain hours of the day, such as when a receptionist is on duty. If you have the rights, you can override these unlock schedules by locking the door when it is scheduled to be unlocked, or by unlocking the door when it is scheduled to be locked.

Preventing access through doors

To temporarily prevent all access through a door, you can deactivate (or shunt) the reader on the side of the door you don't want people to access.

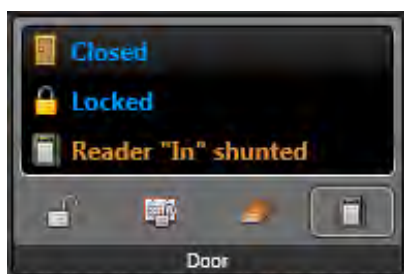
What you should know

Not all readers can be disabled from Security Desk. The ability to shunt a reader depends on your access control equipment. Shunting a reader is equivalent to cutting the power to the reader. For this reason, a cardholder presenting a valid credential at the door would no longer be able to unlock the door. This however does not prevent someone from unlocking the door with a key.

TIP: You can also shunt a defective reader to prevent it from beeping or generating any events.

To prevent access through a door:

- 1 From the **Monitoring** task, select a tile that is displaying a door.
The *Door widget* is displayed in the dashboard.
- 2 In the door widget, click the **Reader** (📶) button, and select the reader you want to shunt.
The reader that is shunted is indicated in the door widget.



Investigating area events

You can investigate events related to *areas* (Access granted, First person in, Antipassback violation, and so on), using the *Area activities* report.

To investigate area events:

- 1 From the home page, open the **Area activities** task.
- 2 Set up the query filters for the report. Choose from one or more of the following filters:
 - **Areas:** Select the areas to investigate.
 - **Cardholders:** Restrict the search to certain cardholders.
 - **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 has been 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 area events are listed in the report pane.
- 4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If the area is not associated to a URL or a map file through a tile plugin, the area icon is displayed.
- 5 To control the areas, use the area widget.

Example

If you want to see all the activity that went on in a particular area during the weekend, or since the last time you logged on, you can select a specific area and time range for the report. You can search for critical events that happened in an area (such as *Access granted* or *Access denied: Stolen credential* events), and then review the video associated with that event to see what happened during that time, and to find evidence.

Related Topics

[Area widget](#) on page 33

Report pane columns for the Area activities 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.

- **Area:** Area name.
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.

- **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 have been 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.).
- **Email address:** Cardholder or visitor's email address.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **First name:** Cardholder or visitor's first name.
- **IP address:** IP address of the unit or computer that generated the event.
- **Last name:** Cardholder or visitor's last name.
- **Occurrence period:** Period when the event occurred.
- **Picture:** Cardholder or visitor's picture.
- **Product type:** Model of the unit involved.
- **Security clearance:** The cardholder's security clearance level.
- **Side-Direction:** Entrance or exit.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door or elevator.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, intrusion detection, or LPR unit involved.

Investigating door events

You can investigate events related to *doors* (Door forced open, Door open too long, Hardware tamper, and so on), using the *Door activities* report.

To investigate door events:

- 1 From the home page, open the **Door activities** task.
- 2 Set up the query filters for your report. Choose one or more of the following filters:
 - **Cardholders:** Restrict the search to certain cardholders.
 - **Credentials:** Restrict the search to specific credentials.
 - **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 has been made visible to you when it was created or last configured.
 - **Doors:** Select the doors to investigate.
 - **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 door events are listed in the report pane.
- 4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If there is no camera attached to the door, the door icon is displayed.
- 5 To control the doors, use the door widget.

Example

You can see how many access denied events have occurred in the last week, or since your last shift, or search for other critical events (For example, *Door forced open*). If you see suspicious cardholder activity while monitoring live video, you can investigate what other doors the cardholder accessed in the last day. If you want to see if the maintenance staff has completed work at a particular door, you can investigate on that door, and select the *Door maintenance completed* event.

Related Topics

[Door widget](#) on page 37

Report pane columns for the Door activities 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.

NOTE: If you generated the Door activities report using Web Client, not all of the report columns are available.

- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.

- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.
- **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 have been 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.).
- **Door:** Door name.
- **Email address:** Cardholder or visitor's email address.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **First name:** Cardholder or visitor's first name.
- **IP address:** IP address of the unit or computer that generated the event.
- **Last name:** Cardholder or visitor's last name.
- **Occurrence period:** Period when the event occurred.
- **Picture:** Cardholder or visitor's picture.
- **Product type:** Model of the unit involved.
- **Side:** Door side name.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door or elevator.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, intrusion detection, or LPR unit involved.

Investigating elevator events

You can investigate events related to elevators (Floor accessed, Elevator offline: Device is offline, Hardware tamper, and so on), using the *Elevator activities* report.

What you should know

Using the *Elevator activities*, you can see which cardholders or credentials accessed which elevators and floors, for a given time period. You also can search for access denied events at an elevator, to see who tried to access a floor they did not have permission to enter.

To investigate elevator events:

- 1 From the home page, open the **Elevator activities** task.
- 2 Set up the query filters for your report. Choose one or more of the following filters:
 - **Cardholders:** Restrict the search to certain cardholders.
 - **Credentials:** Restrict the search to specific credentials.
 - **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 has been made visible to you when it was created or last configured.
 - **Elevators:** Select the elevators to investigate.
 - **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 elevator events are listed in the report pane.
- 4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If the elevator is not associated to a URL or a map file through a tile plugin, the elevator icon is displayed.
- 5 To control the tiles, use the widgets in the dashboard.

Report pane columns for the Elevator activities 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.
- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.
- **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 have been 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.).

- **Elevator:** Elevator name.
- **Email address:** Cardholder or visitor's email address.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **First name:** Cardholder or visitor's first name.
- **Floor:** Elevator floor name.
- **IP address:** IP address of the unit or computer that generated the event.
- **Last name:** Cardholder or visitor's last name.
- **Occurrence period:** Period when the event occurred.
- **Picture:** Cardholder or visitor's picture.
- **Product type:** Model of the unit involved.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door or elevator.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, intrusion detection, or LPR unit involved.

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](#).

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 have been 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.

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.

For information about modifying the properties of doors or elevators, see the *Security Center Administrator Guide*.

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](#).

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 have been 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 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.

For information about modifying the members of an access rule, see the *Security Center Administrator Guide*.

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 has been 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.

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 have been 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.

Access control units

This section includes the following topics:

- ["Investigating events related to access control units"](#) on page 287
- ["Viewing I/O configuration of access control units"](#) on page 288
- ["Enabling external access control devices"](#) on page 289

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 has been 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 have been 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.

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 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 has been 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 101

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 have been 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.

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.

Part IV

License Plate Recognition

This part includes the following chapters:

- Chapter 20, "[LPR at a glance](#)" on page 291
- Chapter 21, "[LPR events](#)" on page 293
- Chapter 22, "[Reads, hits, hotlists, and permits](#)" on page 302
- Chapter 23, "[Patroller](#)" on page 328
- Chapter 24, "[Mobile License Plate Inventory](#)" on page 337

LPR at a glance

This section includes the following topics:

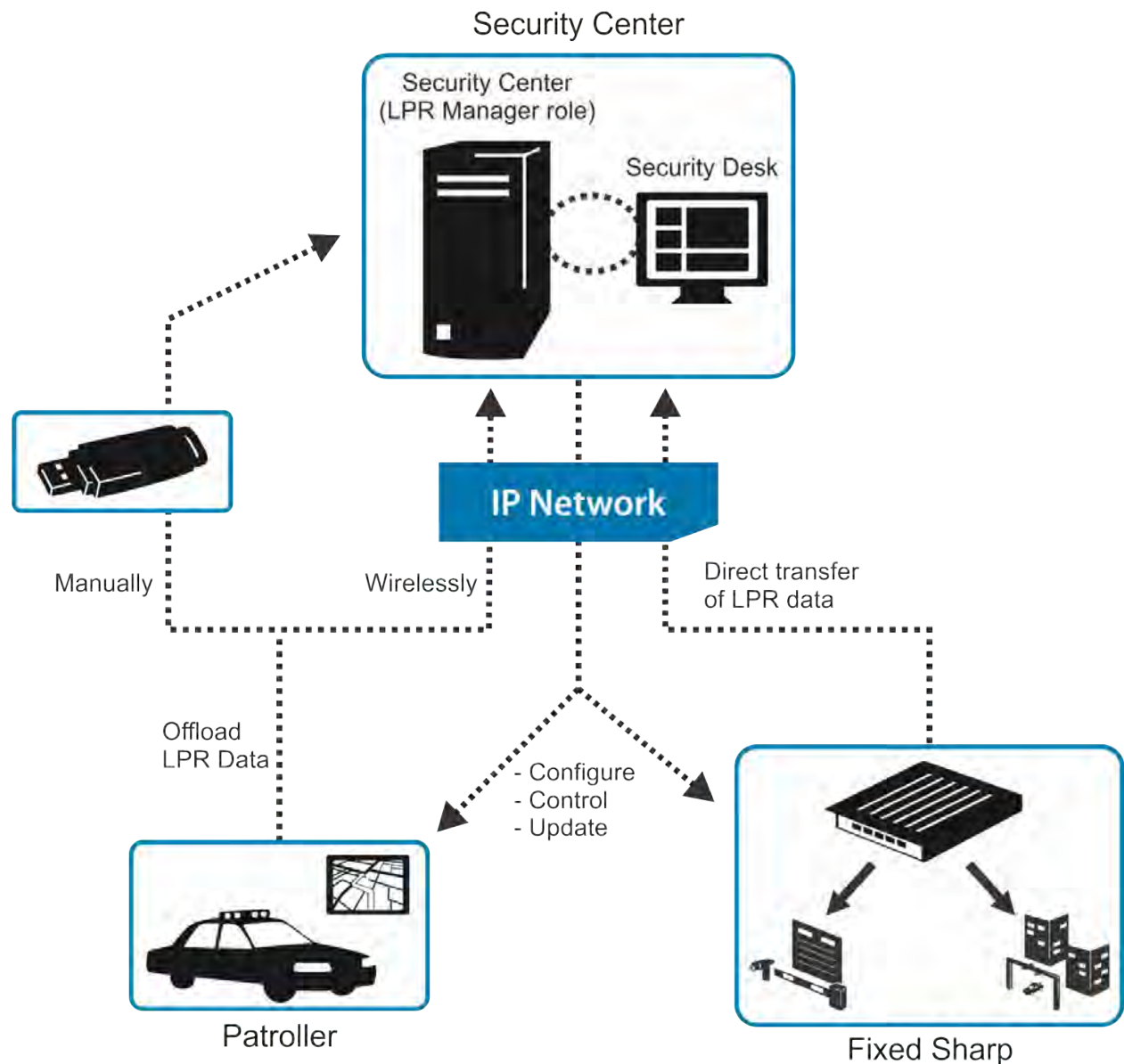
- ["About AutoVu "](#) on page 292

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:



LPR events

This section includes the following topics:

- ["How LPR events are viewed in Security Desk"](#) on page 294
- ["Configuring Security Desk to automatically display high-resolution context images"](#) on page 295
- ["Customizing which LPR information to display in Security Desk"](#) on page 296
- ["Monitoring LPR events in tile mode"](#) on page 298
- ["Monitoring LPR events in map mode"](#) on page 300

How LPR events are viewed in Security Desk

LPR events are license plate reads and hits that are generated by LPR entities, such as Patrollers and LPR units. You can track LPR events in real time, using the *Monitoring* task.

When an LPR event occurs, you can view the event information in the event list, including the plate and context images, the GPS position of the Patroller vehicle or Sharp camera that recorded the event, the reason a hit was rejected, and so on. In fixed Sharp configurations with video (Omnicast), you can stream live video from the Sharp context camera, and other cameras located with the Sharp. You can also print hit events, and use them as proof of violation. You can choose to view LPR events in the canvas in Tile mode (individual tiles) or Map mode (a road map).

The GPS position of recorded reads and hits is the GPS position of the Patroller or Sharp camera that recorded the event.

CAUTION: For events to be kept in the database and available for reporting, they must be offloaded from Patroller. You can monitor live events from the *Monitoring* task and receive live data in some reports without offloading from Patroller.

Configuring Security Desk to automatically display high-resolution context images

You can configure Security Desk to automatically load the high resolution vehicle context images for plate reads and hits displayed in Monitoring task tiles.

Before you begin

Close Security Desk.

What you should know

This can increase the efficiency of Security Desk operators that would normally have to manually display the high-res images, but it requires higher than normal bandwidth, and results in increased CPU usage on the computer hosting the LPR Manager role.

When this feature is enabled, the button to manually display high-res images in Security Desk is disabled. Operators will always see the high-res version of the images.

To configure Security Desk to automatically display high-res context images:

- 1 On the Security Desk client computer, go to *C:\Program Files (x86)\Genetec Security Center 5.5\ConfigurationFiles*.
This is the default folder location.
- 2 Open the *App.SecurityDesk.config* file in Notepad or a similar text editor.
- 3 In the `<Presentation>` tag, find the parameter **AutoLoadHighResImages**, and change the value to **True**.
- 4 Save and close Notepad.
- 5 Start Security Desk.

All vehicle context images are displayed in high-resolution, and the button to toggle between high and low resolution images is no longer visible.

After you finish

Repeat these steps on any Security Desk client machine that requires automatically displayed high-resolution context images in Monitoring task tiles.

Customizing which LPR information to display in Security Desk

You can choose what kind of LPR information you want to display in Monitoring task tiles for reads and hits. This ensures that Security Desk operators see only the information that is required for your LPR deployment scenario.

Before you begin

Close Security Desk.

What you should know

This feature works by adding different XML attributes and parameters to a specific Security Desk configuration file located on the Security Desk client machine. Each XML attribute corresponds to different LPR information.

To customize which LPR information to display in Security Desk:

- 1 On the Security Desk client computer, go to *C:\Program Files (x86)\Genetec Security Center 5.5\ConfigurationFiles*.

This is the default folder location.

- 2 Open the *App.SecurityDesk.config* file in Notepad or a similar text editor.

- 3 Find the following tag in the config file: `<Presentation IgnoreSizeConstraints="False" DisplayResourcesIds="False" SearchFormState="" AutoLoadHighResImages="False"/>`.

You can add additional XML attributes anywhere between the opening bracket and the closing slash and bracket.

- 4 To customize the display of read-related information in a tile, add the "ReadDescription=" attribute, followed by any of the following parameters:

NOTE: Add the character `` if you want to force a carriage return in the Security Desk tile.

- **{Read.Address}**: The address of the plate read.
- **{Read.Confidence Score}**: The Confidence Score analytic information of the plate read (read accuracy). If the Sharp camera is not configured to send this analytic information, the XML tag will be displayed in the Security Desk tile.
- **{Read.Vehicle Type}**: The Vehicle Type analytic information of the plate read. If the Sharp camera is not configured to send this analytic information, the XML tag will be displayed in the Security Desk tile.
- **{Read.Relative Motion}**: The Relative Motion analytic information of the plate read. If the Sharp camera is not configured to send this analytic information, the XML tag will be displayed in the Security Desk tile.
- **{Read.Plate}**: The license plate characters as read by the LPR matcher.
- **{Read.PlateState}**: The license plate's issuing state, province, or country.
- **{Read.Timestamp}**: The date and time of the plate read.
- **{Read.User}**: The name of the Patroller unit that read the plate.

Example: Here is what the config file looks like with all the read attributes

```
included:<Presentation IgnoreSizeConstraints="False"
DisplayResourcesIds="False" SearchFormState=""
AutoLoadHighResImages="False" ReadDescription="{Read.Plate},
{Read.Confidence Score}%, {Read.PlateState}, {Read.Timestamp}&#13;
{Read.Address}, User:{Read.User}"/>
```

- To customize the display of hit-related information in a tile, add the "HitDescription=" attribute, followed by any of the following parameters.

NOTE: Add the character  if you want to force a carriage return in the Security Desk tile.

- **{Hit.Category}:** The "category" attribute of the hotlist or permit list.
- **{Hit.Id}:** The GUID of the hit.
- **{Hit.MatchPlate}:** The plate number that was matched by the LPR matcher.
- **{Hit.Rule}:** The name of the hotlist or permit list entity in Security Center.
- **{Hit.Timestamp}:** The date and time of the hit.
- **{Hit.Type}:** The type if hit (hotlist, permit, overtime, MLPI).
- **{Hit.User}:** The name of the Patroller unit that raised the hit.
- **{Hit.Watermark}:** The watermark of the hit.

Example: Here is what the config file looks like with all the read and hit attributes

```
included:<Presentation IgnoreSizeConstraints="False"
DisplayResourcesIds="False" SearchFormState=""
AutoLoadHighResImages="true" ReadDescription="{Read.Plate},
={Read.Confidence Score}%, {Read.PlateState}, {Read.Timestamp}&#13;
{Read.Address}, User: {Read.User}" HitDescription="{Read.Plate},
{Read.ConfidenceScore}%, {Read.PlateState}, {Read.Timestamp},
{Read.Address}&#13;{Hit.Type}, {Hit.Rule} / {Hit.MatchPlate},
{Hit.Timestamp}&#13;Category: {Hit.Category}, User: {Hit.User}&#13;
{Hit.Id}"/>
```

NOTE: You can add read information to a hit description because all hits are linked to at least one read. For example, you may want both the read and hit timestamps in the hit description because there may be a delay in the hit being processed.

- Save and close Notepad.
- Start Security Desk.

The Monitoring task tiles will now display the LPR information you added to the config file.

After you finish

Repeat these steps on any Security Desk client machine that requires specific LPR information in Monitoring task tiles.

Monitoring LPR events in tile mode

By default, LPR events are displayed in the canvas in tile mode, which allows you to view information about the read or hit, view the plate images from the events in high resolution, print hits, and so on, in individual tiles.




To monitor LPR events in tile mode:

- 1 In the **Monitoring** task, select an LPR event in a tile, or double-click an event from the event list.



The following information about the LPR event is displayed in the tile by default:

- **Entity name:** Name of the entity you are monitoring, shown in the tile toolbar.
 - **LPR event name:** Event type (License plate read, License plate hit, and so on), shown in the tile toolbar.
 - **Tile background color:**
 - *Black* (Default). Plate read event.
 - *Red* (Default). Hotlist hit event.
 - *Green* (Default). Permit hit event.
 - *Blue* (Default). Shared permit hit and overtime hit event.
- NOTE:** You can change the default colors of LPR events from *hotlists*, *overtime rules*, and *permit restrictions* in Config Tool. For more information, see the *Security Center Administrator Guide*.
- **Context image:** Wide-angled image of the vehicle that was read by the *LPR unit* context camera.
 - **Plate image:** Image captured by the LPR camera and the OCR interpretation from the event.
 - **Plate number:** License plate number.
 - **Plate state:** Origin of the license plate.

- **Date and time:** Date and time of the plate capture assigned to the hit rule that matched the plate.
 - **Address:** Location of the unit when the plate image was captured.
NOTE: The address is only shown if the *geocoder* module is enabled in Config Tool. If Patroller is not equipped with maps, then the address is only shown if the geocoder is enabled to resolve the GPS position.
 - **(Hits only) Hit rule:** Hit rule that produced the hit.
 - **(Overtime hits only) Tire/Overview image:** Wheel image captured by the *wheel-imaging* camera that is mounted at the back of the Patroller vehicle. Wheel images are only shown if the hit was captured by a Patroller that supports wheel imaging.
- 2 To check the *watermark* status of the LPR event, right-click inside the tile, and then click **Verify watermark**.
A watermark confirms that an LPR event is valid (for example, that it has not been tampered with). Security Center adds a watermark to all reads and hits recorded by fixed Sharps, and Patroller adds a watermark to Sharps installed on the vehicle. The three watermark statuses are the following:
 - Good (🟢).
 - Invalid (🔴).
 - If no icon appears, the watermark has been tampered with.
 - 3 To view a high-resolution monochrome image of the license plate captured by the LPR camera, click  in the tile.
This button is only available if Security Desk is not already configured to display the high-resolution images by default.
 - 4 (Hits only) To view more information about the hit, such as its hotlist attributes, click  in the tile (user, accept or reject reason, plate state, and so on).
 - 5 (Hits only) To print the event data as proof of the violation, click  in the tile.

Related Topics

[Printing hit reports](#) on page 313

Monitoring LPR events in map mode

You can use map mode in the *Monitoring* task to view all the LPR events on a map.

What you should know

In map mode, the canvas displays a road map. The map opens centered on the location you zoomed in to, the last time you switched to map mode. You can use your mouse to pan or zoom on the map.

NOTE: The map mode can only be used to display static LPR events. To show Patroller positions on a map, use the *Patroller tracking* task. To work with a general purpose map, display a map (🗺️) in a tile, or use the *Maps* task.

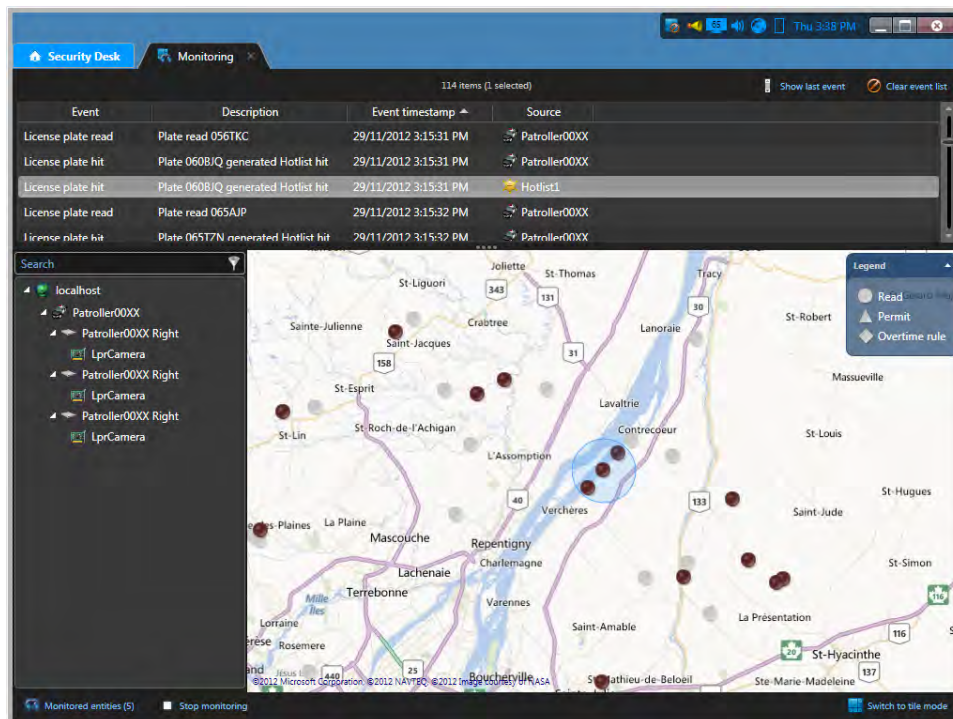
The following symbols represent each LPR event type on the map:

- **Circle:** Reads and hotlist hits.
- **Triangle:** Permit reads and hits.
- **Diamond:** Overtime reads and hits.

You can change the default colors of LPR events from *hotlist*, *overtime rule*, and *permit restriction* in Config Tool. For more information, see the *Security Center Administrator Guide*.

To monitor LPR events in Map mode:

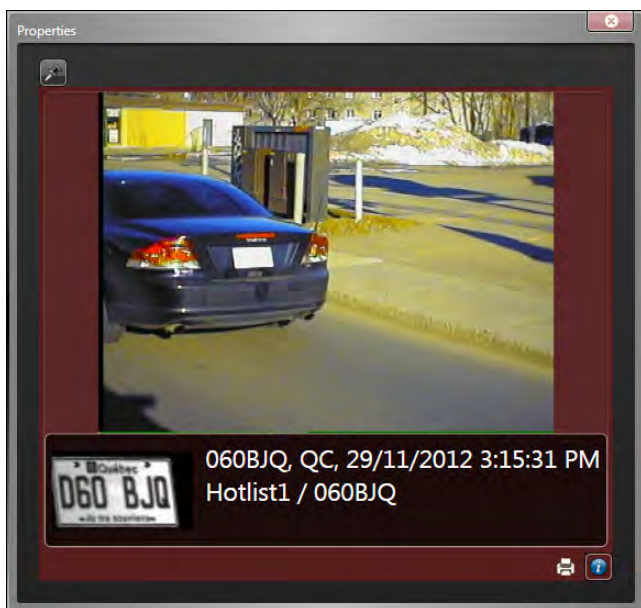
- 1 In the **Monitoring** task, click **Switch to map mode** (🗺️).



- 2 To locate an event on the map, double-click the event in the event list.

The event location is displayed on the map and the event is circled.

- 3 To view information about the event, click the event on the map.



The *Properties* window opens. The event properties and commands shown in the *Properties* window are similar to those available in tile mode.

- 4 To keep the *Properties* window open, click **Push pin** (📌).

Related Topics

[Replaying Patroller routes](#) on page 330

Reads, hits, hotlists, and permits

This section includes the following topics:

- ["About hotlists"](#) on page 303
- ["About permits"](#) on page 304
- ["Editing hotlists and permit lists"](#) on page 306
- ["Hotlist annotation fields"](#) on page 307
- ["Investigating reported hits"](#) on page 308
- ["Investigating reported hit statistics"](#) on page 311
- ["Printing hit reports"](#) on page 313
- ["Editing plate reads"](#) on page 315
- ["Investigating reported license plate reads"](#) on page 316
- ["Investigating reported read statistics"](#) on page 318
- ["Investigating reported reads \(Multi-region\)"](#) on page 320
- ["Investigating reported hits \(Multi-region\)"](#) on page 322
- ["Investigating reported reads and hits per day"](#) on page 324
- ["Investigating reported reads and hits per parking zone"](#) on page 326

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.

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

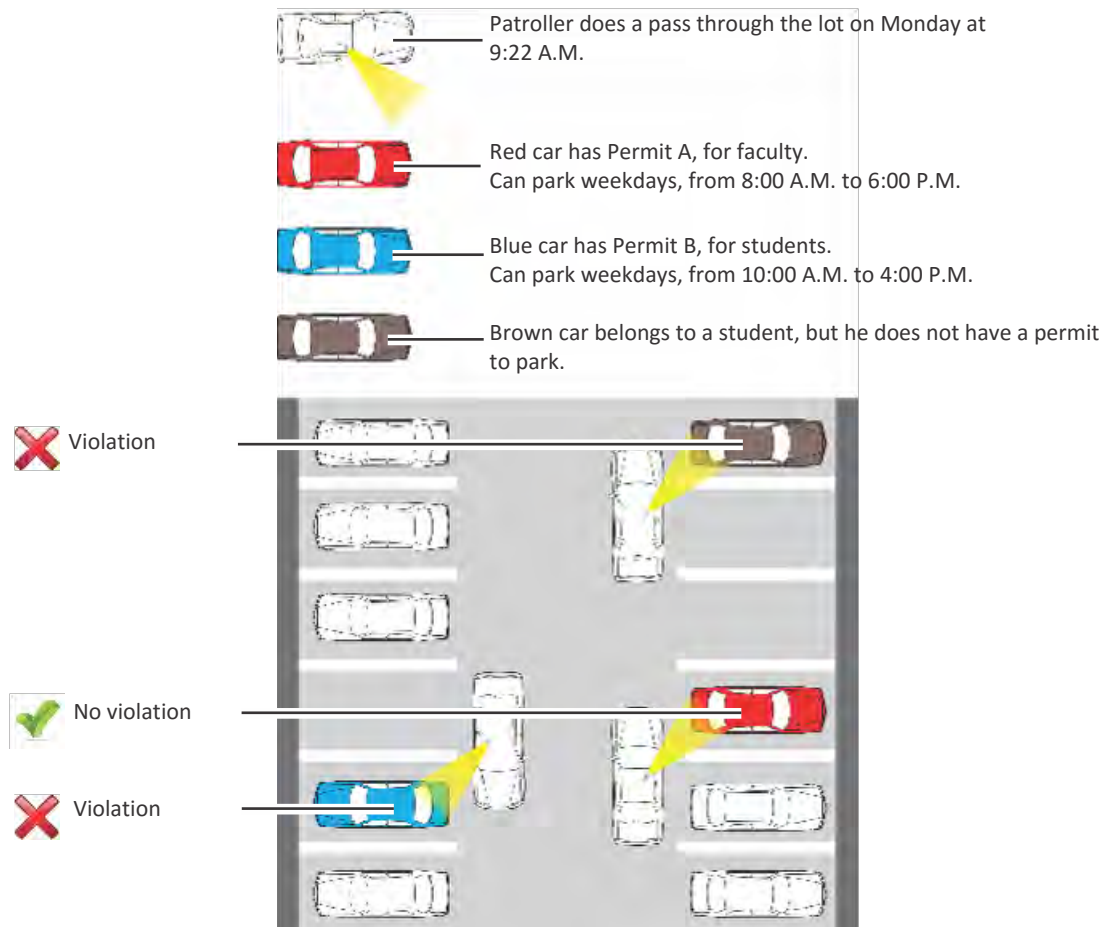
In City Parking Enforcement, you create the permit list and configure its basic properties, but you do not need to define a parking lot or permit restriction. It is the city or municipality that decides when and where the permit is applicable. When you're patrolling, you choose which permit to enforce 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.



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.

Editing hotlists and permit lists

You can edit a *hotlist* or *permit* list using the *Hotlist and permit editor* task.

Before you begin

The hotlist or permit list must be created in Config Tool, the *Enable editor support* option in the entity's Properties tab must be selected, and the user or user groups editing the lists must be granted the required privileges. The changes you can make to a hotlist or permit list might be limited, depending on which privileges you have.

What you should know

Using the *Hotlist and permit editor*, you can add, edit, or delete items from existing lists that were created in *Config Tool*. When you edit a hotlist or permit list, the text file is updated and your Patrollers or Sharps receive the new information.

The following conditions apply:

- Only the first 100,000 rows of a hotlist are loaded in Security Desk.
- If an error occurs while the hotlist is being loaded, the load stops and an error message is shown. However, you can still edit the lists that were loaded before the error occurred.

To edit a hotlist or permit list:

- 1 From the home page, open the **Hotlist and permit editor** task.
The available hotlists and permit lists are displayed in the column on the left.
- 2 Select the hotlist or permit list that you want to edit.
- 3 From the drop-down list, select an LPR Manager, and click **Load**.
- 4 To find a specific row in the list, type the license plate number in the *Search* box.
- 5 Do one of the following:
 - To add a row to your list, click **Add** (+).
 - To delete a row, select a row from your list, and then click **Remove** (X).
 - To edit a row, click an individual item on your list.
- 6 Click **Save**.

The source file of the hotlist or permit list is updated with the changes.

Example

A hotlist of stolen vehicles is downloaded from the ministry of justice each night at midnight. Every morning, when the officers begin their shift, they load the latest hotlist into a Patroller. During the day, some vehicles on the list are found, and new vehicles are stolen. You can remove the vehicles that were found from the list, and add the newly stolen vehicles, so that all the Patrollers have the updated hotlist.

Related Topics

[Overview of the Hotlist and permit editor task](#) on page 474

Hotlist annotation fields

Hit annotation fields are properties of a hit that are not displayed by default in Security Desk (for example, the vehicle's VIN or serial number). They can be fields that are extracted from the hotlist the plate was matched with, or they can be other fields, such as *UserEditedPlate*, custom fields, and so on.

Custom annotation fields are only available if they have been created in Config Tool. For information about adding annotation fields, see the *Security Center Administrator Guide*.

The following are examples of hotlist annotation fields:

- **{Category}**: For hotlist hits, the *Category* is the reason a license plate is of interest (for example, *Amber alert*, *Wanted felon*, *Stolen*, and so on). For *permit hits*, the *Category* is the type of permit (for example, *Zone 35*, *Zone 50*, and so on).

NOTE: This is a mandatory field for hotlists and *permits*. The category is taken from the hotlist or permit list that the license plate is matched against. For a *new wanted* license plate, the category is defined in the LPR settings *new wanted* categories and downloaded to a Patroller. When a *new wanted* license plate is entered manually in Patroller, the user selects the appropriate *Category* from the downloaded list.

- **{MatchPlate}**: The plate number as it appears in the hotlist.
- **{PlateState}**: The plate state/province as it appears in the hotlist.
- **{EffectiveDate}**: The hotlist is effective from this date.
- **{ExpiryDate}**: The hotlist expires on this date.
- **{UserEditedPlate}**: The license plate was edited manually.

Investigating reported hits

You can investigate *hits* reported within a time range and geographic area, using the *Hits* report.


Before you begin

To view your query results in the canvas, you must know how to [monitor LPR events in Security Desk in map mode](#).

What you should know

If you must report on all the hits that occurred in a specific region at a certain time, you can select the region, and the time range. If you want to see how many hits one Patroller got during their shift, you can search for that Patroller, and set a time range. If you want to see if a Patroller got a hit on a specific license plate, you can search for that license plate.

To investigate reported hits:

- 1 From the home page, open the **Hits** task.
- 2 To restrict your search to one or more specific areas, draw one or more regions in your map as follows:
 - a) In the *Filters* tab, click the **Region** filter.
 - b) Click **Switch to map mode**.
 - c) In the **Region** filter, click **Draw region**.
 - d) Drag your mouse pointer to create a box.
A numbered **Region** box is created.
 - e) To resize the region, drag the box handles.
 - f) To move the region, hold down the mouse button and drag the box to a new location.
 - g) Create other regions as required.
 - h) Select the region(s) of interest.
To view all the regions you created, click  in the *Filters* tab.
- 3 Set up the other query filters for your report. Choose one or more of the following filters:
 - **Accept reasons:** Reason selected by the Patroller user when enforcing a hit. Accept reasons are created and customized in Config Tool.
 - **Action taken:** Patroller hit actions (Accepted, Rejected, Not enforced) selected by the Patroller user. For fixed Sharps, a hit raised by the Hit Matcher module is always automatically Accepted and Enforced.
 - **Annotation fields:** Patroller hit annotations used by the Patroller user.
 - **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 has been 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.
 - **Hit rules:** Select the hit rules to include in the report.
 - **Hit type:** Select the type of hits to include in the report: *Permit*, *Shared permit*, *Overtime*, and *Hotlist*.

- **License plate:** Enter a *Full* or *Partial* license plate number.
 - **LPR units - Patrollers:** Restrict the search to Patroller units (including all their fitted LPR units) and/or LPR units representing fixed Sharp cameras on the Patroller unit.
 - **Offload timestamp:** The date and time that the Patroller offloaded the reads/hits to Security Center.
 - **Reject reason:** Reason selected by the Patroller user when rejecting a hit. Reject reasons are created and customized in Config Tool. This filter only affects the value in the *Rejected hits* column.
 - **Users:** Select the Patroller user name, or the Patrollers' parent user groups.
- 4 Click **Generate report**.
- The hits are listed in the report pane.
- 5 View your query results in the canvas, in one of the following modes:
- **tile mode:** To show the LPR event in a tile, double-click or drag the item from the report pane to the canvas.
 - **map mode:** To locate an LPR event on the map, double-click the item in the report pane.

After you finish

[Print a hit for proof of violation if required.](#)

Report pane columns for the Hits 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.

- **Accept reasons:** Reason selected by the Patroller user when enforcing a hit. Accept reasons are created and configured in Config Tool.
- **Address:** Location of the LPR read.
- **Annotation fields:** Any annotation field defined in **System > LPR Settings** in the Config Tool. Shown in brackets.
- **Context image:** Wide angle color image of the vehicle captured by the context camera.
- **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 have been 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 timestamp:** Date and time that the event occurred.
- **Latitude:** The coordinates of where the LPR event occurred.
- **Longitude:** The coordinates of where the LPR event occurred.
- **Offload timestamp:** The date and time that the Patroller offloaded the reads/hits to Security Center.
- **Patroller:** Patroller entity name. The Patroller entity name field is not populated for fixed Sharp cameras.
- **Plate image:** License plate image captured by the LPR camera.
- **Plate origin:** State that issued the license plate.

- **Plate read:** The license plate read generated by the Sharp unit.
- **Protected:** Record is not purged from the database of its parent AutoVu LPR Manager ES when the Hit Retention period (for this record) expires.
- **Reject reason:** Reason selected by the Patroller user when rejecting a hit.
- **Rule:** Hit rule that matched the plate read.
- **Unit:** The LPR unit that read the plate and populated for a Patroller (for example, Patroller - Left, Patroller - Right, etc.), and for a fixed Sharp.
- **User:** The Patroller user name. Not available at a Security Center Federation host for federated Patroller entities.
- **Wheel image:** Image of the vehicle wheels. Used for virtual tire-chalking.


Investigating reported hit statistics

You can quickly investigate hit statistics within a time range and geographic area, using the hits statistics report.

What you should know

To view your query results in the canvas, you must know [how to monitor LPR events](#) in Security Desk.

To investigate reported hit statistics:

- 1 From the home page, open the **Hits** task.
- 2 To restrict your search to one or more specific areas, draw one or more regions in your map as follows:
 - a) In the *Filters* tab, click the **Region** filter.
 - b) Click **Switch to map mode**.
 - c) In the **Region** filter, click **Draw region**.
 - d) Drag your mouse pointer to create a box.
A numbered **Region** box is created.
 - e) To resize the region, drag the box handles.
 - f) To move the region, hold down the mouse button and drag the box to a new location.
 - g) Create other regions as required.
 - h) Select the region(s) of interest.
To view all the regions you created, click  in the *Filters* tab.
- 3 Set up the other query filters for your report. Choose one or more of the following filters:
 - **Accept reasons:** Reason selected by the Patroller user when enforcing a hit. Accept reasons are created and customized in Config Tool.
 - **Action taken:** Patroller hit actions (Accepted, Rejected, Not enforced) selected by the Patroller user. For fixed Sharps, a hit raised by the Hit Matcher module is always automatically Accepted and Enforced.
 - **Annotation fields:** Patroller hit annotations used by the Patroller user.
 - **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 has been 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.
 - **Hit rules:** Select the hit rules to include in the report.
 - **Hit type:** Select the type of hits to include in the report: *Permit*, *Shared permit*, *Overtime*, and *Hotlist*.
 - **License plate:** Enter a *Full* or *Partial* license plate number.
 - **LPR units - Patrollers:** Restrict the search to Patroller units (including all their fitted LPR units) and/or LPR units representing fixed Sharp cameras on the Patroller unit.
 - **Offload timestamp:** The date and time that the Patroller offloaded the reads/hits to Security Center.

- **Reject reason:** Reason selected by the Patroller user when rejecting a hit. Reject reasons are created and customized in Config Tool. This filter only affects the value in the *Rejected hits* column.
 - **Users:** Select the Patroller user name, or the Patrollers' parent user groups.
- 4 Expand the options under the **Generate report** button and select **Generate report statistics**.
The hits are listed in the report pane.

Example

If you must quickly report how many hits occurred in a specific region at a certain time, you can select the region, and the time range.


Printing hit reports

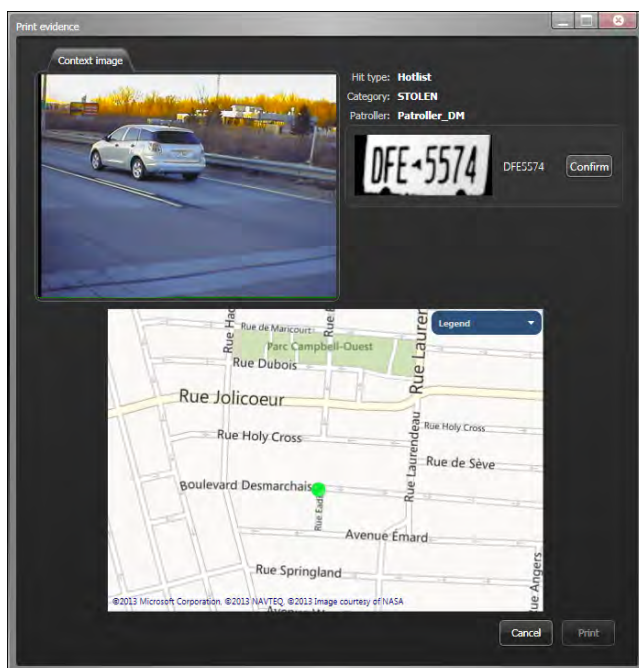
You can print a *Hits-Photo evidence* report for License plate hit events from the Monitoring task and other LPR tasks.

What you should know

The printed report includes the current date, hit information (plate number, GPS coordinates, address, hit date, hit type, and so on), the LPR image, the context image, wheel images (if applicable), and the map context.

To print a hit report:


- 1 From the home page, open the Monitoring task or an LPR task.
- 2 [If needed, generate your report.](#)
- 3 Select a hit event in a tile or on the map.
- 4 In the tile or *Properties* window, click .
- 5 In the *Print evidence* dialog box, confirm the license plate number so you do not print a false read.





- 6 Confirm that the OCR interpretation matches the LPR image.
- 7 In the text box, type the license plate number, and then click **Confirm**.
- 8 Click **Print**, select a printer, and then click **Print**.

The *Hits-Photo evidence* report is printed.

Hits - Photo evidence - 4/16/2012 (Page 1/1)

Hit information		LPR
Plate read	J21BQJ	
Location	(45.52704),(-73.69854)	
Address	2642 Boul O'Brien	
Date	16/04/2012 12:16:49 AM	
Hit type	Hotlist	
Hotlist name	PMessier- Hotlist	
Category	STOLEN	
Patroller	Patroller_DM	
User		

Context	Map
	

Editing plate reads

In certain situations, you may need to modify a plate read in Security Desk. This may be necessary if you notice that the system has incorrectly captured a plate read, or if the system prompts you to verify a plate read that is unclear (low confidence score).

What you should know

- Depending on your user privileges, you can modify plate reads that are displayed in tiles. You can edit plate reads in *Reads* reports, *Reads (Multi-region)* reports, monitoring tiles, and in alarms triggered by license plate read events.
- You cannot edit a plate read if the read is protected, a hit, or if the read is from a federated system or an MLPI inventory.
- When a plate read is edited, if there is a confidence score associated with the plate read, the confidence score will be changed to 100%.
- The details of the plate read edit will appear in the *Activity trails* report.

To modify a plate read:

- 1 From the license plate read tile, click **Modify** (✎).

NOTE: If you are trying to modify a plate read in a *Reads* report, you must first double-click the read to display it in a tile.

- 2 In the *Edit read* window, manually modify the **Plate** and/or **State** information as required.
- 3 Click **Save**.

In *Reads* reports, the **Edited** column will show you if the plate read has been edited. For more information on displaying columns, refer to the [Reporting task workspace overview](#).

Investigating reported license plate reads

You can find the license plate reads reported within a time range and geographic area, using the *Reads* report.


Before you begin

To view your query results in the canvas, you must know how to [monitor LPR events in Security Desk in map mode](#).

What you should know

If you must report on all the reads that occurred in a specific region at a certain time, you can select the region, and the time range. If you want to see how many reads a Patroller got during their shift, you can search for that Patroller, and set a time range. If you want to see if a Patroller got a read on a specific license plate, you can search for that license plate.

To investigate reported license plate reads:

- 1 From the home page, open the **Reads** task.
- 2 To restrict your search to one or more specific areas, draw one or more regions in your map as follows:
 - a) In the *Filters* tab, click the **Region** filter.
 - b) Click **Switch to map mode**.
 - c) In the **Region** filter, click **Draw region**.
 - d) Drag your mouse pointer to create a box.
A numbered **Region** box is created.
 - e) To resize the region, drag the box handles.
 - f) To move the region, hold down the mouse button and drag the box to a new location.
 - g) Create other regions as required.
 - h) Select the region(s) of interest.
To view all the regions you created, click  in the *Filters* tab.
- 3 Set up the other 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 has been made visible to you when it was created or last configured.
 - **Generated a hit:** Include reads that generated a hit in the report.
 - **Hit rules:** Select the hit rules to include in the report.
 - **License plate:** Enter a *Full* or *Partial* license plate number.
 - **LPR units - Patrollers:** Restrict the search to Patroller units (including all their fitted LPR units) and/or LPR units representing fixed Sharp cameras on the Patroller unit.
 - **Offload timestamp:** The date and time that the Patroller offloaded the reads/hits to Security Center.
 - **Rule:** Hit rule that matched the plate read.
 - **Users:** Select the Patroller user name, or the Patrollers' parent user groups.

4 Click **Generate report**.

The reads are listed in the report pane.

5 View your query results in the canvas, in one of the following modes:

- **tile mode:** To show the LPR event in a tile, double-click or drag the item from the report pane to the canvas.
- **map mode:** To locate an LPR event on the map, double-click the item in the report pane.

Report pane columns for the Reads 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.

- **Address:** Location of the LPR read.
- **Context image:** Wide angle color image of the vehicle captured by the context camera.
- **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 have been 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 timestamp:** Date and time that the event occurred.
- **Generated a hit:** Indicates if the read generated a hit with a checkmark.
- **Latitude:** The coordinates of where the LPR event occurred.
- **Longitude:** The coordinates of where the LPR event occurred.
- **Lot:** Parking zone where a given parking regulation is in force.
- **Manual capture:** Displays the plate number entered manually by the Patroller user.
- **Offload timestamp:** The date and time that the Patroller offloaded the reads/hits to Security Center.
- **Patroller:** Patroller entity name. The Patroller entity name field is not populated for fixed Sharp cameras.
- **Permit name:** Name of the permit list under the permit restriction.
- **Plate image:** License plate image captured by the LPR camera.
- **Plate origin:** State that issued the license plate.
- **Plate read:** The license plate read generated by the Sharp unit.
- **Protected:** Record is not purged from the database of its parent AutoVu LPR Manager ES when the Hit Retention period (for this record) expires.
- **Rule:** Hit rule that matched the plate read.
- **Unit:** The LPR unit that read the plate and populated for a Patroller (for example, Patroller - Left, Patroller - Right, etc.), and for a fixed Sharp.
- **Wheel image:** Image of the vehicle wheels. Used for virtual tire-chalking.

Investigating reported read statistics

You can quickly investigate read statistics within a time range and geographic area, using the reads statistics report.


What you should know

To view your query results in the canvas, you must know [how to monitor LPR events](#) in Security Desk.

To investigate reported read statistics:

- 1 From the home page, open the **Reads** task.
- 2 To restrict your search to one or more specific areas, draw one or more regions in your map as follows:
 - a) In the *Filters* tab, click the **Region** filter.
 - b) Click **Switch to map mode**.
 - c) In the **Region** filter, click **Draw region**.
 - d) Drag your mouse pointer to create a box.

A numbered **Region** box is created.
 - e) To resize the region, drag the box handles.
 - f) To move the region, hold down the mouse button and drag the box to a new location.
 - g) Create other regions as required.
 - h) Select the region(s) of interest.

To view all the regions you created, click  in the *Filters* tab.
- 3 Set up the other 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 has been made visible to you when it was created or last configured.
 - **Generated a hit:** Include reads that generated a hit in the report.
 - **Hit rules:** Select the hit rules to include in the report.
 - **License plate:** Enter a *Full* or *Partial* license plate number.
 - **LPR units - Patrollers:** Restrict the search to Patroller units (including all their fitted LPR units) and/or LPR units representing fixed Sharp cameras on the Patroller unit.
 - **Offload timestamp:** The date and time that the Patroller offloaded the reads/hits to Security Center.
 - **Rule:** Hit rule that matched the plate read.
 - **Users:** Select the Patroller user name, or the Patrollers' parent user groups.
- 4 Click the small arrow on the right of the **Generate report** button and select **Generate report statistics**.

The read count is listed in the report pane.

Example

If you must quickly report how many reads occurred in a specific region at a certain time, you can select the region, and the time range.

Investigating reported reads (Multi-region)

You can view the number of reads common to multiple regions of interest for a specific time period, using the *Reads (Multi-region)* report.


What you should know

To view your query results in the canvas, you must know [how to monitor LPR events](#) in Security Desk.

To investigate the reads for multiple regions:

- 1 From the home page, open the **Reads (Multi-region)** task.
- 2 To restrict your search to one or more specific areas, draw one or more regions in your map as follows:
 - a) In the *Filters* tab, click the **Region** filter.
 - b) Click **Switch to map mode**.
 - c) In the **Region** filter, click **Draw region**.
 - d) Drag your mouse pointer to create a box.

A numbered **Region** box is created.
 - e) To resize the region, drag the box handles.
 - f) To move the region, hold down the mouse button and drag the box to a new location.
 - g) Create other regions as required.
 - h) Select the region(s) of interest.

To view all the regions you created, click  in the *Filters* tab.
- 3 Set up the other 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 has been 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.
 - **Hit rules:** Select the hit rules to include in the report.
 - **License plate:** Enter a *Full* or *Partial* license plate number.
 - **LPR units - Patrollers:** Restrict the search to Patroller units (including all their fitted LPR units) and/or LPR units representing fixed Sharp cameras on the Patroller unit.
- 4 Click **Generate report**.

The reads that are common to all regions you have defined are listed in the report pane.
- 5 View your query results in the canvas, in one of the following modes:
 - **Tile mode:** To show the LPR event in a tile, double-click or drag the item from the report pane to the canvas.
 - **Map mode:** To locate an LPR event on the map, double-click the item in the report pane.

Example

If you must report on all the reads that occurred in multiple regions for a specific time period, you can create multiple regions, and specify the time range.

Report pane columns for the Reads (Multi-region) 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 have been made visible to you when they were created or last configured.
- **Rule:** Hit rule that matched the plate read.


Investigating reported hits (Multi-region)

You can view the number of hits common to multiple regions of interest for a specific time period, using the *Hits (Multi-region)* report.

What you should know

To view your query results in the canvas, you must know [how to monitor LPR events](#) in Security Desk.

To investigate the hits for multiple regions:

- 1 From the home page, open the **Hits (Multi-region)** task.
- 2 To restrict your search to one or more specific areas, draw one or more regions in your map as follows:
 - a) In the *Filters* tab, click the **Region** filter.
 - b) Click **Switch to map mode**.
 - c) In the **Region** filter, click **Draw region**.
 - d) Drag your mouse pointer to create a box.
A numbered **Region** box is created.
 - e) To resize the region, drag the box handles.
 - f) To move the region, hold down the mouse button and drag the box to a new location.
 - g) Create other regions as required.
 - h) Select the region(s) of interest.
To view all the regions you created, click  in the *Filters* tab.
- 3 Set up the other 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 has been 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.
 - **Hit rules:** Select the hit rules to include in the report.
 - **License plate:** Enter a *Full* or *Partial* license plate number.
 - **LPR units - Patrollers:** Restrict the search to Patroller units (including all their fitted LPR units) and/or LPR units representing fixed Sharp cameras on the Patroller unit.
- 4 Click **Generate report**.
The reads that are common to all regions you have defined are listed in the report pane.
- 5 View your query results in the canvas, in one of the following modes:
 - **Tile mode:** To show the LPR event in a tile, double-click or drag the item from the report pane to the canvas.
 - **Map mode:** To locate an LPR event on the map, double-click the item in the report pane.

Example

If you must report on all the hits that occurred in multiple regions for a specific time period, you can create multiple regions, and specify the time range.

Report pane columns for the Hits (Multi-region) 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 have been made visible to you when they were created or last configured.
- **Rule:** Hit rule that matched the plate read.

Investigating reported reads and hits per day

You can view the number of reads and hits per day for a specific date range, using the *Reads/hits per day* report.

What you should know

The statistics in this report helps you to assess the performance of Patrollers and fixed Sharp cameras in the field. For example, if you want to see how efficient the location of a mounted fixed Sharp is, you can search for that Sharp, and set a time range of a week.

To investigate the reads/hits reported on a particular day:

- 1 From the home page, open the **Reads/hits per day** 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 has been made visible to you when it was created or last configured.
 - **Hit rules:** Select the hit rules to include in the report.
 - **Hit type:** Select the type of hits to include in the report: *Permit*, *Shared permit*, *Overtime*, and *Hotlist*.
 - **LPR units - Patrollers:** Restrict the search to Patroller units (including all their fitted LPR units) and/or LPR units representing fixed Sharp cameras on the Patroller unit.
 - **Reject reason:** Reason selected by the Patroller user when rejecting a hit. Reject reasons are created and customized in Config Tool. This filter only affects the value in the *Rejected hits* column.
 - **Time range:** The time range for the report.
 - **Users:** Select the Patroller user name, or the Patrollers' parent user groups.
- 3 Click **Generate report**.

The read and hit events are listed in the report pane.
- 4 View the statistics on the total number of reads, hits, and hit actions taken during the selected time range in the *Statistics* section.

Report pane columns for the Reads/hits per day 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 have been made visible to you when they were created or last configured.
- **Enforced hits:** Number of enforced hits.
- **Hits:**

Number of hits.

NOTE: If the *Hit rules* and *Hit type* query filters are used, this value might not be the total number of hits in the day.

- **Not enforced hits:** Number of hits that were not enforced.
- **Reads:** Number of license plate reads.
- **Rejected hits:** Number of hits that were rejected.

Investigating reported reads and hits per parking zone

You can view the number of reads and hits per *parking zone* for a specific date range, using the *Reads/hits per zone* report.

What you should know

By viewing the activity within a parking zone, you can assess the performance of Patrollers and fixed Sharp cameras in the field. For example, if you want to see how efficient the location of a mounted fixed Sharp is, you can search for that Sharp, and set a time range of a week.

To investigate the reads/hits reported in a parking zone:

- 1 From the home page, open the **Reads/hits per zone** 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 has been made visible to you when it was created or last configured.
 - **Hit rules:** Select the hit rules to include in the report.
 - **Hit type:** Select the type of hits to include in the report: *Permit*, *Shared permit*, *Overtime*, and *Hotlist*.
 - **LPR units - Patrollers:** Restrict the search to Patroller units (including all their fitted LPR units) and/or LPR units representing fixed Sharp cameras on the Patroller unit.
 - **Reject reason:** Reason selected by the Patroller user when rejecting a hit. Reject reasons are created and customized in Config Tool. This filter only affects the value in the *Rejected hits* column.
 - **Time range:** The time range for the report.
 - **Users:** Select the Patroller user name, or the Patrollers' parent user groups.
- 3 Click **Generate report**.
The read and hit events are listed in the report pane.
- 4 View the statistics on the total number of reads, hits, and hit actions taken during the selected time range in the *Statistics* section.

Report pane columns for the Reads/hits per zone 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 have been made visible to you when they were created or last configured.
- **Enforced hits:** Number of enforced hits.
- **Hits:**
Number of hits.

NOTE: If the *Hit rules* and *Hit type* query filters are used, this value might not be the total number of hits in the day.

- **Not enforced hits:** Number of hits that were not enforced.
- **Reads:** Number of license plate reads.
- **Rejected hits:** Number of hits that were rejected.
- **Time zone:** Time zone of the unit.

Patroller

This section includes the following topics:

- ["About AutoVu Patroller"](#) on page 329
- ["Replaying Patroller routes"](#) on page 330
- ["Tracking the current location of a Patroller"](#) on page 331
- ["Investigating how Patroller applications are used daily"](#) on page 332
- ["Investigating logon/logoff records of Patrollers"](#) on page 334
- ["Investigating the number of vehicles in parking zones"](#) on page 335

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.

Replaying Patroller routes

You can replay the route taken by a Patroller on a given date on a map, using the [Patroller tracking](#) report.

Before you begin

To view your query results in the canvas, you must know how to [monitor LPR events in Security Desk in map mode](#).

What you should know

The Patroller tracking report gives you a more visual representation than the *Hits* or *Reads* reports. For example, if you want to see the exact route a Patroller took during their shift select that Patroller, and the date of their shift.

An animated playback of the Patroller route is displayed in map mode, and a graphical representation of the Patroller route is displayed in the timeline chronologically. In the map, the 15 LPR events that occurred before and after the current Patroller location are displayed. You can navigate through the route from the timeline, and review the hits and reads captured by the Patroller.

To replay a Patroller route:

- 1 From the home page, open the Patroller tracking task.
- 2 From the **Patroller** drop-down list, select a Patroller unit.
- 3 Click **Date**, and select the day you want to view.
- 4 Click **Refresh**.

Security Center receives the Patroller data from the *database*. The route is plotted on the map, and on the timeline.

- 5 To navigate through the Patroller route and locate LPR events, use the timeline controls.
- 6 To view the properties of an LPR event, double-click an item on the map.

After you finish

[Print a hit for proof of violation if required.](#)

Related Topics

[Overview of the Patroller tracking task](#) on page 476

[Patroller tracking timeline controls](#) on page 477

Tracking the current location of a Patroller

You can view the current location of Patroller vehicles on a map using the Patroller tracking report.

What you should know

Patroller requires a live connection to Security Center for this feature to work.

To view the current location of a Patroller:

- 1 From the home page, open the Patroller tracking task.
- 2 Click **Go live**.

Any active Patroller vehicles are plotted on the map, and you can see their current position.

Investigating how Patroller applications are used daily

You can view the *total* daily time (in minutes) and the *percentage* of daily time a Patroller application is opened, stopped, or shut down, using the Daily usage per Patroller report. You can also view the average amount of time the Patroller was opened, stopped, shut down, and so on, for the selected time range.

What you should know

This report is used in mobile Patroller installations only. You can use these statistics to calculate the efficiency of your Patrollers. For example, to view the statistics of a specific Patroller during their last shift, you can search for that Patroller, and set the time range.

To investigate how a Patroller application is used on a particular day:

- 1 From the home page, open the **Daily usage per Patroller** 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 has been made visible to you when it was created or last configured.
 - **Patrollers:** Restrict the search to Patroller units (including all their fitted LPR units).
 - **Time range:** The time range for the report.
- 3 Click **Generate report**.
The results are listed in the report pane.
- 4 In the **Statistics** section, review the following usage statistics of the selected Patroller:
 - **Operating time (Average):** Average operating time over the selected time range.
 - **Longest stop (min.) (Average):** Average longest stop time in minutes over the selected time range.
 - **Longest stop % (Average):** Average longest stop time percentage during the selected time range.
 - **Total Stop (min.)(Average):** Average total stop time in minutes during the selected time range.
 - **Total stop % (Average):** Average total stop time in percentage during the selected time range.
 - **Instances (Average):** Average number of times that Patroller was opened during the selected time range.
 - **Longest shutdown (min.) (Average):** Average longest shutdown time in minutes during the selected time range.
 - **Longest shutdown % (Average):** Average longest shutdown time in percentage during the selected time range.
 - **Total Shutdown (Average):** Average total shutdown time in minutes during the selected time range.
 - **Total shutdown % (Average):** Average total shutdown time in percentage during the selected time range.

Report pane columns for the Daily usage per Patroller 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 have been made visible to you when they were created or last configured.
- **Date:** Day of the Patroller shift.
- **Instances:** Total number of times the Patroller application is opened during the day.
- **Longest shutdown (%):** Percentage of Longest shutdown over the total number of minutes in a day.
- **Longest shutdown (min.):** Single longest number of minutes in a day that the Patroller application is closed.
- **Longest stop (%):** Percentage of longest stop time over operating time.
- **Longest shutdown (min.):** Single longest number of minutes in a day that the Patroller application is closed.
- **Operating time:** Total number of minutes in a day that the Patroller application is open.
- **Total shutdown (%):** Percentage of Total shutdown over the number of minutes in a day.
- **Total shutdown (min.):** Total number of minutes in a day that the Patroller application is closed. The total shutdown value plus the operating time value equals 1440 minutes.
- **Total stop (%):** Percentage of total stop time over operating time.
- **Total stop (min.):** Total number of minutes in operating time when the vehicle is stationary.

Investigating logon/logoff records of Patrollers

You can view the logon and logoff records for Patrollers during a specific time range, using the *Logons per Patroller* report.

What you should know

Using this report, you can keep track of which Patrollers are out in the field. This report is used in mobile Patroller installations only.

NOTE: When using this report at a Security Center Federation host, the User column will remain empty for federated Patroller entities because the user entities are not federated.

To investigate the logon/logoff records of a Patroller:

- 1 From the home page, open the **Logons per Patroller** 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 has been made visible to you when it was created or last configured.
 - **Patrollers:** Restrict the search to Patroller units (including all their fitted LPR units).
 - **Time range:** The time range for the report.
 - **Users:** Select the Patroller user name, or the Patrollers' parent user groups.
- 3 Click **Generate report**.

The results for the selected Patroller are listed in the report pane.

Report pane columns for the Logons per Patroller 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 have been made visible to you when they were created or last configured.
- **Date:** Day of the Patroller shift.
- **Log on/Log off:** Log on and log off timestamp.
- **User:** The Patroller user name. Not available at a Security Center Federation host for federated Patroller entities.

Investigating the number of vehicles in parking zones

You can view the number of vehicles parked in a *parking zone*, and the percentage of occupancy, using the *Zone occupancy* task.

What you should know

You can also use the *Zone occupancy* report to search for *overtime rules* and *permit restrictions* that occurred in a zone. For example, on a university campus or in an airport, you can find out the occupancy of a parking lot at certain times of the day. If the occupancy is always at full capacity during that time, the report can help you determine that you need more spots in your parking lot.

The percentage of occupancy of a parking zone is calculated differently whether the Patroller was used for *University Parking Enforcement* or for *City Parking Enforcement*.

Patroller configuration	Percentage of occupancy
University Parking Enforcement	Calculated using the specific zone selected in Patroller, which corresponds to a single parking lot defined in an overtime rule or in a permit restriction.
City Parking Enforcement	<ul style="list-style-type: none"> If an overtime rule is selected: calculated using all parking lots defined within the rule. If no overtime rule is selected: occupancy cannot be calculated because no parking lot is associated to a permit. In this case the <i>Spaces</i> and <i>Percentage of occupancy</i> columns will show 0.

To investigate the reads/hits reported in a parking zone:

- From the home page, open the **Zone occupancy** task.
- 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 has been made visible to you when it was created or last configured.
 - Hit rules:** Select the hit rules to include in the report.
 - Overtime and permit restriction:** Both rules have parking lots configured and each parking lot can be defined in terms of a number of parking spaces. This allows the occupancy to be estimated when selecting these rules in Patroller.
 - Patrollers:** Restrict the search to Patroller units (including all their fitted LPR units).
 - Time range:** The time range for the report.
- Click **Generate report**.
The results are listed in the report pane.
- View the statistics on the total number of vehicles in all the selected parking zones in the *Statistics* section.

Report pane columns for the Zone occupancy 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 have been made visible to you when they were created or last configured.
- **From/To:** Date and timestamp of read vehicles within the zone.
- **Lot:** Parking zone where a given parking regulation is in force.
- **Percentage Occupancy:** Percentage of occupied places within the parking zone.
- **Spaces:** Number of spaces in the parking lot.
- **To/from:** Date and timestamp of read vehicles within the zone.
- **Vehicles:** Number of vehicles that were read within the zone.
- **Zone:** The name of the Overtime rule or Permit restriction.

Mobile License Plate Inventory

This section includes the following topics:

- ["How AutoVu MLPI works"](#) on page 338
- ["Removing license plate reads from offload files"](#) on page 339
- ["Removing data from offload files"](#) on page 340
- ["Creating parking facility inventories"](#) on page 341
- ["Viewing and comparing parking facility inventories"](#) on page 344


How AutoVu MLPI works

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 AutoVu MLPI process works as follows:

- A *parking facility* is created in Config Tool. The parking facility describes the layout of the parking area in sectors and rows. For information about configuring a parking facility, see the *Security Center Administrator Guide*.
- Patroller routes are associated to sectors and rows configured in the parking facility. The sector and row of a *license plate read* represents the location of the vehicle in the parking facility.
- *AutoVu MLPI* Patroller (or Genetec approved handheld device) collects license plate reads in the parking facility, and then offloads the data to Security Center.

NOTE: Handheld device reads are imported to the LPR Manager database using the XML import module. A single *ghost patroller*, called XML import, appears in the list to identify this. No matter how many handheld devices exist, all their reads are imported to the same ghost patroller.

- Security Center polls the *Offload* folder for new MLPI data.
- The Inventory icon () in Security Desk indicates when there is new data that can be added to an inventory.

For more information about reconciling reads or about the MLPI solution, see the *AutoVu Patroller Mobile License Plate Inventory User Guide*.

Removing license plate reads from offload files

Before adding the data from an offload file to an inventory using the *Inventory management* task, you can remove license plate reads from the offload.

What you should know

You can only remove *unreconciled reads* from an offload file. You cannot compare inventories, since unreconciled reads have not been added to an inventory.

To remove a license plate read from an offload file:

- 1 From the home page, open the Inventory report task.
- 2 In the **Inventory** section in the **Filters** tab, click **Unreconciled reads**.
- 3 Set up other query filters to refine your search.
Example: In the **License plate** section, enter the plate numbers of the vehicles that were towed away since the plate reads were taken by Patroller.
- 4 To only display unreconciled reads that were manually removed, select the **Only show manually removed reads** option from the **Advanced search** section.
- 5 Click **Generate report**.
- 6 In the report pane, select the vehicle you want to remove.
- 7 At the bottom of the report pane, click **Remove** (✕).

The plate read is displayed as *Vehicle manually removed* in the *Statistics* section.

After you finish

After you have removed the unreconciled reads from the offload file, you can [create the inventory for the offload](#).

Related Topics

[Investigating reported license plate reads](#) on page 316

Removing data from offload files


You can remove the data in an offload file from the LPR Manager database.

What you should know

Patrollers and handheld devices offload to an *LPR Manager*. The offloads are duplicated and stored in the LPR Manager *database*. In the *Inventory management* task, the reads are associated with a parking facility, and they are marked as not yet part of an inventory.

If you delete an offload from the *Offloads* list, the reads are no longer linked to a parking facility. However, the data remains in the Security Center database as regular plate reads, and they can still be queried using the *Reads* task.

To remove data from an offload file:

- 1 From the home page, open the Inventory management task
- 2 In the *Offloads* section, select a Patroller from the list.
If a handheld device is used, use the Patroller named **XML Import**.
- 3 Under the *Offloads* section, click .

Creating parking facility inventories

You can add and reconcile MLPI license plate reads from an offload file to a parking facility inventory, using the *Inventory management* task.

Before you begin

Before adding the data from an offload files to an inventory, you can remove unreconciled plate reads from the offload, using the *Inventory Report* task.

What you should know

You must know the following about creating inventories:

- When new MLPI plate reads are available in the database, a notification appears on the Inventory icon (📄) in the notification tray. The inventory alert is updated every 10 minutes. You can also update the alert by right-clicking the Inventory icon, and clicking **Refresh**.
- You can only create one parking facility inventory at a time.
- If a Patroller offloads multiple times before an inventory is created, they are all grouped in a single entry.
- You cannot set the start time of an inventory. The first time you create an inventory, the start time is undefined. The next time you create an inventory, the start time is the end time of the previous inventory.
- Reconciling is when a read is confirmed and added to an inventory. If there is a conflict while reconciling a read to an inventory (for example, two vehicles with the same plate numbers, but from different states), you might have to manually confirm the read.
- A partial inventory is when you perform a spot check on an inventory at a specific time, and the reads are not reconciled with the previous inventory. This is useful if Patroller is unable to perform a complete sweep of a parking facility. For example, if there is a heavy snowfall and Patroller can only sweep half of the parking lot because the other half has not been plowed, a partial inventory can be created so the reads are still recorded.

To create a parking facility inventory:

- 1 From the home page, open the **Inventory management** task.

NOTE: The *Offloads* panel only contains information if an offload file has been duplicated and stored in the LPR Manager database.

The *Offloads* panel includes the following information:

- **Patroller:** Name of the Patroller unit that performed the offload.
 - NOTE:** A single *ghost patroller*, called XML import, is displayed for reads that were taken by a handheld device, because they were imported to the LPR Manager database using the XML import module.
- **First seen:** Timestamp of the first read in the offload.
- **Last seen:** Timestamp of last read in the offload.
- **Read count:** Number of reads in the offload.

- 2 From the **Parking facility** drop-down list, select the parking facility you want to add the inventory to.
- 3 Click **Create inventory**.

- 4 In the *Create inventory* dialog box, type the name of inventory, and the end time.
- 5 If you want to create a partial inventory, select **Partial**.
- 6 Click **Create**.

The plate reads are reconciled and the plate read data is added to the parking facility inventory.

- 7 If there is a conflict while the reads are being reconciled (for example, a license plate appears in two locations), then the *Plate confirmation* dialog box opens, and you must verify that the license plate in the context image is the same as the plate image and *OCR* read as follows:

TIP: You should only compare the LPR image and the OCR read, because the plate in the context image might be difficult to see.



- a) If the OCR reading is incorrect, type the correct license plate number in the **OCR reading** box.

NOTE: This plate read is tagged as *Edited* in the *Inventory report* task.

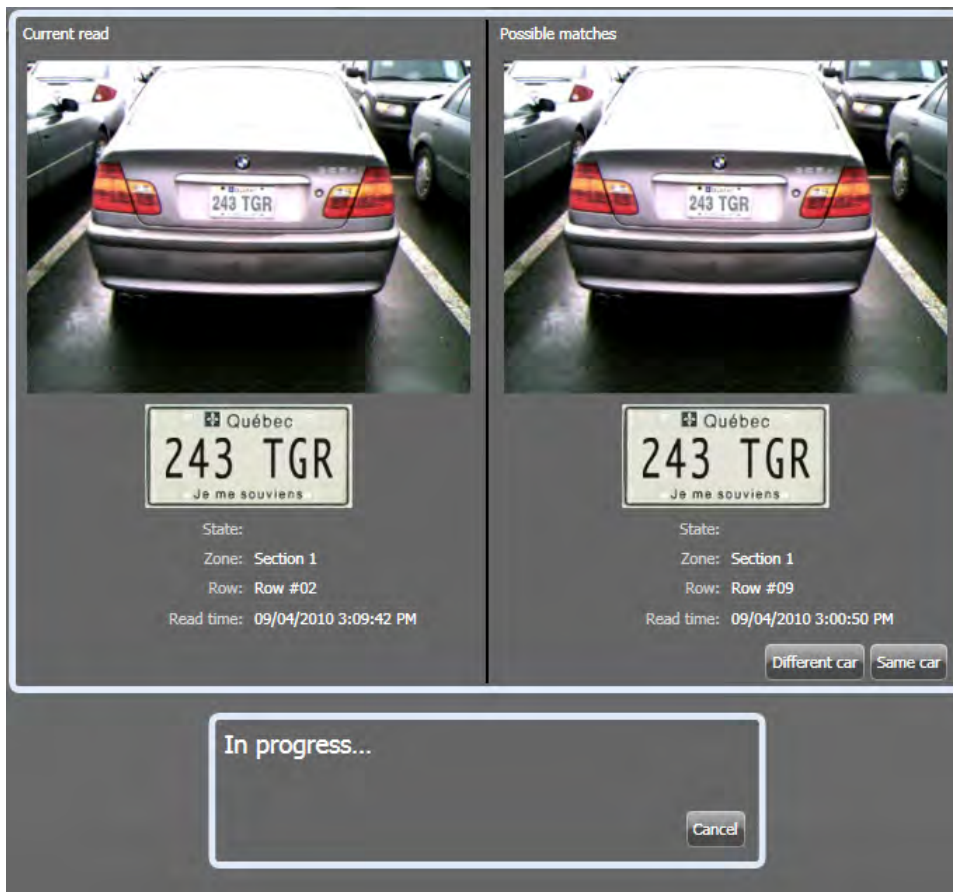
- b) If the OCR reading is correct, but the plate state is different, enter the state name in the **State** box.

You can enter the state abbreviation or full name.

- c) Click **Confirm**.

The data from the offload is added to the parking facility inventory.

- 8 If a conflict is detected during the inventory process (for example, a license plate appears in two locations), then a dialog box opens that displays the plate read in the current parking facility inventory (**Current read**), and the possible plate match (**Possible matches**) in the data it is trying to reconcile to that inventory.



Select one of the following:

- **Different car:** Select if the plate numbers are the same, but the plate state and the vehicle are different from the vehicle in the current inventory. The vehicle displayed under **Possible matches** is added as a new vehicle in parking facility inventory.
- **Same car:** Select if the plate numbers, state, vehicle are the same, but the vehicle has moved locations since the last inventory was taken.
- **Cancel:** Cancel the reconciliation. If the conflicts are not reconciled, a new plate read is created which says that a new vehicle arrived (as opposed to marking the same vehicle down for an additional day), and it is considered a **Different car**.

A message appears warning you that the operation was cancelled. Click **OK**.

The inventory you cancelled appears in red under *Existing inventories*, but the offload data remains in the Offload folder until it is added or removed from the parking facility.

- 9 If there are any cancelled inventories, you must delete them before you can create another inventory as follows:
 - a) In the *Existing inventories* panel, select the cancelled inventory (in red).
 - b) Under the *Existing inventories* panel, click **Delete** (X).

Related Topics

[How AutoVu MLPI works](#) on page 338

[Removing license plate reads from offload files](#) on page 339

[Overview of the Inventory management task](#) on page 475

Viewing and comparing parking facility inventories

You can view an inventory or compare two inventories from a specific *parking facility*, using the *Inventory report* task.

What you should know

In the *Inventory report*, you can view and compare vehicle inventories from different time periods to determine the following:

- Current and previous inventories of parked cars
- Vehicles that have been added (entered) or removed (exited)
- Vehicle location (sector and row)
- Vehicles that have been manually removed (towed)
- Vehicle stay duration
- Vehicles whose data was edited and manually reconciled into the inventory.

To prevent performance issues, plate images are not displayed for reports that include more than a thousand rows.

BEST PRACTICE: For best results, compare the more recent inventory with the previous inventory. For example, if the parking facility is swept on a daily basis, you should compare the inventory from today and yesterday.

To view or compare parking facility inventories:

- 1 From the home page, open the Inventory report task.
- 2 From the **Parking facility** drop-down list in the **Source** section, select the name of the parking facility.
- 3 In the **Inventory** section, select the inventory you want to view or compare.
 - **Latest non-partial:** The latest inventory.
 - **Specific:** A specific inventory.
- 4 To compare the inventory with another inventory in the parking facility, select a second inventory from **Other inventory** drop-down list.
- 5 From the Added drop-down list, select the vehicle state you want to compare.

You can query vehicles that were *Unchanged*, *Added*, *Removed*, or *Moved*. You can select multiple actions at the same time.
- 6 Set up other query filters to refine your search. Choose from one or more of the following filters:
 - **Advanced search:** By default, LPR images are not displayed in the Inventory report. To view images, click **Get images**. To prevent performance issues, plate images are not displayed if a report includes more than a thousand rows.
 - **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 has been made visible to you when it was created or last configured.
 - **License plate:** Enter a *Full* or *Partial* license plate number.
 - **Location:** Specify the location in the parking facility you want to view. You can select the entire facility, or specify the sectors and rows within the facility.

- 7 To include LPR images in the report, select the **Get images** option from the **Advanced search** section.
- 8 Click **Generate report**.

The results are listed in the report pane. The following statistics of the changes between the two inventories are shown:

- **Vehicles added:** Total number of vehicles added to the parking facility.
- **Vehicles removed:** Total number of vehicles removed from the parking facility.
- **Vehicles moved:** Total number of vehicles that moved in the parking facility.
- **Vehicles manually removed:** Total number of vehicles manually removed from the parking facility.
- **Number of manual entries:** Total number of unreconciled reads removed from the offload file.

Report pane columns for the Inventory report 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.

- **Action:** The change in the vehicle state: added, removed, moved, or unchanged.
- **Arrival:** The first time the vehicle was read. This is used to calculate the elapsed time if a vehicle is read a second time, for example the next day.
- **Context image:** Wide angle color image of the vehicle captured by the context camera.
- **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 have been made visible to you when they were created or last configured.
- **Edited:** Vehicle license plate and state were edited by a user in Security Desk.
- **Elapsed time:** The difference between the Arrival time and the Event timestamp.
- **Event timestamp:** Date and time that the event occurred.
- **Manual capture:** Displays the plate number entered manually by the Patroller user.
- **Manually removed:** Vehicle was removed manually (towed) from the parking facility.
- **Parking:** Parking facility name.
- **Patroller:** The Patroller entity that read the plate. If a handheld device was used, *XML import* is shown instead.
- **Plate image:** License plate image captured by the LPR camera.
- **Plate origin:** State that issued the license plate.
- **Plate read:** The license plate read generated by the Sharp unit.
- **Row:** Row name.
- **Sector:** Sector name.

Part V

Alarms and critical events

This part includes the following chapters:

- Chapter 25, "[Alarms](#)" on page 347
- Chapter 26, "[Incidents and threat levels](#)" on page 365
- Chapter 27, "[Zones and intrusion detection](#)" on page 376

Alarms

This section includes the following topics:

- ["How alarms are displayed in the Security Desk canvas"](#) on page 348
- ["Enabling alarm monitoring in the Monitoring task"](#) on page 350
- ["Acknowledging alarms"](#) on page 351
- ["Filtering and grouping alarms in Security Center"](#) on page 354
- ["Muting repeated alarm sounds"](#) on page 356
- ["Forwarding alarms to other users automatically"](#) on page 357
- ["Forwarding alarms to other users manually"](#) on page 358
- ["Investigating current and past alarms"](#) on page 359
- ["Triggering alarms manually"](#) on page 362
- ["Customizing alarm behavior"](#) on page 363
- ["Customizing picture-in-picture windows for alarms"](#) on page 364

How alarms are displayed in the Security Desk canvas

You can view active and past alarms in the canvas in the *Alarm monitoring* task, the *Alarm report* task, and the *Monitoring* task.

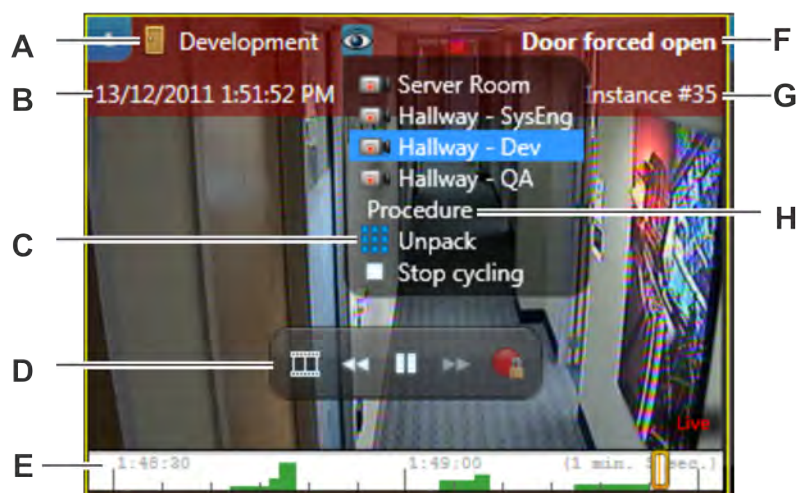
In the *Alarm monitoring* task and *Monitoring* task, active alarms are automatically displayed in the canvas so you can review the alarm details and the associated video. In the *Alarm report* task, all videos associated to the alarm are displayed in playback mode. The playback starts at the time the alarm was triggered.

NOTE: The examples in this topic are based on the *Alarm monitoring* task, but also apply when viewing alarms in the *Monitoring* task. For more information about how to enable alarms in the *Monitoring* task, see [Enabling alarm monitoring in the Monitoring task](#) on page 350.

Alarms are often *composite entities* because they are attached to multiple cameras, doors, or areas, and might include still frames. To view all the attached entities at once, you must unpack the tile where the alarm is displayed.

NOTE: If the triggered alarm is attached to an entity (for example a door) that is linked to cameras, then the linked cameras are displayed first in the canvas, before the attached entity itself.

The following figure shows an active alarm in a canvas tile in the Alarm monitoring task.



A	Source of the alarm
B	Alarm timestamp
C	Allows you to view all attached entities at once
D	On-tile video controls
E	Timeline
F	Alarm name
G	Alarm instance number
H	Displays the alarm procedure if it is defined

Related Topics

[On-tile video controls](#) on page 129

[Unpacking content in tiles](#) on page 24

Enabling alarm monitoring in the Monitoring task

To avoid switching between tasks when an alarm occurs, you can enable **Alarm monitoring** in the *Monitoring* task.

Before you begin

Create your alarms. For more information, see the *Security Center Administrator Guide*.

What you should know

Once tiles are armed to monitor alarms in the *Monitoring* task, alarms will no longer appear as pop-ups in the notification tray. You can [configure alarms as pop-ups](#).

To enable alarm monitoring in the Monitoring task:

- 1 Open the *Monitoring* task.
- 2 At the bottom of the *Monitoring* task, click **Monitoring** (🔔).
- 3 Switch the **Alarm monitoring** option to **ON**.


You can arm or disarm all the tiles from monitoring alarms by clicking (🔔). When a tile is armed to monitor alarms, the tile ID background is red.

- 4 Select whether you want to monitor **All** alarms or **Specific** alarms.

The **Events** and **Alarms** toggle button will appear in the top right corner of the **Monitoring** task so you can easily switch between monitoring events and alarms.

You can pause tile monitoring at any time by clicking **Suspend tile monitoring**.

- 5 If you selected **Specific**:

a) Click  and select the alarms you want to monitor.

TIP: To select multiple alarms, hold **CTRL** or **SHIFT** when selecting the alarms.

b) Click **Add**.

The Events and Alarms toggle button appears in the top right corner of the *Monitoring* task so you can easily switch between monitoring events and alarms.

Related Topics

[Filtering and grouping alarms in Security Center](#) on page 354

Acknowledging alarms







You can view and acknowledge the alarms from the *Alarm monitoring* task, and the *Monitoring* task.

What you should know

- If you want to view and acknowledge alarms in the *Monitoring* task, the **Alarm monitoring** option must be enabled for the *Monitoring* task. For more information, see [Enabling alarm monitoring in the Monitoring task](#) on page 350.
- You only receive an alarm in Security Desk if you are a recipient of that alarm. Alarms are displayed in the canvas by order of their priority.

NOTE: You might not have to acknowledge all the alarms that are triggered. Certain alarms are configured to be automatically acknowledged after a set amount of time.

To acknowledge an alarm:

- 1 In the notification tray, double-click the **Alarms**  icon in the notification tray.
All new alarms are automatically listed the alarm list and the associated video is displayed in the *canvas*.
- 2 To filter the alarm list, click the filter icon () and select one or more of the following filters:
 - **Show all:** Display all alarms (no filter).
 - **Show active:** Show active alarms.
 - **Show under investigation:** Show alarms that are currently under investigation.
 - **Show acknowledgement required:** Show alarms where their source conditions are cleared but they must still be acknowledged.
 - **Show acknowledged:** Show acknowledged alarms.
- 3 Double-click or drag an alarm from the alarm list to view the alarm video in a tile. The video is displayed with a red overlay that provides the alarm details.
- 4 Click one of the following:
 - **Acknowledge (Default)** (): Acknowledge the alarm. The alarm is no longer active, and is removed from the canvas and the alarm list.
NOTE: Certain alarms require you to report an incident when you acknowledge them.
 - **Acknowledge (Alternate)** (): Set the alarm to the *alternate* acknowledged state. The reasons for using this acknowledgement type are defined by your company. For example, if a false alarm is triggered, you can acknowledge the alarm this way. This state can be used as a filter in alarm queries.
 - **Forcibly acknowledge** (): Force the alarm to be acknowledged. This is helpful for clearing alarms that are currently under investigation and their acknowledgement condition is not yet cleared. You can only force acknowledge an alarm if you are logged on as an administrator.
 - **Forcibly acknowledge all alarms** (): Force all the active alarms to be acknowledged. This is helpful for clearing alarms that are currently under investigation and their acknowledgement condition is not yet cleared. You can only force acknowledge alarms if you are logged on as an administrator.

- **Snooze alarm** (🕒): Put the alarm to sleep for 30 seconds. When the alarm is snoozing, it is temporarily removed from the canvas. You can change the default snooze time from the Options dialog box.
- **Investigate** (🔍): Investigate the alarm. This button is only available if an alarm is triggered that has an acknowledgement condition attached to it, and the condition is not yet cleared. This lets other users in the system know that you have seen the alarm.
- **Show alarm procedure** (📄): Show the alarm's specific procedure (if one is defined by the administrator). Alarm procedures are simple to create and can take the form of HTML pages or a web application developed by the end user.
- **Forward alarm** (➡): Forward the alarm to another user in the system. Before forwarding the alarm, you must select a user, and you can also type a message.

Related Topics

[How alarms are displayed in the Security Desk canvas](#) on page 348

[Overview of the Alarm monitoring task](#) on page 484

Alarm information available when monitoring alarms

When an alarm is triggered, you can view the following information in the *Alarm monitoring* and *Monitoring* 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 have been made visible to you when they were created or last configured.
- **Alarm:** Alarm entity name.
- **ID:** Alarm instance number. Uniquely identifies each alarm instance.
- **Occurrence period:** Period when the event occurred.
- **Priority:** Alarm priority. All alarms imported from Omnicast have their priority set to 1 by default. You can change their priority at a later time in the Config Tool.
- **Source:** The source entity that triggered the alarm, when the alarm is triggered by an event-to-action. It shows a username when the alarm is triggered manually.
- **Source time:** Time of the alarm triggering event. The only time *Source time* and *Triggering time* are different is when the event occurred while the access control unit was offline.
- **State:**
Current state of the alarm.
 - **Active:** Alarm is not yet acknowledged. Selecting an active alarm shows the alarm acknowledge buttons in the report pane.
 - **Acknowledged (Default):** Alarm was acknowledged using the default mode.
 - **Acknowledged (Alternate):** Alarm was acknowledged using the alternate mode.
 - **Acknowledged (Forcibly):** Alarm was forced to be acknowledged by an administrator.
 - **Under investigation:** Alarm with an acknowledgement condition that is still active was put under investigation..
 - **Acknowledgement required:** Alarm with an acknowledgement condition that was cleared is ready to be acknowledged.

- **Triggering event:** Event that triggered the alarm (if triggered through an event-to-action). *Manual action* is indicated when the alarm was manually triggered by a user.
- **Trigger time:** Time the alarm was triggered in Security Center.
- **Priority:** Alarm priority. All alarms imported from Omnicast have their priority set to 1 by default. You can change their priority at a later time in the Config Tool.

Filtering and grouping alarms in Security Center

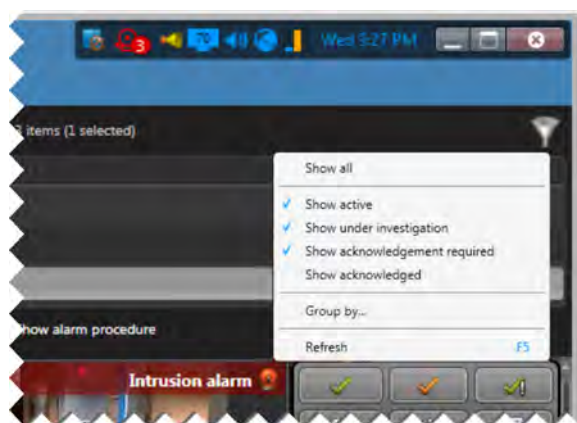
You can filter and group alarms to control how they appear in the *Alarm monitoring* task and the *Monitoring* task.

To filter alarms:

- 1 In the *Alarm monitoring* task or the *Monitoring* task, click the filter icon (🔍).

NOTE:

- In the *Monitoring* task, you must select **Alarms** from the **Events/Alarms** toggle button. The **Events/Alarms** toggle button only appears when you enable Alarm monitoring in the *Monitoring* task.
- If you cannot see the **Filter** (🔍) or **Events/Alarms** button, drag the top of the canvas down to expose the alarm list that appears at the top of the screen.



- 2 Select or clear the following filters:

- Show all
- Show active
- Show under investigation
- Show acknowledgment required
- Show acknowledged

To group alarms:

- 1 In the *Alarm monitoring* task or the *Monitoring* task, click the filter icon (🔍) and select **Group by...**

NOTE:

- In the *Monitoring* task, you must select **Alarms** from the **Events/Alarms** toggle button. The **Events/Alarms** toggle button only appears when you enable Alarm monitoring in the *Monitoring* task.
- If you cannot see the **Filter** (🔍) or **Events/Alarms** button, drag the top of the canvas down to expose the alarm list that appears at the top of the screen.

- 2 In the **Group by** dialog box, select **Enable grouping**.
- 3 From the drop-down list, select the highest level of grouping you would like to apply to the alarms.

You can group the items by:

- Alarm
- Source
- State
- Priority

4 To apply additional grouping levels, select **Then by:**.

5 Click **Apply**.

Related Topics

[Enabling alarm monitoring in the Monitoring task](#) on page 350

Muting repeated alarm sounds

If many *active alarms* on your system is causing sound bites to be repeatedly played, you can silence the alarm sounds by muting them from the notification tray.

What you should know

To avoid unintentionally ignoring alarms, you can configure your Security Desk to play a sound bite repeatedly as long as there are active alarms in the system. The sound will stop when all alarms are acknowledged, or when you decide to mute them temporarily.

To mute all sounding alarms:

- In the notification tray, right-click the **Alarms** icon () , and click **Mute all alarms**.

All sounding alarms are muted. The sounding will restart the moment a new alarm is received, and will continue as long as there are active alarms in the system.

Related Topics

[Customizing alarm behavior](#) on page 363

Forwarding alarms to other users automatically




If you must leave your desk and you want someone else to receive alarms while you are gone, you can set alarms to *auto-forward*.

Before you begin

Make sure that you have the *Forward alarms* user privilege.

To forward an alarm automatically:

1 Do one of the following:

- In the notification tray, right-click the **Alarms** icon ( or ) , and click **Start alarms auto-forward**.
- In the upper-left corner of the **Alarm monitoring** or **Monitoring** task, click **Start alarms auto-forward** (.




2 In the *Select alarm recipients* dialog box, select the destination user or user group.

3 (Optional) Write a message to send with the forwarded alarm.

4 Click **Start alarms auto-forward**.

All alarms sent to you are forwarded to the specified user until you cancel the *auto-forward* option.

5 To cancel *auto-forward*, do one of the following:

- In the notification tray, right-click the **Alarms** icon ( or ) , and click **Stop alarms auto-forward**.
- In the upper-left corner of the **Alarm monitoring** or **Monitoring** task, click **Stop alarms auto-forward** (.

Forwarding alarms to other users manually

If you receive an important alarm and you want someone else to see it, you can manually forward the alarm to them from the *Alarm monitoring*, *Monitoring*, and *Alarm report* tasks.

Before you begin

Make sure that you have the *Forward alarms* user privilege.

What you should know

Forwarding an alarm does not remove it from your workspace. The alarm is forwarded to the user you selected, and one of you must acknowledge the alarm.

To forward an alarm manually:

- 1 Under the alarm list, or in the alarm widget, click **Forward alarm** (↔).
- 2 In the *Select alarm recipients* dialog box, select the destination user or user group.
- 3 (Optional) Write a message to send with the forwarded alarm.
- 4 Click **Forward alarm**.

Investigating current and past alarms

You can search for and investigate current and past alarms, using the *Alarm report* task.

What you should know

For example, you might want to see which alarms were triggered during the last week, or since your last shift. You could search for major events that happened in your system, by only selecting critical alarms. You can see who acknowledged a specific alarm, and why. If there was a critical alarm that occurred and you must re-examine it, you can search for the alarm, and then review the attached video. If needed, you can also export the alarm video, and send it to law enforcement as evidence.

To investigate an alarm:

- 1 From the home page, open the **Alarm report** task.
- 2 Set up the query filters for your report. Choose one or more of the following filters:
 - **Acknowledged by:** Users who acknowledged the alarm.
 - **Acknowledged on:** Alarm acknowledgement time range.
 - **Acknowledgement type:**

Select one of the following acknowledgement type options:

 - **Alternate:** Alarm was acknowledged by a user using the alternate mode.
 - **Default:** Alarm was acknowledged by a user, or auto-acknowledged by the system.
 - **Forcibly:** An administrator forced the alarm to be acknowledged.
 - **Alarm priority:** Alarm priority.

NOTE: All alarms imported from Omnicast have their priority set to 1 by default. You can change their priority at a later time in the Config Tool.
 - **Alarms:** Select the types of alarms you want to investigate. Alarms can be locally defined (👤), or imported from federated systems (🌐).
 - **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 has been made visible to you when it was created or last configured.
 - **Investigated by:** Which user put the alarm into the *under investigation* state.
 - **Investigated on:** Specify a time range when the alarm was put into the *under investigation* state.
 - **Source:** Source entity that triggered the alarm in the case of an event-to-action, or the user who triggered the alarm manually.
 - **State:** Current state of the alarm.
 - **Active:** Alarm is not yet acknowledged. Selecting an active alarm shows the alarm acknowledge buttons in the report pane.
 - **Acknowledged:** Alarm was acknowledged by a user, or auto-acknowledged by the system.
 - **Under investigation:** Alarm with an acknowledgement condition that is still active was put under investigation.
 - **Acknowledgement required:** Alarm with an acknowledgement condition that was cleared is ready to be acknowledged.

- **Triggered on:** Alarm trigger time range.
 - **Triggering event:** Events used to trigger the alarm.
- 3 Click **Generate report**.
The alarms are listed in the report pane.
 - 4 To show the corresponding video of an alarm in a tile, double-click or drag the item from the report pane to the canvas.
 - 5 To control the alarms, use the alarm widget.

Related Topics

[How alarms are displayed in the Security Desk canvas](#) on page 348

[Alarm widget](#) on page 31

[Overview of the Alarm report task](#) on page 485

Report pane columns for the Alarm report 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.

NOTE: If you generated the Alarm report using Web Client, not all of the report columns are available.

- **Acknowledged by:** User who acknowledged the alarm. When the alarm is acknowledged automatically by the system, **Service** is indicated.
- **Acknowledged on:** Time the alarm was acknowledged.
- **Alarm:** Alarm 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 have been made visible to you when they were created or last configured.
- **External instance ID:** Only for federated alarms. The original alarm instance ID on the federated system.
- **ID:** Alarm instance number. Uniquely identifies each alarm instance.
- **Investigated by:** Which user put the alarm into the *under investigation* state.
- **Investigated on:** The timestamp when the alarm was put into *under investigation* state.
- **Occurrence period:** Period when the event occurred.
- **Priority:** Alarm priority. All alarms imported from Omnicast have their priority set to 1 by default. You can change their priority at a later time in the Config Tool.
- **Source:** The source entity that triggered the alarm, when the alarm is triggered by an event-to-action. It shows a username when the alarm is triggered manually.
- **Source time:** Time of the alarm triggering event. The only time *Source time* and *Triggering time* are different is when the event occurred while the access control unit was offline.
- **State:**
Current state of the alarm.
 - **Active:** Alarm is not yet acknowledged. Selecting an active alarm shows the alarm acknowledge buttons in the report pane.
 - **Acknowledged (Default):** Alarm was acknowledged using the default mode.
 - **Acknowledged (Alternate):** Alarm was acknowledged using the alternate mode.

- **Acknowledged (Forcibly):** Alarm was forced to be acknowledged by an administrator.
- **Under investigation:** Alarm with an acknowledgement condition that is still active was put under investigation..
- **Acknowledgement required:** Alarm with an acknowledgement condition that was cleared is ready to be acknowledged.
- **Triggering event:** Event that triggered the alarm (if triggered through an event-to-action). *Manual action* is indicated when the alarm was manually triggered by a user.
- **Trigger time:** Time the alarm was triggered in Security Center.


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:

- 1 From the home page, open the *Alarm monitoring* task or the *Monitoring* task.
- 2 Click **Trigger alarm** .
- 3 From the list, select an alarm, and then click **Trigger alarm**.

All pre-configured alarm recipients receive the alarm if they are logged on to Security Desk.


Customizing alarm behavior

Once you are familiar with how alarms work, you can customize how the system handles alarms from the *Options* dialog box.

What you should know

The alarm settings are saved locally for your Windows user profile.

To customize the alarm behavior:

- 1 From the home page, click **Options > Alarms**.
- 2 Set the following alarm options:
 - **Bring Security Desk in front of other windows:** Brings the Security Desk window to the foreground when a new alarm occurs.
 - **Play a sound:** Sets the sound bite to play when a new alarm occurs and how often to play it: *Once* (default), *Every n seconds*, or *Continually*. Click **Test** to hear the selected sound bite.
 - **Display in:**
 - **Popup:** Select this option to have alarms appear in a popup window in the notification tray of the *Monitoring* task.
NOTE: Popup alarms only appear when there are no armed tiles in the *Monitoring* task.
 - **Alarm monitoring task (and bring to front):** Automatically switches to the *Alarm monitoring* task when a new alarm occurs. If Alarm monitoring is not in the active task list, it is added.
 - **Map (and bring to front):** Automatically switches to display alarms in the *Maps* task. If the *Maps* task is not in the active task list, it is added.
 - **Revert to original task after alarm is handled:** Automatically returns to the task you were working on before the alarm occurred after you have acknowledged the alarm.
 - **Automatically display alarm in unpacked mode:** When the alarm is triggered, displays all the attached entities of the alarm in separate tiles instead of cycling through them.
 - **Snooze time:** Sets the duration of the snooze when an alarm is put to sleep with the  command.
- 3 Click **Save**.

Related Topics

[Acknowledging alarms](#) on page 351

[Muting repeated alarm sounds](#) on page 356

[Overview of the Alarm monitoring task](#) on page 484

[How alarms are displayed in the Security Desk canvas](#) on page 348

[Muting repeated alarm sounds](#) on page 356

Customizing picture-in-picture windows for alarms

In Security Desk, you can customize the size and position of the inset window for an alarm that is configured for picture-and-picture display. You can also switch the content displayed in the inset window.

Before you begin

Configure picture-in-picture as the video display option for your alarm. For more information, see the *Security Center Administrator Guide*.

To customize the inset window of a picture-in-picture alarm:

- 1 Open the *Monitoring* or *Alarm monitoring* task.
- 2 Select a tile that is displaying an alarm configured for picture-in-picture display.
- 3 You can do the following:
 - Click within the inset window to switch the displayed video type with the video type displayed in the full tile. For example, if you configure your alarm to display live and playback video, and live video is displayed in the inset window, clicking within the inset window switches the content to playback video.
 - Click and drag the inset window to move it to a new location.
 - Click and drag the box handles around the inset window to resize it.

Your changes are applied immediately.

Incidents and threat levels

This section includes the following topics:

- ["Reporting incidents"](#) on page 366
- ["Creating incident packages"](#) on page 368
- ["Reviewing and modifying reported incidents"](#) on page 371
- ["Responding to critical events through threat levels"](#) on page 373

Reporting incidents



When you see a situation that must be remembered, you can report it as an *incident*. Events and entities (cameras, doors, and so on) can be attached to an incident report as supporting information.

What you should know

When you report an incident about an event or an alarm, the event is attached to the reported incident, along with the entities referenced by that event or alarm. You might also be required to report an incident when you acknowledge an alarm, if the alarm is configured that way in Config Tool.

Incident reports can be searched for at a later time from the Incidents task.

To report an incident:

- 1 Do one of the following:
 - To report an incident that is not related to an entity, click the home tab, and then click **Tools > Report an incident**.
 - To report an incident about an event or alarm, right-click an item in the event list or report pane, and then click **Report an incident**.
 - To report an incident about the entity in the selected tile, right-click inside the tile, and then click **Report an incident**.
- 2 In the *Report an incident* dialog box, type a **Title** for the incident.
- 3 From the **Category** drop-down list, do one of the following:
 - Select a category for the incident.
 - If no categories exist, then click **Manage categories > Add an item**, type a name for the category, and then click **Add > Save**.
- 4 In the **Description** section, describe the incident.
The description you add is searchable in the Incidents task.
- 5 In the *References* section, click  to add other entities as supporting information.
All the entities related to what you were viewing in the tile are added by default.
- 6 To add a video sequence to the incident, click **More**, and do the following:
 - a) In the *Video sequences* section, click **Add an item** (.
 - b) Select a camera and a time range, and click **Add**.
- 7 Create the incident report one of the following ways:
 - Click **Create**.
 - To create the incident report and notify other users on the system, click **Create and email**, select the users, and click **Create and email**.

NOTE: The user must have a valid email address and the server must be configured to send emails.

The report is saved in the database for reporting purposes. If you selected a user, the incident report is sent to them.

Related Topics

[Tile menu commands](#) on page 20

[Reviewing and modifying reported incidents](#) on page 371

Creating incident packages

You can add live and playback video to a tile, and then saving the information as an incident package. This is helpful when you want to report a situation and build a case.

What you should know

When incident recording is turned on, the live or playback video related to any entity that is placed in the tile (cameras, areas, doors, cardholders, and so on) is recorded. Entity cycling inside the tile is supported.

You can export the related video sequences as a single G64x file. The G64x file can be played back in Security Desk, or in the Genetec Video Player.

You can create multiple incident package simultaneously.

When incident recording is turned on for a specific tile, cameras that are placed in the tile start recording if they are not already recording.

To create an incident package:

- 1 To make sure that the tile contents are not overwritten when new events are received in Security Desk, turn off monitoring for that tile as follows:
 - a) In the *Monitoring* task, select the tile in the canvas.
 - b) In the tile widget, click **Monitoring** (🔍).
 - c) Click **Monitor alarms** and **Monitor events** to make sure you turn off all monitoring for the tile.

TIP:

When monitoring is turned off for a tile, the tile ID background turns black.

- 2 Right-click inside the tile that is displaying the camera where the incident is happening, and then click **Start incident recording** (📹).

The tile is outlined in red.
- 3 To build your case, add other cameras, or entities that have attached cameras, to the tile.

The sequence is created in the order that you add a new cameras and entities, and can be adjusted afterwards.
- 4 Right-click inside the tile, and click **Stop incident recording** (📹).
- 5 In the *Report an incident* dialog box, type a **Title** for the incident.

- 6 From the **Category** drop-down list, do one of the following:
 - Select a category for the incident.
 - If no categories exist, then click **Manage categories > Add an item**, type a name for the category, and then click **Add > Save**.
- 7 In the **Description** section, describe the incident.
The description you add is searchable in the Incidents task.
- 8 In the *References* section, click **+** to add other entities as supporting information.
All the entities related to what you were viewing in the tile are added by default.
- 9 In the *Video sequences* section, do the following:
 - For each camera, edit the time range of the video sequence you want to include in the incident report.
For example, one of the cameras might only have two minutes of video that relates to the incident.
 - To add another camera to the package, click **Add an item (+)**, select a camera and the time range, and click **Add**.
Adding additional cameras is helpful if you forgot to place one of the cameras in the tile while it was recording the incident.
- 10 Create the incident package one of the following ways:
 - Click **Create**.
 - To create the incident report and notify other users on the system, click **Create and email**, select the users, and click **Create and email**.
NOTE: The user must have a valid email address and the server must be configured to send emails.
 - To export the video sequences from all the cameras and stitch them together as a G64x file, click **Create and export**.

The incident package is saved in the database for reporting purposes. If you selected a user, the package is sent to them by email.

After you finish

After the incident package is created, you can send it to authorities or other users, or review it a later time using the Incidents report.

Related Topics

[Reviewing and modifying reported incidents](#) on page 371

Reviewing and modifying reported incidents

You can search for, review, and modify reported *incidents* and incident packages, using the Incidents report.

What you should know

If you previously reported an incident, but must edit its content (for example, modify the description, or add another camera to the report), you can search for that report using the title you wrote while creating it. Or, if you remember what camera you wrote the incident for, you can search by specific camera. If you want to search for all the noteworthy activity that was logged by other users during the last week, or since your last shift, you can search for those incidents by setting a time range.

To modify an incident, you need the *Modify reported incidents* user privilege.

To review and modify a reported incident:

- 1 From the home page, open the Incidents task.
- 2 Set up the query filters for your report. Choose one or more of the following filters:
 - **Category:** If incident categories are created, restrict the search to specific categories.
 - **Creation time:** Incidents created/reported within the specified time range.
 - **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 has been made visible to you when it was created or last configured.
 - **Description:** Restrict the search to entries that contain this text string.
 - **Incident time:** Incidents reported within the specified time range. The incident time corresponds to the event or alarm timestamp the incident refers to. If the incident does not refer to any event or alarm, then the incident time corresponds to the creation time.
 - **Modification time:** Incidents modified within the specified time range.
 - **References:** Incidents referencing all the selected entities.
 - **Title:** Restrict the search to incidents containing specific text in their title.
- 3 Click **Generate report**.

The reported incidents and incident packages are listed in the report pane.
- 4 To review an incident and show the corresponding video in a tile, double-click or drag the item from the report pane to the canvas.

If there is no camera attached to the incident, the *Edit incident* dialog box opens. If you select an incident package, the video sequences are played back within a single tile in the order that they were recorded, and entities that were added as additional resources are displayed in different tiles.
- 5 If you are viewing video from an incident package, you can control the playback from the *Video sequences* widget in the dashboard, as follows:
 - To switch to another camera in the package, select a camera the drop-down list.
 - To jump to the next or previous cameras in the package, click **Next sequence** (▶) or **Previous sequence** (◀).
 - To jump to a specific moment in time, move your cursor to that spot on the timeline.
- 6 Modify the incident, as follows:

- a) Select an incident in the report pane.
 - b) At the bottom of the report pane, click **Edit** (✎).
 - c) In the *Edit incident* dialog box, edit the incident description.
 - d) From the **Category** drop-down list, change the incident category.
 - e) In the *References* section, click **+** or **×** to add or remove referenced entities.
 - f) If you are modifying an incident package, you can edit the following in the *Video sequences* section:
 - Edit the time ranges of the video sequences included in the incident report.
 - To add another camera to the package, click **Add an item** (**+**), select a camera and the time range, and click **Add**.
- 7 To save the report, do one of the following:
- To save the incident report, click **Save**.
 - To save the incident and notify other users on the system, click **Save and email**, select the users, and click **Save and email**.
- NOTE:** The user must have a valid email address and the server must be configured to send emails.

The updates you made to the incident report are saved in the database. If you selected a user, the incident report is sent to them by email.

Related Topics

[Reporting incidents](#) on page 366

[Creating incident packages](#) on page 368

Report pane columns for the Incidents 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.

- **Category:** Category of the incident.
- **Created by:** User who originally reported the incident.
- **Creation time:** Time the incident was reported.
- **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 have been made visible to you when they were created or last configured.
- **Description:** Description of the event, activity, entity, or incident.
- **Event:** Event name.
- **Incident time:** The timestamp of the referenced alarm or event. If no event is referenced, it corresponds to the incident creation time.
- **Modification time:** Time the incident was last modified.
- **Modified by:** User who last modified the incident.
- **References:** List of entities referenced by the incident.
- **Source (entity):** Source entity associated to the alarm or event. This column is empty if the incident is not based on an alarm or event.
- **Title:** Title of the incident.

Responding to critical events through threat levels

If a dangerous situation arises while you are monitoring your system (for example, a fire or shooting), you can respond by changing the state of the entire Security Center system or specific areas, using threat levels.

Before you begin

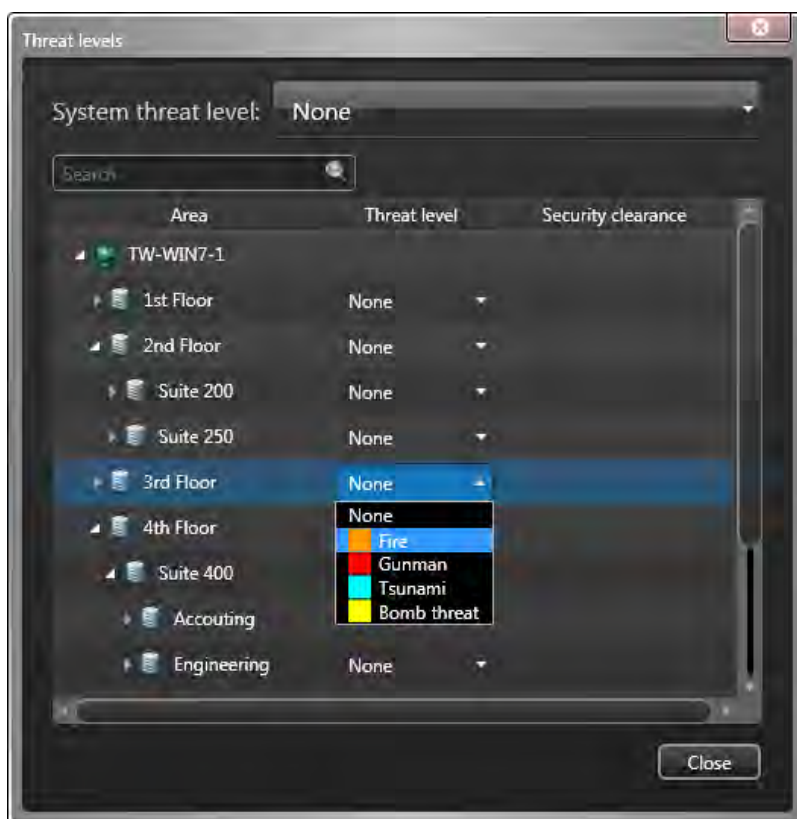
To set threat levels, you need the *Set threat level* user privilege. If the Threat levels icon (🔒) is not displayed in the notification tray, you can show it from the Options dialog box.

What you should know

When you set a threat level, you could force a complete lock down, temporarily override lock schedules, trigger an alarm, deny certain cardholders access to areas, and so on. The exact effects of setting a threat level depend on how it is configured in Config Tool. For information about configuring threat levels, see the *Security Center Administrator Guide*.

To set a threat level:

- 1 Open the **Threat levels** dialog box one of the following ways:
 - In the notification tray, double-click the **Threat levels** (🔒) icon.
 - From the home page, click **Tools > Threat levels**.
- 2 Do one of the following:
 - To set a threat level on the entire system, select a threat level from the **System threat level** drop-down list.
 - To set a threat level on a specific area, select a threat level from the drop-down list next to the desired entity.



- 3 In the confirmation dialog box that opens, click **Apply**.
- 4 Click **Close**.

The **Threat levels** icon in the notification tray turns red (🔴). If you set a threat level on the entire system, the background of Security Desk turns the color of the threat level. Additional effects of setting the threat level depend on how the threat level was configured.

TIP: You can view the current threat level status of areas in the *System status* task.

Example

If a fire broke out and you set the *Fire* threat level, the fire alarm could be triggered, all doors could be unlocked, cameras could start recording, and so on.

Related Topics

[Configuring the notification tray](#) on page 73

Clearing threat levels

Once the critical event is no longer active, you can clear the threat level and return Security Center to its normal state.

To clear a threat level:

- 1 From the notification tray, double-click the **Threat levels** (🔴) icon.
- 2 To reset the security clearance level to **None** (level 7) for all areas while the threat is still set, click **Reset minimum security clearance**.

- 3 To clear the threat level, do one of the following:
 - If a threat level was set on the entire system, from the **System threat level** drop-down list, select **None**.
NOTE: You can also clear the threat level on specific areas. This also clears the threat level on all sub-areas.
 - If a threat level was set on a specific area, from the drop-down list next to the entity, select **None**.
- 4 Click **Close**.

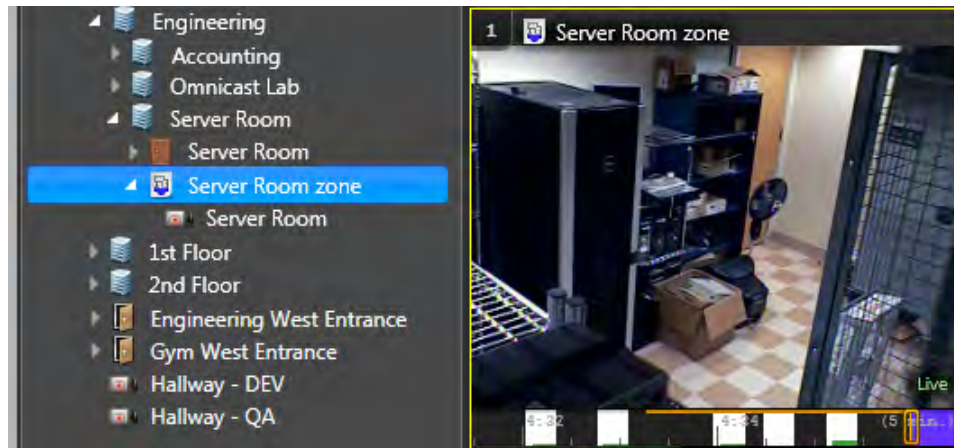
Zones and intrusion detection

This section includes the following topics:

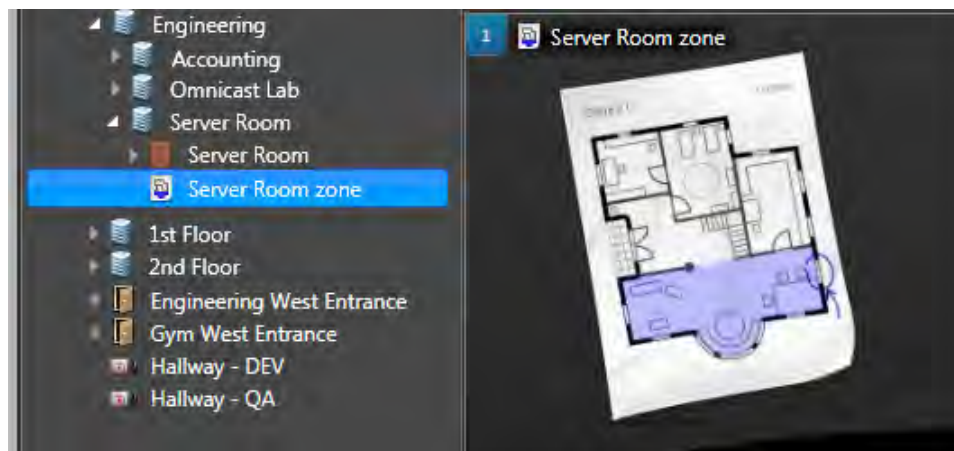
- ["How zones are displayed in the Security Desk canvas"](#) on page 377
- ["Arming and disarming zones"](#) on page 378
- ["Investigating zone events"](#) on page 379
- ["Changing intrusion detection area statuses"](#) on page 380
- ["Investigating intrusion detection area events"](#) on page 381
- ["Investigating intrusion detection unit events"](#) on page 383

How zones are displayed in the Security Desk canvas

When you double-click or drag a zone entity (📷) into a tile and there is a camera linked to the zone, the camera video stream is displayed.



If a zone is not linked to any cameras, the zone icon is displayed.



Arming and disarming zones

You can arm and disarm a zone from the *System status* task.

What you should know

You can also arm and disarm zones using the *Zone* widget in the dashboard when a zone is displayed in a tile.

To arm or disarm a zone:

- 1 From the home page, open the **System status** task.
- 2 From the **Monitor** drop-down list, select **Zones**.
- 3 In the *Selector*, select an area.
- 4 To search for zones within sub-areas, select the **Search member entities** option.

The zones are listed in the report pane.

- 5 Select a zone, and do one of the following:
 - To arm the zone, click **Arm** (🔔).
 - To disarm the zone, click **Disarm** (🔕).

Related Topics

[Zone widget](#) on page 43

Investigating zone events

You can investigate events related to *zones* (zone armed, zone disarmed, lock released, and so on), using the *Zone activities* report.

What you should know

For example, if you want to see all the activities that happened in a particular zone during a certain time period, you can select a zone, and a time range for the report. You can search for critical events only, by selecting the zone related events you are interested in (for example, door forced open).

To investigate zone events:

- 1 From the home page, open the **Zone activities** 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 has been 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.
 - **Zones:** Select the zones to investigate.
- 3 Click **Generate report**.

The zone events are listed in the report pane.
- 4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If there is no camera attached to the zone, the zone icon is displayed.
- 5 To control the zones, use the zone widget.

Related Topics

[Zone widget](#) on page 43

Report pane columns for the Zone activities 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 have been 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.
- **Zone:** Zone name.




Changing intrusion detection area statuses

You can arm and disarm an intrusion detection area, and trigger an intrusion alarm, from the *System status* task.

What you should know

You can also arm, disarm, and trigger an intrusion alarm using the *Intrusion detection area* widget in the dashboard when an intrusion detection area is displayed in a tile. For more information about the effects of arming or disarming an intrusion detection area, or triggering an intrusion alarm, see [Intrusion detection area widget](#) on page 38.

To change the status of an intrusion detection area:

- 1 From the home page, open the **System status** task.
- 2 From the **Monitor** drop-down list, select **Intrusion detection area**.
- 3 In the *Selector*, select an intrusion detection area.
- 4 To search for intrusion detection areas within sub-areas, select the **Search member entities** option.
The intrusion detection areas are listed in the report pane.
- 5 Select an intrusion detection area, and do one of the following:
 - To arm the area, click .
 - To disarm the area, click .
 - To trigger an intrusion alarm, click .

Investigating intrusion detection area events

You can investigate events that occur in *intrusion detection areas* (Intrusion detection area master armed, Intrusion detection area duress, Intrusion detection area input trouble, and so on), using the *Intrusion detection area activities* report.

What you should know

For example, if you are aware of a critical intrusion detection event (for example, *Intrusion detection area duress*) that occurred in the last 5 minutes, you can search for that event, review the video associated with the event, and trigger an intrusion alarm if needed.

To investigate intrusion detection area events:

- 1 From the home page, open the **Intrusion detection area activities** 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 has been 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.
 - **Intrusion detection areas:** Select the intrusion detection areas to investigate.
- 3 Click **Generate report**.

The intrusion detection area events are listed in the report pane.
- 4 To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas.

If there is no camera attached to the intrusion detection area, the intrusion detection area icon is displayed.
- 5 To control the selected tile, use the intrusion detection area widget.

Related Topics

[Intrusion detection area widget](#) on page 38

Report pane columns for the Intrusion detection area activities 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 have been 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.).

NOTE: This column is empty if the event is an *input bypass*.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.

- **Intrusion detection area:** Intrusion detection area name.
- **Intrusion detection unit:** Intrusion detection unit involved.
- **Occurrence period:** Period when the event occurred.
- **User:** Name of the user who triggered the event. The user name is empty if the event was not triggered from Security Desk.

Investigating intrusion detection unit events

You can investigate events related to *intrusion detection units* (AC fail, Unit lost, Intrusion detection unit input trouble, and so on), using the *Intrusion detection unit events* task.

To investigate intrusion detection unit events:

- 1 From the home page, open the **Intrusion detection unit events** 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 has been 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.
 - **Intrusion detection units:** Select the intrusion detection units to investigate.
- 3 Click **Generate report**.

The intrusion detection unit events are listed in the report pane.

Report pane columns for the Intrusion detection 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 have been 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.).
NOTE: This column is empty if the event is an *input bypass*.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **Intrusion detection unit:** Intrusion detection unit involved.
- **Occurrence period:** Period when the event occurred.
- **User:** Name of the user who triggered the event. The user name is empty if the event was not triggered from Security Desk.

Part VI

Troubleshooting

This part includes the following chapters:

- Chapter 28, "[General troubleshooting](#)" on page 385
- Chapter 29, "[Troubleshooting video](#)" on page 400
- Chapter 30, "[Troubleshooting access control](#)" on page 419

General troubleshooting

This section includes the following topics:




- ["Viewing system messages"](#) on page 386
- ["Viewing system health events"](#) on page 388
- ["Viewing the health status and availability of entities"](#) on page 390
- ["Monitoring the status of your system"](#) on page 392
- ["Entity states"](#) on page 394
- ["Troubleshooting: entities"](#) on page 395
- ["Deactivating and activating roles"](#) on page 396
- ["Troubleshooting: query filters"](#) on page 397
- ["Collecting diagnostic data"](#) on page 398

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

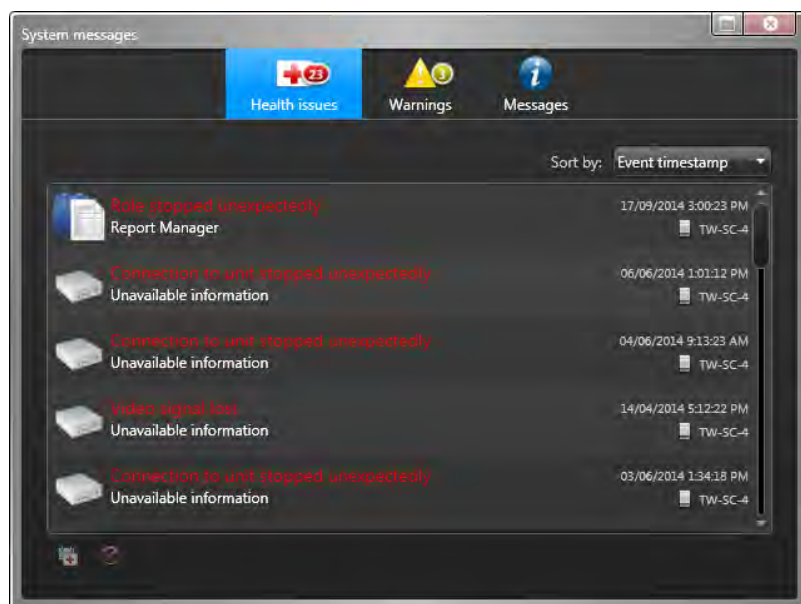
You can receive three types of messages from the system:


-  Health issues
-  Warnings
-  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**  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. You must have access to Config Tool.
 - 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.



- 3 In the *Warnings*  tab, do one of the following:
 - Click an entity to open its configuration pages. You can only jump to the entity's configuration pages if you have access to Config Tool.

- Click **Details** () 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* () 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 388

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 information about selecting which health events to monitor in Config Tool, see the *Security Center Administrator Guide*.





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 your search only for errors, and set a time range.

NOTE: Health events also appear in the notification tray as system messages () 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 has been 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

[Viewing system messages](#) on page 386

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 have been 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:
 -  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 has been 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. For information about selecting which health events to monitor in Config Tool, see the *Security Center Administrator Guide*.
- **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 have been 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 the status of your 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

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
 - 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

[Viewing system health events](#) on page 388

[Troubleshooting: entities](#) on page 395

[Overview of the System status task](#) on page 479

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. For information about schedule conflicts, see the *Security Center Administrator Guide*.
- Troubleshoot the Archiver role.

Related Topics

[Viewing entities in the canvas](#) on page 22

[Searching for entities](#) on page 69

[Troubleshooting: entities](#) on page 395

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 394

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. For more information about configuring roles in Config Tool, see the *Security Center Administrator Guide*.

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** ().

Troubleshooting: query filters

When you are generating a report or searching for entities, you must use filters to specify your search criteria. When a filter is activated, it is indicated with the On (🟢) LED icon. However, if a filter is invalid, an error or warning message is displayed.

- **Warning (🟡):** There is a potential problem with the information in the filter. The report or search might take longer than usual to generate.
- **Error (🔴):** There is a problem with the information in the filter. You cannot generate the report or search when there is an error.

Hover your mouse over the icon to see the warning or error message in a tooltip. The following table lists some examples of messages you can receive, and what you do to fix the issue.

Warning/error message	Try this
The search covers multiple days	Decrease the time range for your report or search.
There are no selected entities	Your filter is empty. Select an entity, or turn off the filter.
There is no selection	Your filter is empty. Select an option, or turn off the filter.
The dates and times are invalid	The time range is invalid. You might have set the start date and time after the end date and time, or the end date and time before the start date and time. Reconfigure your time range for the report.

Related Topics

[Generating reports](#) on page 55

[Searching for entities](#) on page 69

[Selecting date and time ranges for reports](#) on page 55

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 Support.

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 Genetec 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 Support.

Troubleshooting video

This section explains some of the reasons why you might not be able to view video in Security Desk, and what you can do to fix those issues. It also explains how to respond when you receive certain error messages when trying to view video, and what to do if you cannot add or remove video units from Security Center. To perform these procedures, you need access to both Config Tool and Security Desk. If you are not an administrator, you might not be able to perform every troubleshooting step.

This section includes the following topics:

- ["Troubleshooting: Video units are offline"](#) on page 401
- ["Troubleshooting: Cannot view live video"](#) on page 402
- ["Troubleshooting: Video stream issues"](#) on page 405
- ["Troubleshooting: Determining whether the workstation or the network cause video degradation"](#) on page 406
- ["Troubleshooting: "Impossible to establish video session with the server" errors"](#) on page 408
- ["Troubleshooting: No playback video available"](#) on page 409
- ["Troubleshooting: Cameras are not recording"](#) on page 410
- ["Troubleshooting: Video units cannot be added"](#) on page 413
- ["Troubleshooting: Video units cannot be deleted"](#) on page 416
- ["Troubleshooting: H.264 video stream issues"](#) on page 417
- ["Troubleshooting: Hardware acceleration issues"](#) on page 418

Troubleshooting: Video units are offline

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: Cannot view live video

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



- **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 Support.
 - 10 Make sure the correct ports are open on your network so there is no firewall blocking the video stream.
For a list of default ports that are used in Security Center, see the *Security Center Administrator Guide*.
 - 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**.

For more information about configuring network settings, see the *Security Center Administrator Guide*.
 - 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 Support.

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: Determining whether the workstation or the network cause video degradation

If the video you are monitoring is jittery or is dropping frames, use the rendering rate video statistic to determine whether the workstation is the cause. Rendering rate is the comparison of how fast the workstation renders a video with the speed the workstation receives that video from the network.

What you should know

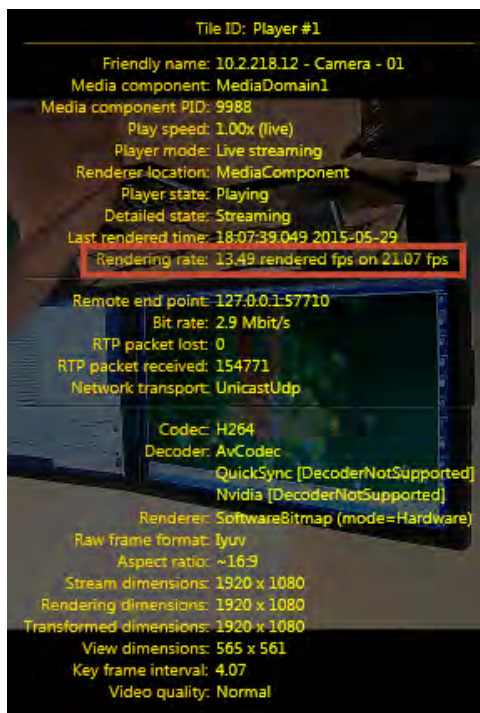
The rendering rate video statistic is made up of:

- The speed the workstation processes the video, which indicates how much load is on the workstation's CPU and memory.
- The speed the network is sending the video to the workstation.

To view the rendering rate of a video:

- 1 Select the tile that is playing video.
- 2 Press Ctrl+SHIFT+A.

Video stream statistics are displayed in the tile.



Example

If your rendering rate is "13.49 rendered fps on 21.07 fps", your workstation is processing 13.49 fps. However, it is receiving videos at 21.07 fps. The workstation cannot process all the frames it is receiving. Your workstation is the cause for the degraded quality of the video you are monitoring. In this case, lighten the load, and check the hardware and its drivers.

- Reduce the number of cameras you are monitoring to reduce the load on the workstation.

- Check the hardware requirements to make sure the workstation can handle the load.
- Check that the graphic card is up to date.
- Check that the network card is up to date.
- Ensure all drivers are up to date.

If your rendering rate is "13.49 rendered fps on 13.49 fps", your workstation is processing every frame that it is receiving from the network. In this case, compare the second value to the camera's configured fps rate to determine whether the network is not sending all the frames it is receiving from the camera. If there is a difference in these two rates, either the camera or the network is the cause of the video degradation.

- Check the camera's firmware.
- Check the health of the network.

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](#).

Troubleshooting: No playback video available

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 [Troubleshooting: Video units are offline](#) on page 401.
- 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.

For a list of default ports that are used in Security Center, see the *Security Center Administrator Guide*.
- 6 If you still cannot view playback video, contact Genetec Technical Support.

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.
For more information about motion detection settings, see the *Security Center Administrator Guide*.
- 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:
- 1 Open your Windows Control Panel.
 - 2 Click **Administrative Tools > Services**.
 - 3 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.

For more information about adding units in Security Center, see the *Security Center Administrator Guide*.
- 10 If you still cannot record video on the camera, contact Genetec Technical Support.

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**.

For more information about configuring network settings, see the *Security Center Administrator Guide*.

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 Support.

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

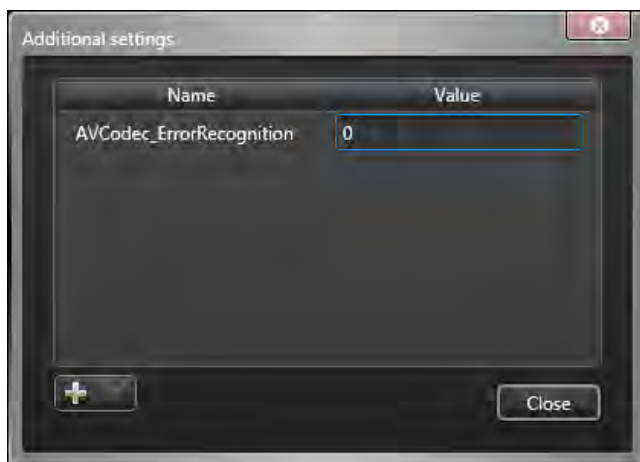
If you are having problems viewing H.264 video streams, you can disable the *AVCodec_ErrorRecognition* advanced Archiver role setting.

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 (+)**.



- 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: 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.

Troubleshooting access control

This section includes the following topics:

- ["Viewing access control health events"](#) on page 420
- [" Access troubleshooter tool"](#) on page 421
- ["Testing access rules at doors and elevators"](#) on page 422
- ["Testing cardholder access rights"](#) on page 423
- ["Troubleshooting: Driver fails to install for HID OMNIKEY USB readers"](#) on page 424

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 have been 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.

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 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 423

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 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 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.

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.

Appendices

Security Desk reference

This section includes the following topics:

- ["Events and actions"](#) on page 426
- ["Graphical overview of Security Desk tasks"](#) on page 452



Events and actions

This section includes the following topics:

- ["Event types"](#) on page 427
- ["Action types"](#) on page 443

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 <i>Access granted</i> 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.

Event	Source entity	Description
Alarm acknowledged (alternate)	alarm	An alarm has been acknowledged by a user using the alternate mode.
Alarm being investigated	alarm	An alarm with a acknowledgment condition that is still active has been put into the <i>under investigation</i> 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 <i>Security Center Release Notes</i> .
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 <i>Security Center Release Notes</i> 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.

Event	Source entity	Description
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.
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 <i>Disk full</i> 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.

Event	Source entity	Description
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.
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 <i>n</i> days of expiring. The credential expiry notification threshold is configured in the <i>General settings</i> 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 <i>Send an email</i> 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 <i>Properties</i> 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 <i>Expired</i>).
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 <i>alarm</i> state.
Input alarm restored	input on intrusion detection unit	The input has left an <i>alarm</i> state.
Input bypass restored	input on intrusion detection unit	The input has left a <i>bypassed</i> state.
Input bypassed	input on intrusion detection unit	The input has entered a <i>bypassed</i> state.
Input state changed: Input active	input on camera, access control unit, or intrusion detection unit	The input has entered an <i>active</i> state.
Input state changed: Input normal	input on camera, access control unit, or intrusion detection unit	The input has entered a <i>normal</i> state.
Input state changed: Input trouble	input on access control unit or intrusion detection unit	The input has entered a <i>trouble</i> 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.

Event	Source entity	Description
Intrusion detection unit input trouble	intrusion detection unit	Intrusion detection unit input trouble.
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 its normal operating position.
Macro 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 <i>Motion on</i> event when motion (measured in terms of number of motion blocks) has dropped below the “motion off threshold” for at least 5 seconds.

Event	Source entity	Description
Motion on	camera	This event is issued when positive motion detection has been made.
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.

Event	Source entity	Description
Offload failed	Patroller	An offload from Patroller to Security Center has failed.
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 <i>Protected video threshold</i> 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 <i>Description</i> 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 <i>Description</i> 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 <i>Description</i> field indicates the user who last used the PTZ.

Event	Source entity	Description
PTZ zoom by user	camera (PTZ)	A user started zooming the PTZ. The Description field indicates the user who performed the zoom. Subsequent <i>PTZ zoom by user</i> events are generated if another user zooms the PTZ, or if the original user zooms the PTZ after the <i>Idle delay</i> 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 <i>Description</i> field indicates the user who last zoomed the PTZ.
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 <i>Description</i> field, and the two sources are labeled <i>Archived</i> and <i>Rejected</i> . 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 <i>Start recording</i> 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.

Event	Source entity	Description
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.
Request to exit	door	Someone has pressed the door release button or has triggered a request to exit motion detector. The <i>Request to exit</i> 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 <i>Description</i> 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.

Event	Source entity	Description
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.
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.

Event	Source entity	Description
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.
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	<p>Adds a <i>bookmark</i> to a <i>camera</i> recording.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Camera: Select the camera. • Message: Bookmark text.
Arm intrusion detection area	<p>Arms an <i>intrusion detection area</i>.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Intrusion detection area: Select the intrusion detection area. • Mode: Either <i>Master arm</i> or <i>Perimeter arm</i>. • When: Either immediately or with a delay.
Arm zone	<p>Arms a <i>virtual zone</i>.</p> <p>Parameter:</p> <ul style="list-style-type: none"> • Zone: Select a virtual zone.
Block and unblock video	<p>Blocks or unblocks a camera from other users in the system.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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	<p>Cancels the postponed arming of an <i>intrusion detection area</i>.</p> <p>Parameter:</p> <ul style="list-style-type: none"> • Intrusion detection area: Select the intrusion detection area.

Action	Description
Clear tasks	<p>Clears the task list in the specified Security Desk monitors.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Destination: Select one of the following: <ul style="list-style-type: none"> • 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	<p>Disarms an <i>intrusion detection area</i>.</p> <p>Parameter:</p> <ul style="list-style-type: none"> • Intrusion detection area: Select the intrusion detection area.
Disarm zone	<p>Disarms a <i>virtual zone</i>.</p> <p>Parameter:</p> <ul style="list-style-type: none"> • Zone: Select a virtual zone.
Display a camera on an analog monitor	<p>Displays a camera in an analog monitor in a canvas tile.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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	<p>Displays a list of entities in the Security Desk <i>canvas</i> of selected <i>users</i>, in terms of one entity per tile. This action is ignored if a user does not have a <i>Monitoring</i> task open in Security Desk.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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	<p>Sends a report (based on a saved reporting task) as an email attachment to a list of <i>users</i>.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Report: Select a saved public task. • Recipients: Select the users to the send the report to. • Export format: Report format, either <i>PDF</i> or <i>Excel</i>.

Action	Description
Email a snapshot	<p>Sends a series of snapshots of a video feed as an email attachment to a list of users.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Camera: Select the camera. • Snapshots: Select how many seconds before (maximum -300 seconds) or after (maximum 5 seconds) the defined <i>Recurrence time</i> to email the snapshot. • Recipients: Select the users who will receive the snapshot. NOTE: An email address must be defined in the user's settings. • Export format: Available image formats: <i>PNG, GIF, JPEG, or Bitmap</i>.
Export report	<p>Generates and saves a saved public task to a file location.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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	<p>Forgives an <i>antipassback</i> violation for a <i>cardholder</i>, or <i>cardholder group</i>.</p> <p>Parameter:</p> <ul style="list-style-type: none"> • Entity: Select a cardholder or cardholder group.
Go home	<p>Commands the PTZ camera to go to its home position. Not all PTZ cameras support this feature.</p> <p>Parameter:</p> <ul style="list-style-type: none"> • Camera: Select a PTZ camera.
Go to preset	<p>Commands the PTZ camera to go to the specified preset position.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Camera: Select a PTZ camera. • Preset: Preset position (number) to go to.
Import from file	<p>Imports a file and sends the import results to a <i>user</i>.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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	<p>Sets the <i>Boost quality on event recording</i> to <i>ON</i> 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 <i>Recording quality as standard configuration</i>, or until the Archiver restarts.</p> <p>Parameter:</p> <ul style="list-style-type: none"> • Camera: Select a camera.
Override with manual recording quality	<p>Sets the <i>Boost quality on manual recording</i> to <i>ON</i> 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 <i>Recording quality as standard configuration</i>, or until the Archiver restarts.</p> <p>Parameter:</p> <ul style="list-style-type: none"> • Camera: Select a camera.
Play a sound	<p>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.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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 <i>C:\Program files\Genetec Security Center 5.5\Audio</i>.
Postpone intrusion detection area arming	<p>Postpones the intrusion detection area arming.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Arming mode: Either <i>Master arm</i> or <i>Perimeter arm</i>. • 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	<p>Restarts a unit.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Entity: Select a video unit or access control unit to restart.
Recording quality as standard configuration	<p>Cancels the effect of the <i>Override with manual recording quality</i> and <i>Override with event recording quality</i> actions and restores the standard recording configuration.</p> <p>Parameter:</p> <ul style="list-style-type: none"> • Camera: Select a camera.

Action	Description
Reset area people count	Resets the people counter in an <i>area</i> . Parameter: <ul style="list-style-type: none"> • Area: Select an area.
Reset external system	Forces the Omnicast Federation role to reconnect to the remote <i>Omnicast</i> system. Parameter: <ul style="list-style-type: none"> • Role: Select an Omnicast Federation role.
Run a macro	Starts the execution of a <i>macro</i> . Parameters: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Recipients: Select a user or user group. • Message: Text to be 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: <ul style="list-style-type: none"> • 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 a Security Desk application. Parameters: <ul style="list-style-type: none"> • Task: Select a saved public task to send. • Destination: Select one of the following: <ul style="list-style-type: none"> • 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	<p>Sets the reader mode for accessing doors.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Location: Select an area, door, or elevator. • Reader mode: Select whether access is granted using <i>Card and PIN</i>, or <i>Card or PIN</i>, for the selected area, door, or elevator. <p>This action only works with door controllers and readers that support this feature.</p>
Set the door maintenance mode	<p>Sets the <i>Unlocked for maintenance</i> status of a <i>door</i> to on or off.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Door: Select a door. • Maintenance: Desired maintenance mode (On or Off).
Set threat level	<p>Sets a threat level on your Security Center system, or on specific areas.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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	<p>Resets the Buzzer output defined for a door. This action sets the <i>Buzzer</i> option to <i>None</i> in the <i>Hardware</i> tab of a door in Config Tool.</p> <p>Parameter:</p> <ul style="list-style-type: none"> • Door: Select a door.
Sound buzzer	<p>Sets the Buzzer output defined for a door. The buzzer sound is specified under the <i>Buzzer</i> option in the <i>Hardware</i> tab of a door in Config Tool.</p> <p>Parameter:</p> <ul style="list-style-type: none"> • Door: Select a door.

Action	Description
Start applying video protection	<p>Starts protecting upcoming video recordings against deletion. The protection is applied on all <i>video files</i> needed to store the protected <i>video sequence</i>. Since no video file can be partially protected, the actual length of the protected video sequence depends on the granularity of the video files.</p> <p>When multiple <i>Start applying video protection</i> actions are applied on the same video file, the longest protection period is kept.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Camera: Select a camera. • Keep protected for: Duration of the video protection. <ul style="list-style-type: none"> • Specific: Sets the protection period in number of days. • Infinite: The protection can only be removed manually from the <i>Archive storage details</i> task. • Protect video for next: Duration of the video to protect. <ul style="list-style-type: none"> • Specific: Sets the duration in minutes and hours. • Infinite: All future recordings are protected until the action <i>Stop applying video protection</i> is executed.
Start recording	<p>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.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Camera: Select a camera. • Recording duration: Sets the duration of the video recording. <ul style="list-style-type: none"> • Default: Sets the duration to follow the value defined in <i>Default manual recording length</i> configured for the camera. • Infinite: The recording can only be stopped by the <i>Stop recording</i> action. • Specific: Sets the recording duration in seconds, minutes, and hours.
Start transfer	<p>Starts an archive transfer.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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.

Action	Description
Stop applying video protection	<p>Stops protecting upcoming video recordings against deletion. This action does not affect the <i>video archives</i> that are already protected.</p> <p>Additional parameter:</p> <ul style="list-style-type: none"> • Camera: Select a camera. • Stop in: Sets the video protection to stop <i>Now</i> or in a <i>Specific</i> amount of time in minutes and hours.
Stop recording	<p>Stops recording on the specified camera. This action only works if the recording was started by the <i>Start recording</i> action.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Camera: Select a camera. • Stop in: Sets the recording to stop <i>Now</i> or in a <i>Specific</i> amount of time in seconds, minutes and hours.
Stop transfer	<p>Stops an archive transfer.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Transfer group: Select a transfer group to stop the transfer for.
Synchronize role	<p>Starts a synchronization process on the specified role (<i>Active Directory</i> or <i>Global Cardholder Synchronizer</i>).</p> <p>Parameter:</p> <ul style="list-style-type: none"> • 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	<p>Temporarily locks or unlocks a door for a given period of time.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Door: Select a door. • Lock mode: Select <i>Unlocked</i> or <i>Locked</i>. <ul style="list-style-type: none"> • For: Amount of time in minutes or hours. • From/To: Date and time range to unlock the door.
Trigger alarm	<p>Triggers an alarm.</p> <p>NOTE: Triggering an alarm might generate additional events, depending on the alarm configuration.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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.

Action	Description
Trigger intrusion alarm	<p>Triggers a physical alarm on an intrusion detection area.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Recipient type: Type of alarm trigger, either the intrusion detection area or a specific alarm input. • Intrusion detection area: Select an intrusion detection area.
Trigger output	<p>Triggers an <i>output behavior</i> on an output pin of a <i>unit</i>. For example, an action can be configured to trigger the output pin of a unit (controller or input/output module).</p> <p>Parameters:</p> <ul style="list-style-type: none"> • Output relay: Select an output pin (unit). • Output behavior: Select the output behavior to trigger.
Unlock door explicitly	<p>Temporarily unlocks a door for five seconds, or the <i>Standard grant time</i> configured for that door.</p> <p>Parameter:</p> <ul style="list-style-type: none"> • Door: Select a door.

Graphical overview of Security Desk tasks

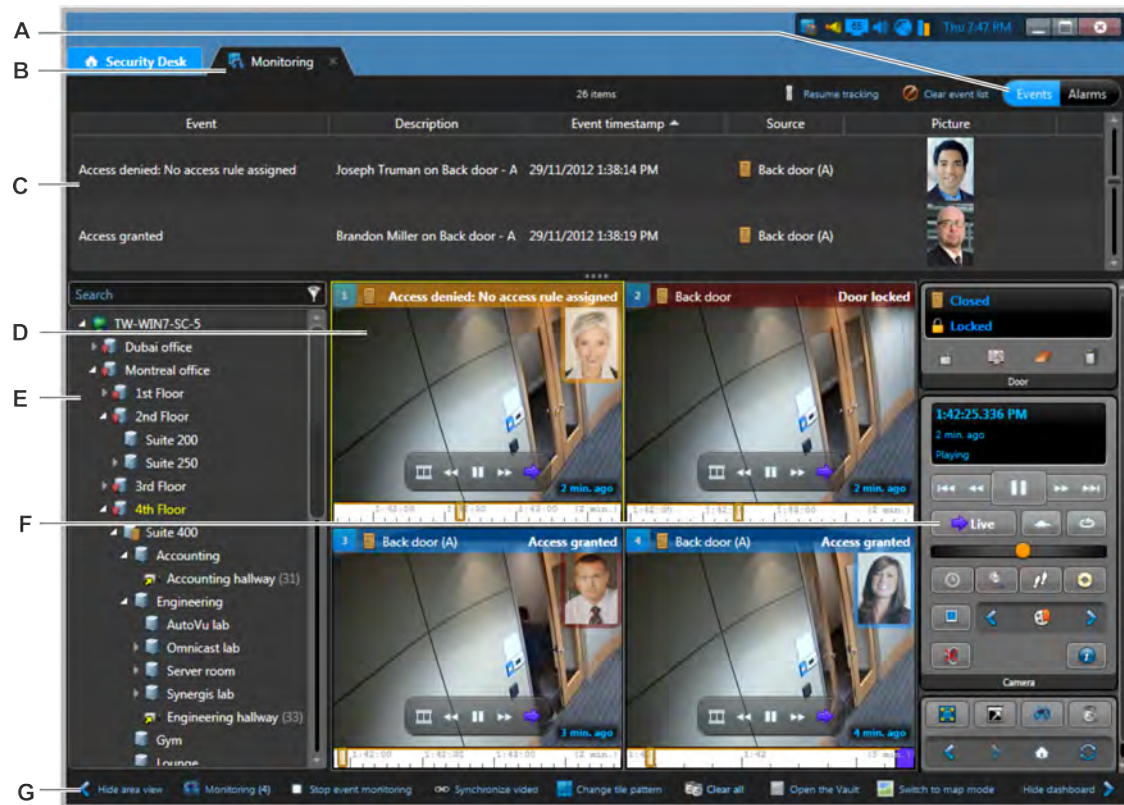
This section includes the following topics:

- ["Overview of the Monitoring task"](#) on page 453
- ["Overview of the Maps task"](#) on page 455
- ["Overview of the Remote task"](#) on page 458
- ["Overview of the Bookmarks task"](#) on page 459
- ["Overview of the Archives task"](#) on page 461
- ["Overview of the Motion search task"](#) on page 462
- ["Overview of the Video file explorer task"](#) on page 464
- ["Overview of the Archive storage details task"](#) on page 466
- ["Overview of the Cardholder management task"](#) on page 468
- ["Overview of the Visitor management task"](#) on page 470
- ["Overview of the Credential management task"](#) on page 472
- ["Overview of the Hotlist and permit editor task"](#) on page 474
- ["Overview of the Inventory management task"](#) on page 475
- ["Overview of the Patroller tracking task"](#) on page 476
- ["Overview of the System status task"](#) on page 479
- ["Overview of the Alarm monitoring task"](#) on page 484
- ["Overview of the Alarm report task"](#) on page 485
- ["Overview of the Enhanced cardholder access rights task"](#) on page 486

Overview of the Monitoring task

Use the Monitoring task to monitor *events*, such as access control events from doors and cardholders, license plate reads and hits from fixed and mobile LPR units, and camera related events, in real time.

The following figure shows a Monitoring task in an access control and video monitoring system.



- A**
- **Events:** Show events in the report pane.
 - **Resume tracking:** Show the events in the list as soon as they occur.
 - **Clear event list:** Remove all the events from the event list.
 - **Alarms:** Show alarms in the report pane. The same commands as found in the [Alarm monitoring task](#).

NOTE: The Events and Alarms toggle button only appears when you [enable alarm monitoring for the Monitoring task](#).

- B** New event alerts appear on the Monitoring tab when the task is not in the foreground.
- C** The report pane lists events (shown here) as they occur in real time, or alarms, based on your selection.
- D** A tile can be used to monitor either events (tile ID is blue), alarms (tile ID is red), both, or neither (tile ID is grey).
- E** Select entities from the area view to view in the canvas. You can select multiple entities, and drag them onto the canvas all at once.

F Widgets used to control the entities that you are monitoring.

- G**
- **Hide area view:** Hide the area view.
 - **Monitoring:** Select which entities to monitor.
 - **Synchronize video:** Synchronize the video that is displayed in the canvas.
 - **Clear all:** Clear all the configured tiles in the Monitoring task.
 - **Change tile pattern:** Change the tile pattern in the canvas.
 - **Open the Vault:** Open the Vault tool to view previously saved snapshots and exported video files.
 - **Switch to map mode:** Switch between tile mode and map mode
 - **Hide dashboard:** Hide the dashboard.
-

Related Topics

[Monitoring events](#) on page 64

[Selecting entities to monitor](#) on page 65

[Synchronizing video in tiles](#) on page 137

[Changing tile patterns](#) on page 27

[Taking snapshots of video](#) on page 146

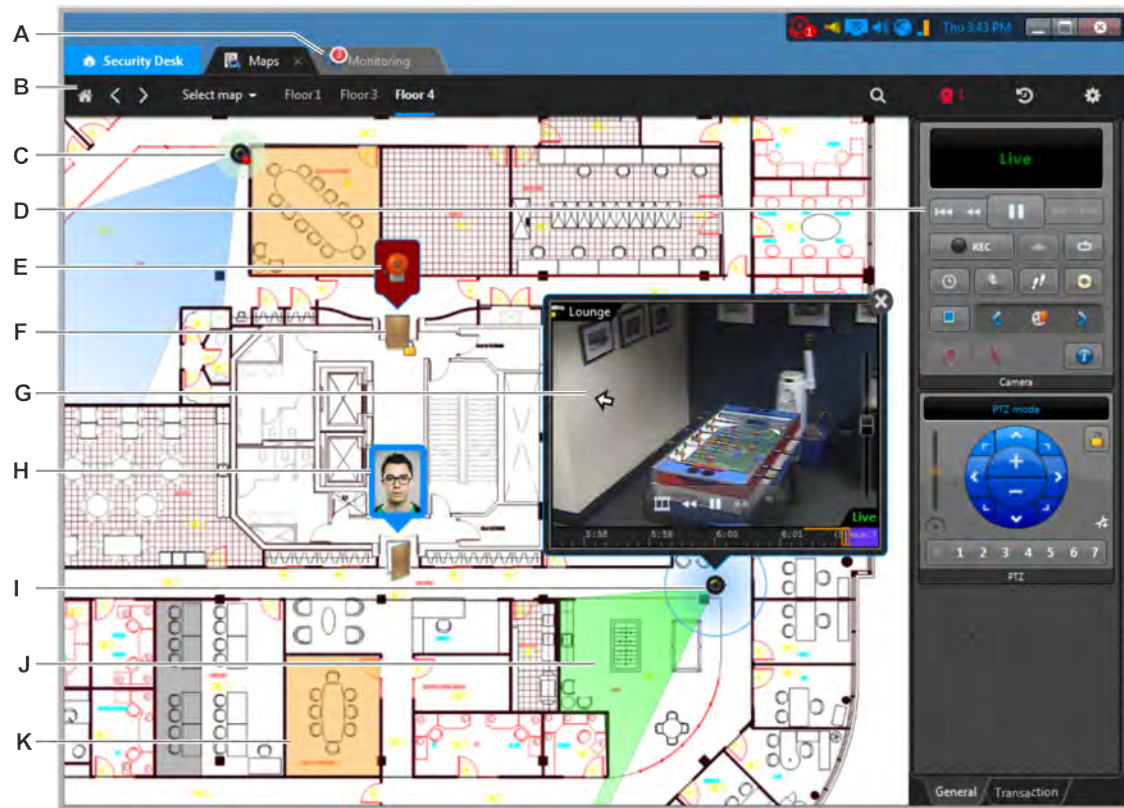
[Viewing exported video files](#) on page 184

[Monitoring LPR events in tile mode](#) on page 298

Overview of the Maps task

Use the Maps task to monitor *events* and *alarms* in real time, while keeping an eye on the overall situation with a map.

The following figure shows a Maps task in an access control and video monitoring system. Security Center entities are represented as clickable icons and colored areas on the map, called *map objects*.










- A** Map objects you double-click are displayed in the Monitoring task.
- B** Use the [Maps toolbar](#) to switch to different maps and to configure your map display options.
- C** Fixed cameras (map objects) are represented with a blue field of view (FOV). Recording state (📹) and *Motion on events* (🌊 green ripple effect) are also shown in real time.
- D** Widgets corresponding to the selected map object (here a PTZ camera) are displayed in the dashboard. To hide the dashboard, click **Settings > Show dashboard** in the toolbar.
- E** A map object that is linked to an active alarm is flagged with an alarm notification bubble. Point to the bubble to show more details. Click the notification bubble to change it into a tile bubble.
- F** Doors (map objects) are represented with an icon that indicates their current state (*open/closed, locked/unlocked*).
- G** Click a map object (here a PTZ camera) to display it in a tile bubble. Click again to hide the bubble. Use Ctrl+Click to open multiple tile bubbles.

-
- H** Events are displayed in event notification bubbles. The color of the bubble corresponds to the color assigned to the event. Point to the bubble to show more details. Click the notification bubble to change it into a tile bubble.
-
- I** PTZ cameras (map objects) are represented with a green FOV.
-
- J** Click and drag the FOV to pan and tilt. Drag the mouse cursor closer to the camera icon to tilt the camera down, or further from the camera icon to tilt it up.
-
- K** Areas (map objects) are represented by colored polygons. Click the polygon to switch to the map linked to the area.
-

Maps toolbar

Use the toolbar in the Maps task to select the map to display and to configure your map display options.

The Maps toolbar is divided in two parts. On the left, you have the map navigation commands. On the right, you have the display option commands.

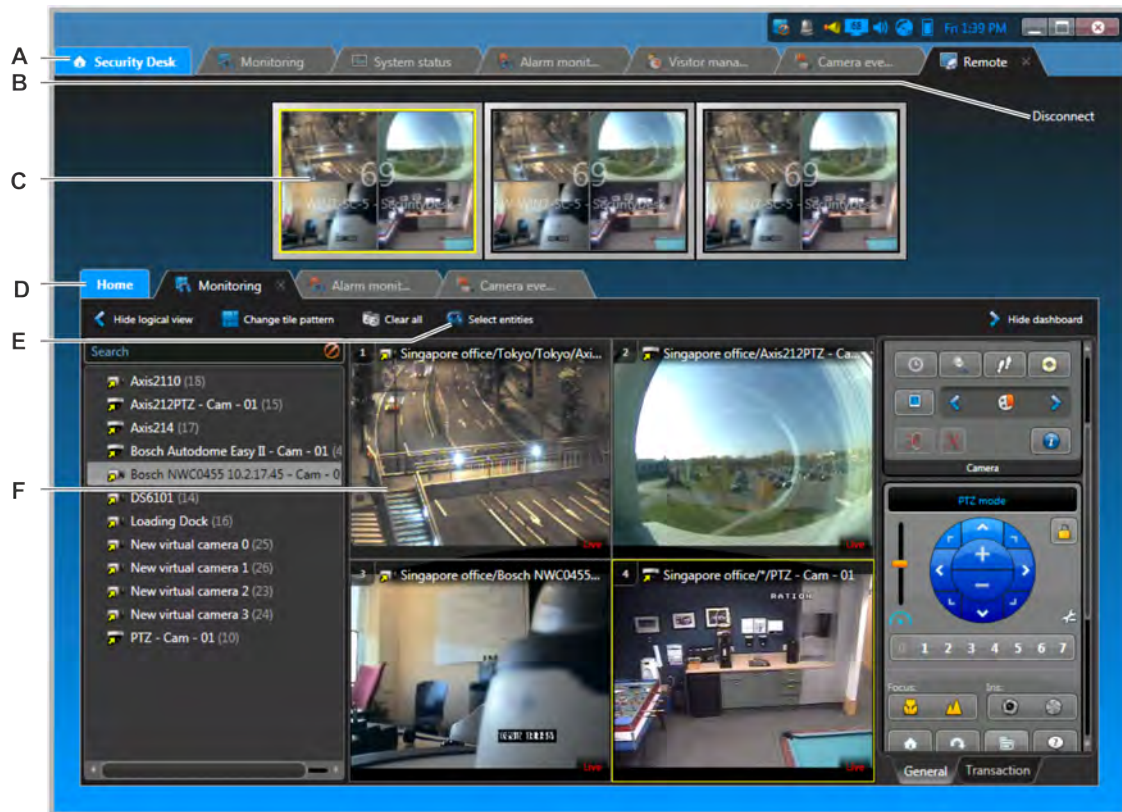
-  **Default map:** Switches to the default map defined for the whole system.
- **Select map:** Shows your list of favorites and the map hierarchy. Listed beside this command are the siblings of the current map.
-  **Search:** Searches for maps and map objects by name.
-  **Alarms:** Lists all active alarms in a floating window. The icon turns red when there are active alarms in the system.
 - Right-click an alarm in the list to access the alarm contextual menu.
 - Double-click an alarm to switch to a map where the alarm is displayed.
 - Click  to change the sorting order of the alarms or the position of the window.
 - Click **Trigger an alarm** to show the list of alarms you can trigger manually.
 - Click **Force ack all** to forcibly acknowledge all alarms in the system.
-  **Past events:** Lists all past events in a floating window.
 - Right-click an event in the list to access the event contextual menu.
 - Double-click an event to switch to the map showing the source of the event.
 - Click  to change the sorting order of the events or the position of the window.
 - Click **Clear** to clear the event list.
-  **Settings:** Opens the **Settings** menu.
 - **Layers:** [Show or hide information on the map.](#)
 - **Show dashboard:** Show or hide the dashboard. Same as typing **F7**.
 - **Span map across all monitors:** Use all monitors attached to Security Desk to display the map.
 - **Manage:** Configure favorites and default maps.
 - **Add map to favorites:** Add the current map to your list of favorites.
 - **Edit map:** Open the Map designer task in Config Tool to edit the current map. You need the *Map designer* privilege to use this command.

- **Set map as default:** Set the current map as your default map, the first map that's loaded when you open the Maps task.
- **Set map as global default:** (Administrators only) Set the current map as the global default map for all users.
- **Help:** View tips to help you get started using maps.

Overview of the Remote task

Use the Remote task to monitor and control other Security Desks that are part of your system remotely.

The following figure shows a Remote task.



- A** Local Security Desk tasks you are working on. Click a tab to switch to that task.
- B** Disconnect from the remote Security Desk.
- C** Switch between Security Desk monitors you are connected to in Wall mode.
- D** Remote Security Desk tasks that are open. When you are connecting remotely, you can only use the *Monitoring* task and the *Alarm monitoring* task.
- E** Select the entities you want to monitor.
- F** Monitor entities in the canvas. What you display in the canvas is also shown in the remote Security Desk canvas.

Related Topics

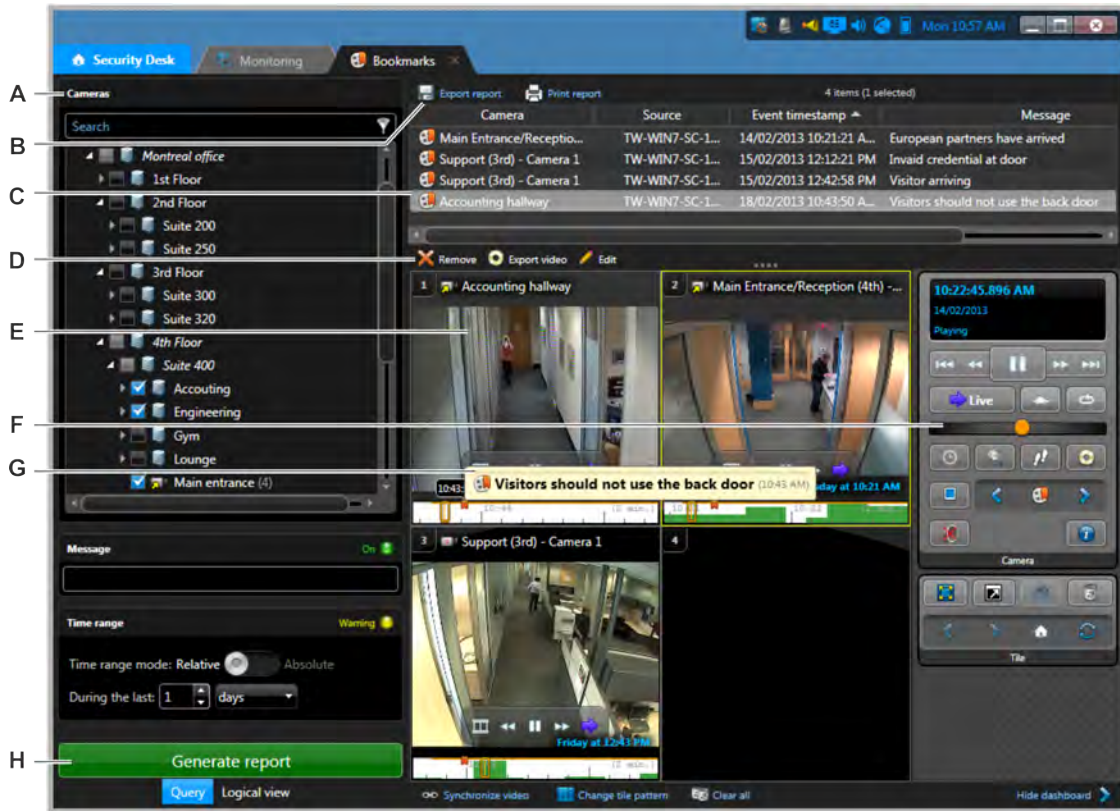
[Remote monitoring](#) on page 77

[Connecting to remote Security Desks](#) on page 78

Overview of the Bookmarks task

Use the Bookmarks task to search for, view, and generate a report of saved bookmarks.

The following figure shows the Bookmarks task.



A Query filters.

B [Export](#) or [print](#) the report.

C The bookmark events are listed in the report pane.

D Options available when a bookmark is selected in the report pane:

- - Delete the selected bookmarks from the database.
- - Export video associated with the selected bookmarks.
- - Edit the selected bookmarks.

E Video of the bookmark in a tile.

F [Camera widget](#).

G The bookmark message appears when you hover your mouse pointer over a bookmark in a tile, if one was written.

H Run the report.

Related Topics

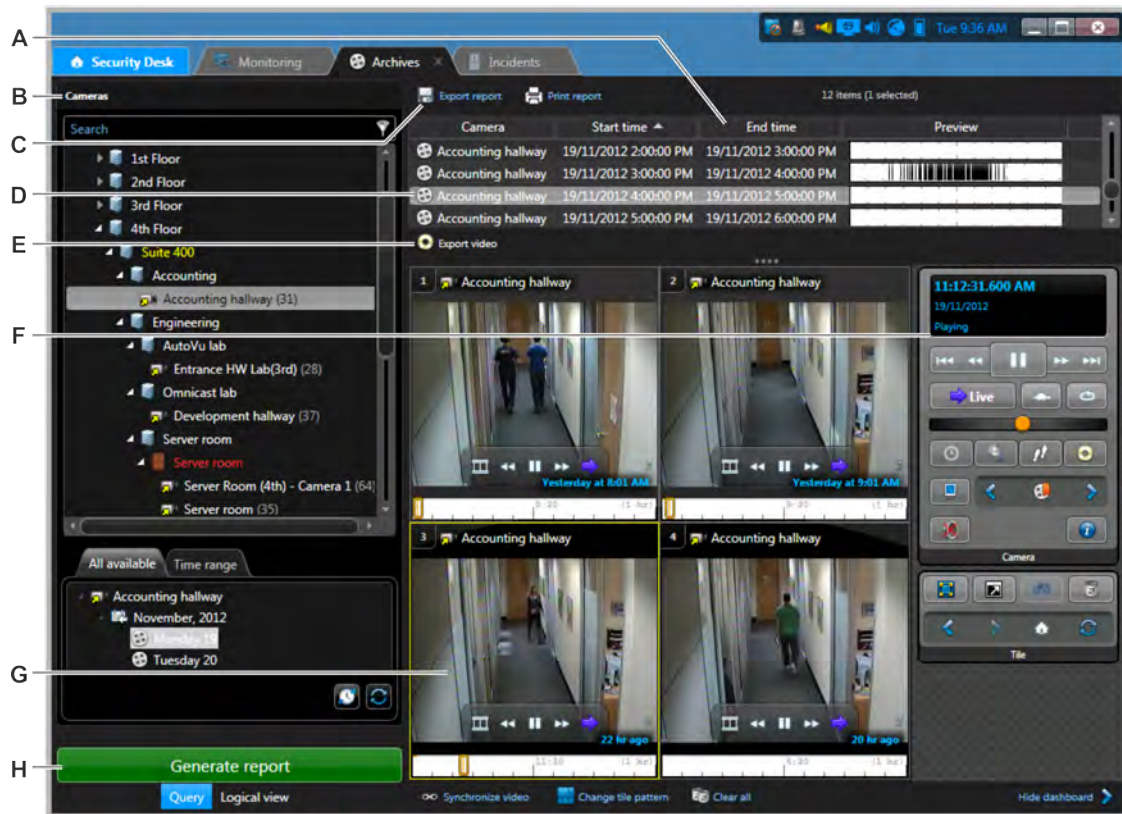
[Adding bookmarks to video sequences](#) on page 143

[Viewing bookmarked videos](#) on page 143

Overview of the Archives task

Use the Archives task to find and view available *video archives* on your system by camera and time range.

The following figure shows the Archives task.



A Report pane columns.

B Query filters.

C [Export](#) or [print](#) the report.

D The related video recordings are listed in the report pane.

E [Export video](#) from the selected archive.

F [Camera widget](#).

G Video sequence of an archive in a tile.

H [Run the report](#).

Related Topics

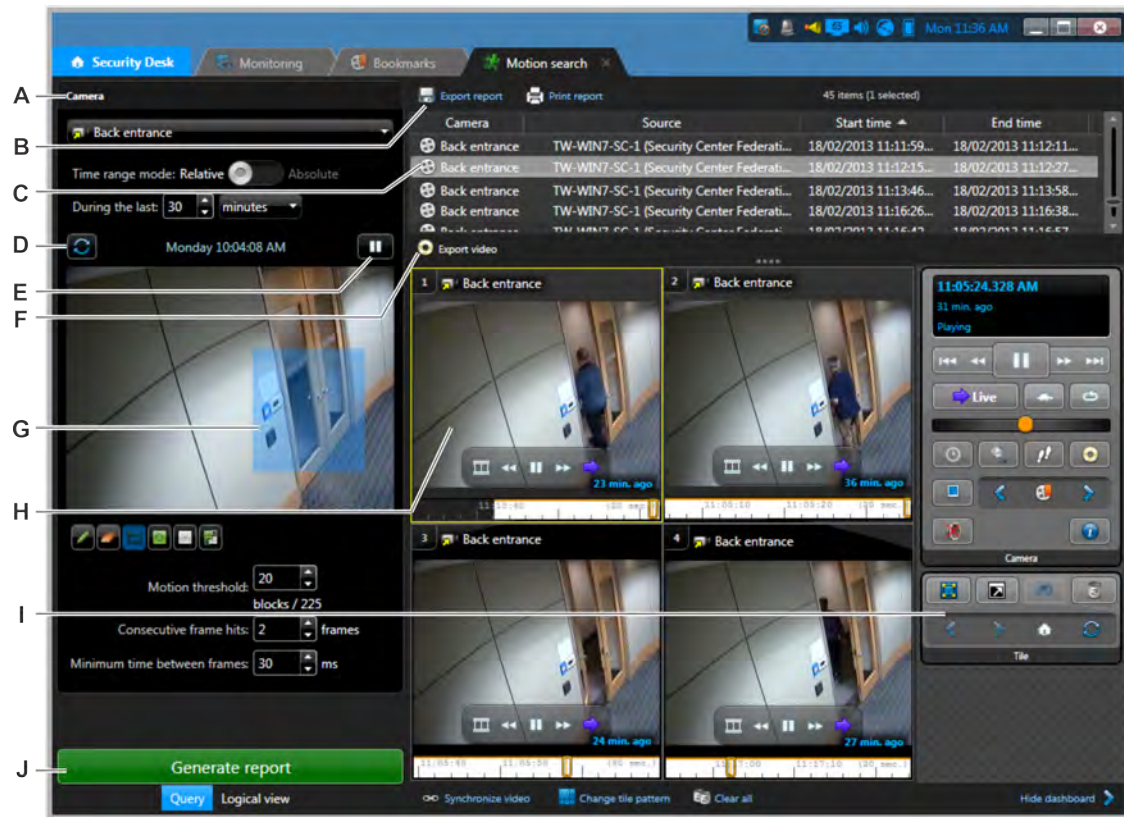
[Viewing video archives](#) on page 161

[Exporting video](#) on page 179

Overview of the Motion search task

Use the Motion search task to search the video archives for *video sequences* that detect motion in specific areas of a camera's field of view.

The following figure shows the Motion search task.



- A Query filters.
- B Export or print the report.
- C The motion events are listed in the report pane.
- D Refresh the preview image.
- E Play the video in the preview image.
- F Export video associated with the selected bookmarks.
- G Motion detection zone for your search.
- H Video sequence of a motion event in a tile.
- I Dashboard widgets.
- J Run the report.

Related Topics

[Searching video archives for motion events](#) on page 164

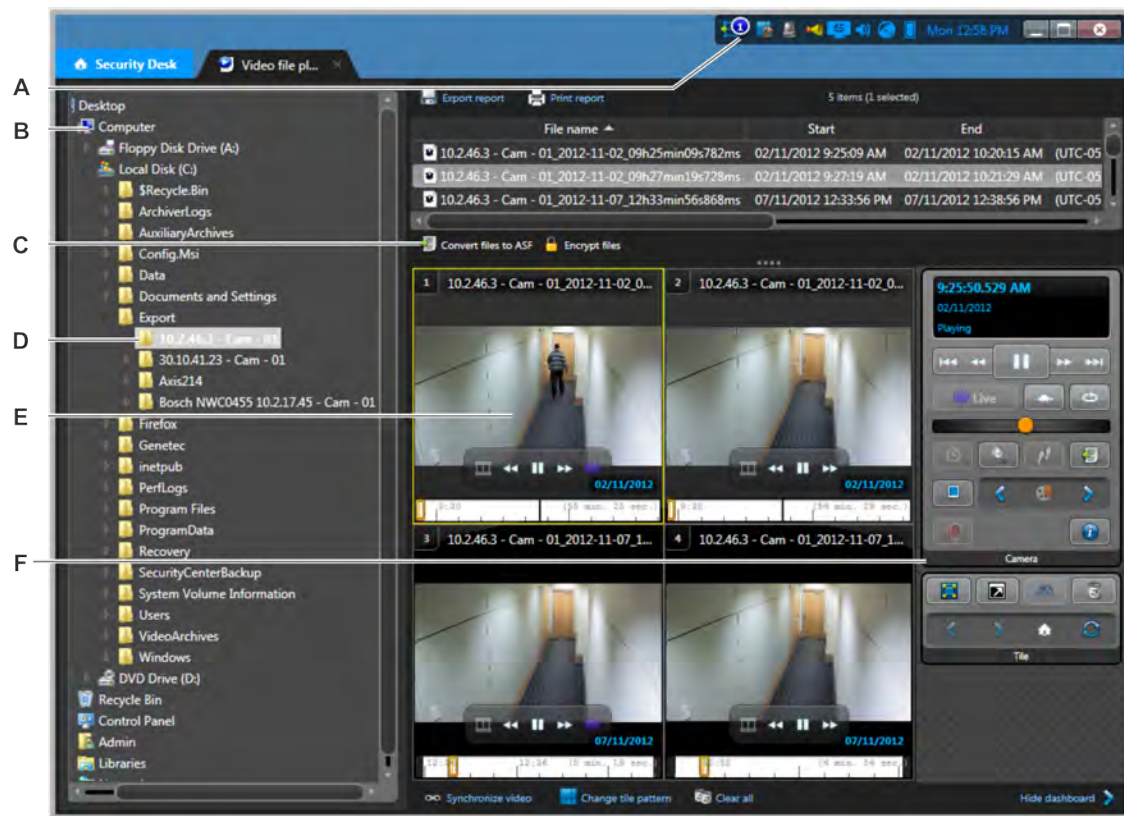
[Exporting video](#) on page 179

Overview of the Video file explorer task

You can use the Video file explorer task to search for and view your exported G64x *video files*.

During the playback of a video file, the timeline does not show any event marker if the following applies:

- The video file was created before Omnicast 4.x. Video files that were created through the *Export* operation from Omnicast 4.x, or later, can contain bookmark or motion event markers.
- The video file is still managed by an Archiver or Auxiliary Archiver (typically found under *\VideoArchives*).
- The video file is part of a backup set (typically found under *\Tables\VideoFile*).



- A** Open the *Conversion* dialog box. This icon only appears when you are converting G64 files to ASF format.
- B** Browse for video files in folders that are on your network.
- C** Options that are available when a video file is selected in the report pane:
- - [Convert the selected video files to ASF format](#).
 - - [Encrypt the selected video files](#). If the video file is already encrypted, is displayed instead.
- D** Selected folder. The video files that are contained in the folder appear in the report pane.

E Exported video file in a tile.

F Dashboard widgets.

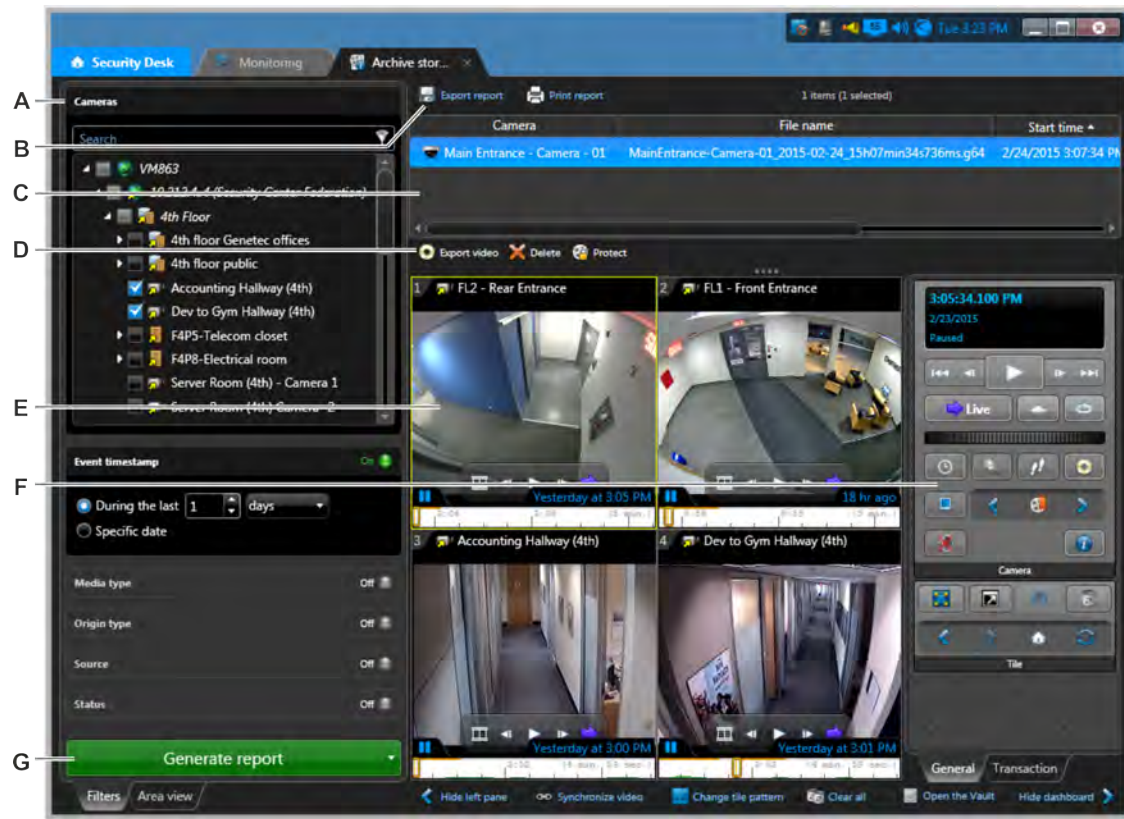
Related Topics

[Viewing exported files in the Video file explorer](#) on page 185

Overview of the Archive storage details task

Use the Archive storage details task to find the *video files* used to store *video archives* from cameras and view the properties of the video files.

The following figure shows the Archive storage details task.



A Query filters.

B [Export](#) or [print](#) the report.

C The video files are listed in the report pane.

D Options available when a video file is selected in the report pane:

- - Export video associated with the selected video files.
- - Remove the selected video file from the database.
- - [Protect the selected video files](#).
- - Remove the automatic deletion protection from selected video files.

E Video file displayed in a tile.

F Dashboard widgets.

G Run the report.

Related Topics

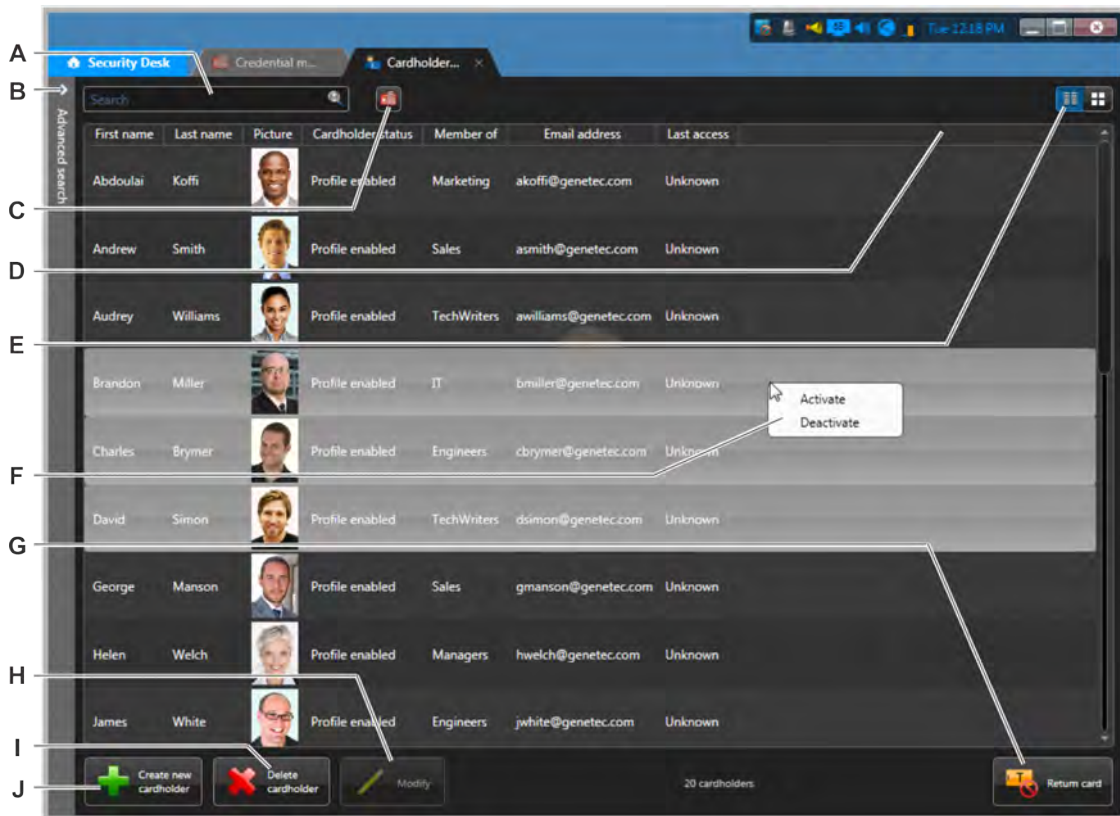
[Viewing the properties of video files](#) on page 192

Overview of the Cardholder management task

Use the Cardholder management task to create new *cardholders* in your system, modify existing cardholders, and assign credentials to cardholders.

The following figure shows the Cardholder management task.

NOTE: You can only have one instance of this task in Security Desk.



A Find a cardholder by name.

B Advanced search options.

C Find a cardholder using their credential.

D Select which columns to display by right-clicking the column headers or by typing Ctrl+SHIFT+C..

E Switch between *Tiles* and *List* view.

- **Tiles:** Shows large pictures. Pictures can be resized.
- **List:** List all information concerning the entity: first name, last name, picture, activation date, expiration date, check-in date, and any custom fields that are defined.

F Activate or deactivate multiple cardholders at once.

You can only make bulk changes to cardholders in the *List* view.

G Return a temporary card.

H View or modify the selected cardholder.

I Delete the selected cardholder.

J Create a new cardholder.

Related Topics

[Creating cardholders](#) on page 214

[Assigning credentials](#) on page 223

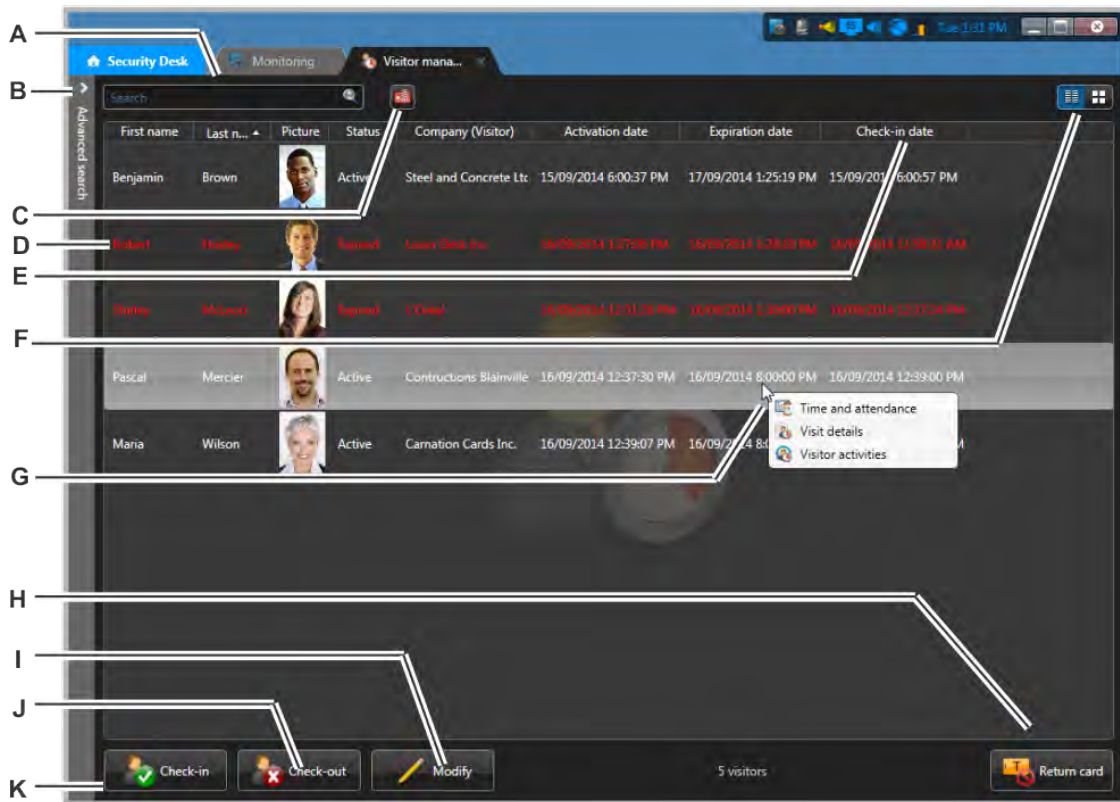
[Assigning temporary cards](#) on page 227

Overview of the Visitor management task

Use the Visitor management task to check-in new visitors, modify existing visitors, and assign credentials to visitors.

The following figure shows the Visitor management task.

NOTE: You can only have one instance of this task in Security Desk.



A Find a visitor by name.

B Advanced search options.

C Find a visitor using their credential.




D Visitors whose profiles are inactive or expired are displayed in red.

E Select which columns to display by right-clicking the column headers or by typing **Ctrl+SHIFT+C**.

F Switch between *Tiles* and *List* view.

- **Tiles:** Shows large pictures. Pictures can be resized.
- **List:** List all information concerning the entity: first name, last name, picture, activation date, expiration date, check-in date, and any custom fields that are defined.

G Generate visitor reports by right-clicking the selected visitor.

-  Time and attendance.
-  Visit details.
-  Visitor activities.

H Return a temporary card.

I View or modify the selected visitor.

J Check-out the selected visitor.

K Check-in a new or returning visitor.

Related Topics

[Searching for cardholders and visitors](#) on page 247

[Checking in new visitors](#) on page 218

[Checking out visitors](#) on page 230

[Tracking attendance in an area](#) on page 238

[Tracking the duration of a visitor's stay](#) on page 239

[Investigating visitor events](#) on page 233

[Restoring original cards to cardholders and visitors](#) on page 227

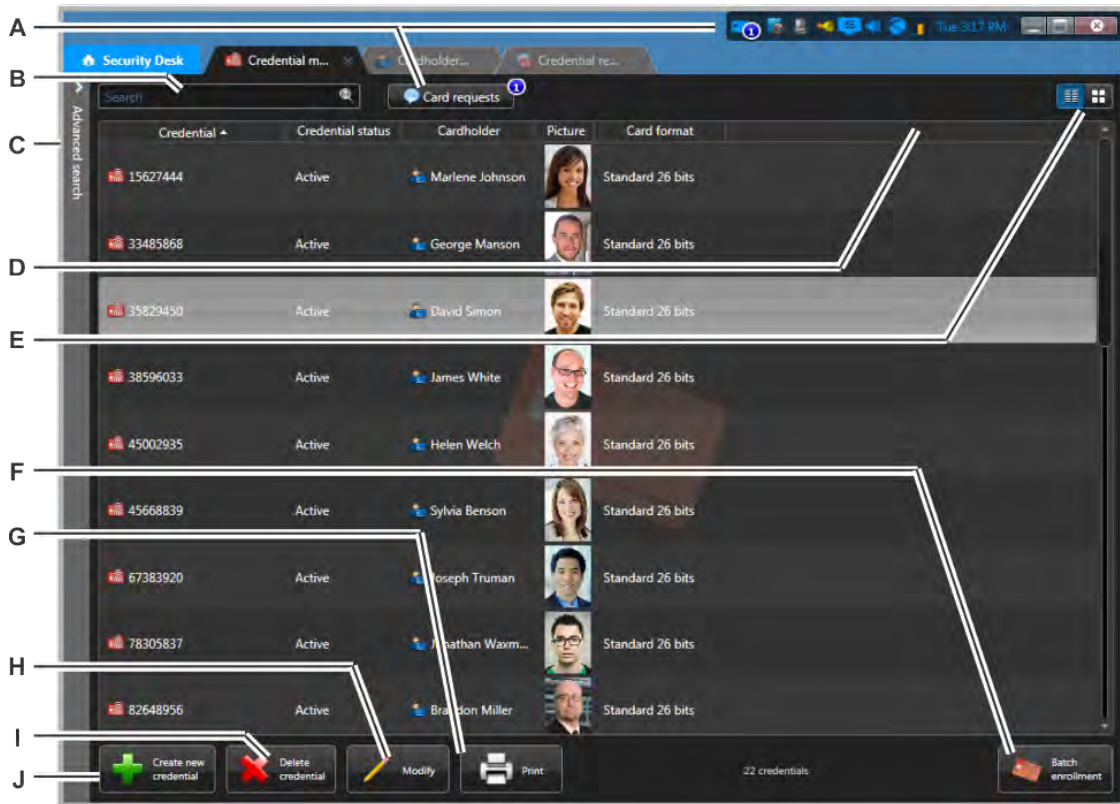
[Checking in returning visitors](#) on page 220

Overview of the Credential management task

Use the Credential management task to create, modify, and delete credentials, and print badges.

The following figure shows the Credential management task.

NOTE: You can only have one instance of this task in Security Desk.



A View, modify, or respond to outstanding credential card requests.

B Find a credential by name.

C Advanced search options.

D Select which columns to display by right-clicking the column headers or by typing Ctrl+SHIFT+C.

E Switch between *Tiles* and *List* view.

- **Tiles:** Shows large pictures. Pictures can be resized.
- **List:** List all information concerning the entity: first name, last name, picture, activation date, expiration date, check-in date, and any custom fields that are defined.

F Enroll multiple credentials into your system at once.

G Print the selected credential cards.

H View or modify the selected credential.

I Delete the selected credentials.

J Create a new credential.

Related Topics

[Creating credentials](#) on page 259

[Enrolling multiple credentials automatically](#) on page 255

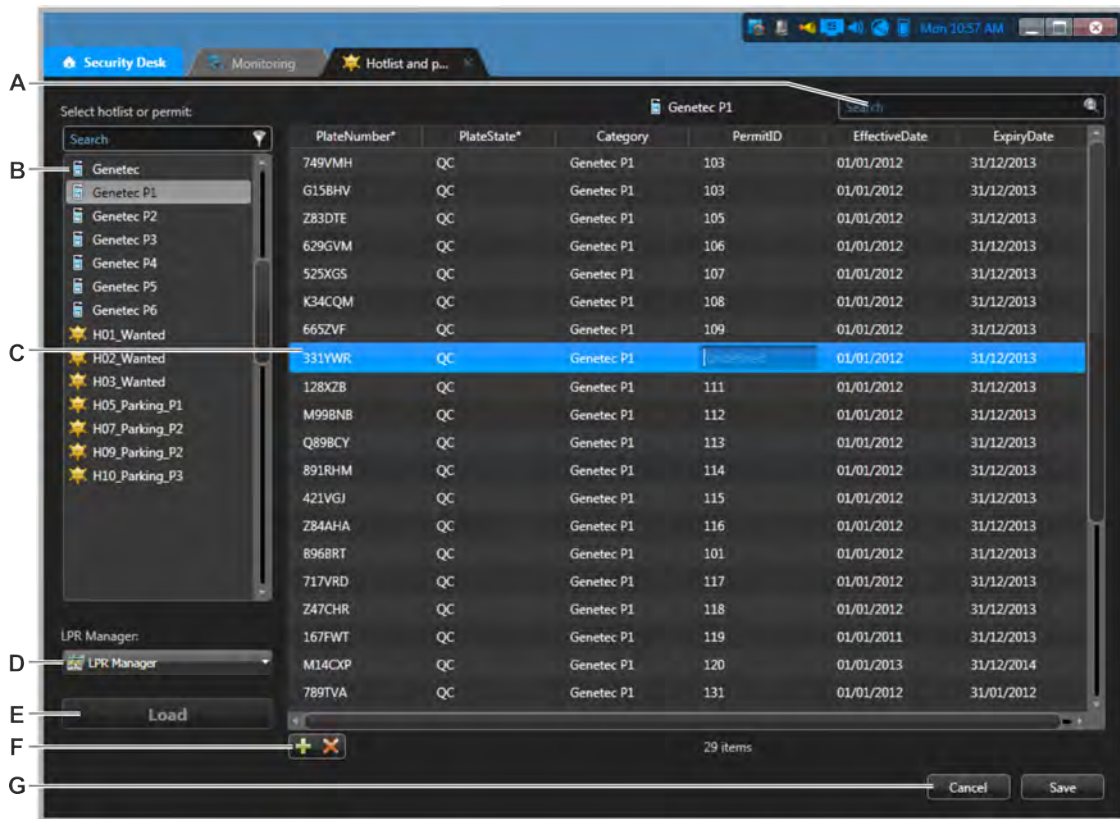
[Enrolling multiple credentials manually](#) on page 257

[Searching for credentials](#) on page 269

Overview of the Hotlist and permit editor task

Use the Hotlist and permit editor task to edit a *hotlist* or parking *permit* list for all your *Patrollers* at the same time.

The following figure shows the Hotlist and permit editor task.



- A** Find specific rows in your list.
- B** Available hotlists and permits.
- C** Selected row available for editing.
- D** List of LPR Managers.
- E** Load the selected hotlist or permit list.
- F** Add or delete the selected row from the list.
- G** Save or cancel your changes.

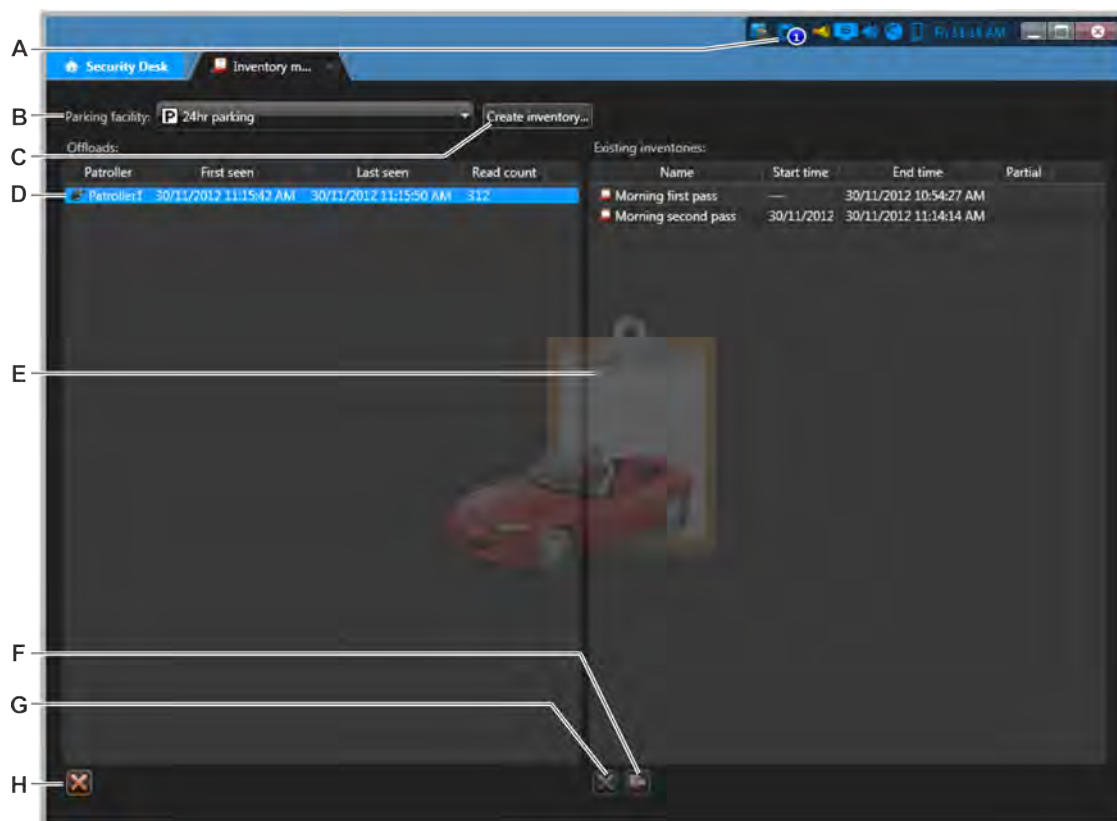
Related Topics

[Editing hotlists and permit lists on page 306](#)

Overview of the Inventory management task

Use the Inventory management task to add and reconcile MLPI license plate reads to a parking facility inventory.

The following figure shows the Inventory management task.



- A** The Inventory icon displays the number of MLPI offload files waiting to be reconciled.
- B** Parking facility selected to add the inventory to.
- C** Create an inventory.
- D** The Offloads section displays information about the MLPI offload. The file remains in the Offloads section until it is added or removed from the parking facility.
- E** The Existing inventories section displays the inventories you created.
- F** Open the Inventory report task to view and compare your parking facilities.
- G** Delete the selected inventory.
- H** Delete an offload file.

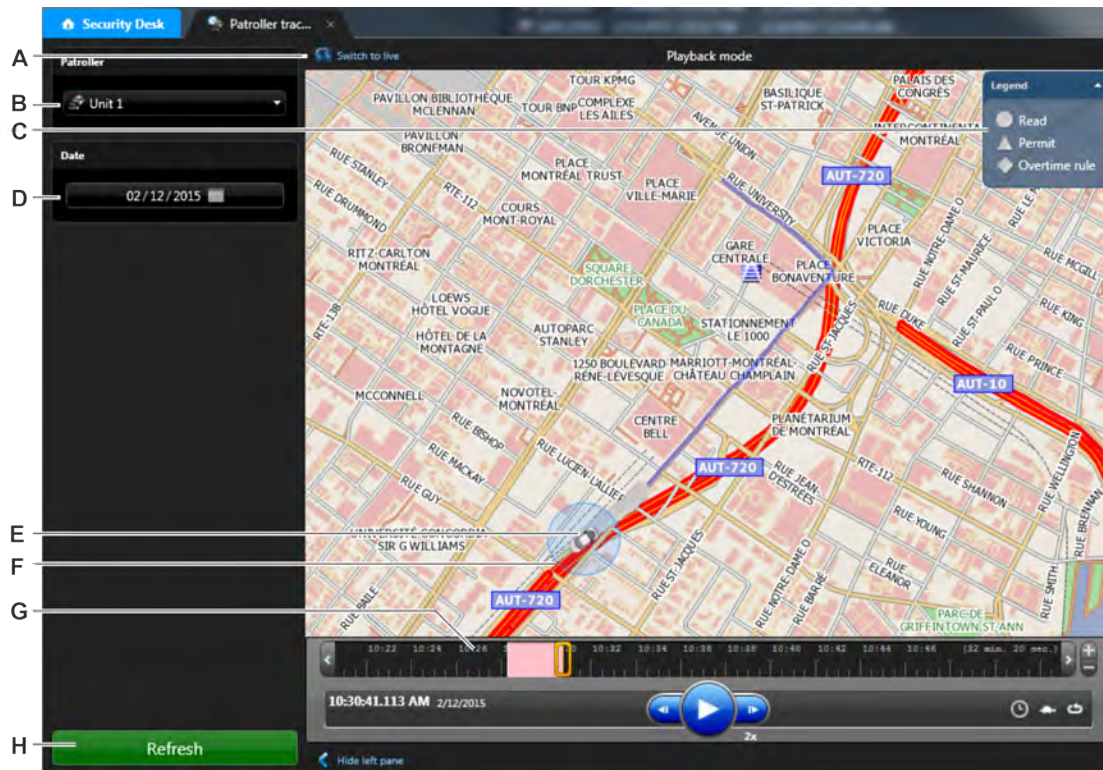
Related Topics

[Creating parking facility inventories](#) on page 341

Overview of the Patroller tracking task

Use the Patroller tracking task to replay the route taken by a Patroller on a given date on a map, or track the Patroller's live position on a map.

The following figure shows the Patroller tracking task.



- A Tracking mode. Click this to select the mode you want. **Playback mode** opens by default but you can click **Switch to live** to track the Patroller's current position on the map.
- B Patroller you are investigating.
- C Map legend.
- D Date of the Patroller route.
- E The car icon indicates the current Patroller position, and the direction of the Patroller unit as it moves through the route.
- F The blue circle indicates the last LPR read or hit that was played back in the timeline.
- G The Patroller route and LPR events are laid out in chronological order in the timeline ruler.
- H Refresh the screen and generate the Patroller route playback report.

Related Topics

[Replaying Patroller routes](#) on page 330

[Monitoring LPR events in map mode on page 300](#)


[Tracking the current location of a Patroller on page 331](#)



Patroller tracking timeline controls

Use the Patroller tracking task to replay the route taken by a Patroller on a given date on a map.

Patroller tracking provides the following timeline controls in playback mode to help you navigate through the Patroller route and locate LPR events.



A	Scroll buttons	Move to another position in the timeline without moving the playback cursor.
B	Playback timestamp	Indicates the time and date of the Playback cursor location in the timeline.
C	Playback cursor	Indicates the current location in the Patroller route. To change the playback frame drag the cursor to the new position or click on the timeline.
D	Rewind/Forward buttons	During playback, the Rewind and Forward buttons appear to the left and right of the Play button. When you click Rewind or Forward, a speed control slider appears. Drag the slider to the right to fast forward (1x, 2x, 4x, 6x, 8x, 10x, 20x, 40x and 100x) or to the left for rewind (-1x, -4x, 10x, -20x, -40x or -100x). When the desired speed is set, release the mouse button. To return to normal speed (1x), click the Play/Pause button. NOTE: The map does not automatically center itself when playback is not running at normal speed.
E	Play/Pause	Switch between playing and pausing the route playback. You can also press the Spacebar.
F	Event markers	Light red vertical lines on the timeline ruler indicate read events. Dark red vertical lines on the timeline ruler indicate hit events. Clicking an event marker moves the view in the map to the location on the event.
G	White areas	White areas on the timeline ruler indicate a Patroller route sequence. Black areas indicate that no one is patrolling during that time. Purple areas indicate the future.
H	Zoom controls	Control the portion of playback sequence that appears in the timeline. Zoom in to the timeline to view the exact location of an LPR event.
	Go to specific time	Open a browser window, and jump to a precise date and time in the recording.

	Slow motion	Play the Patroller route in slow motion. A speed control slider appears to the right of the Play/Pause button. Drag the double-arrow cursor along the slider to change the speed. Slow motion is available in the following speeds: 1/8x, 1/4x, 1/3x, 1/2x and 1x. The default playback speed is 1/8x. NOTE: Slow motion rewind is not supported.
	Loop playback	Automatically restart the route sequence when it reaches the end of the sequence during playback.

Related Topics

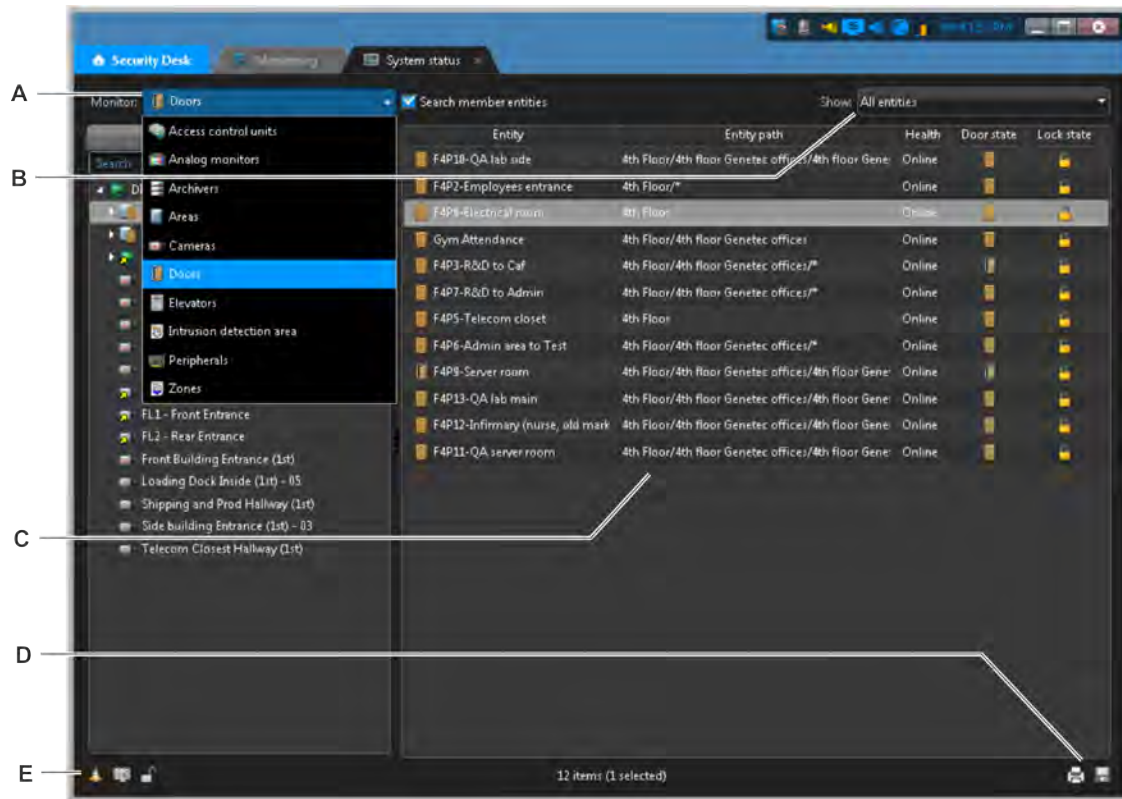
[Replaying Patroller routes](#) on page 330

[Tracking the current location of a Patroller](#) on page 331

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.



- 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.

Related Topics

[Monitoring the status of your system](#) on page 392

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	Columns	Description
Access control units	Entity	Unit name
	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)
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	Columns	Description
	People count	Working (#) or Not working (blank)
	Antipassback	Hard, Soft, or None (no <i>antipassback</i>)
	Interlock	Working (#) or Not working (blank)
	Priority	<i>Interlock</i> input priority: Lockdown or Override
	Tampered	Indicates whether a unit in the area has been tampered with. Yes (#) or No (blank)
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 (<i>IP cameras</i>)
	Blocked	Indicates if the camera is currently blocked from some users. Blocked (#), or not blocked (blank)
Doors	Entity	Door name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
	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 <i>federated entity</i> , shows the federation role name

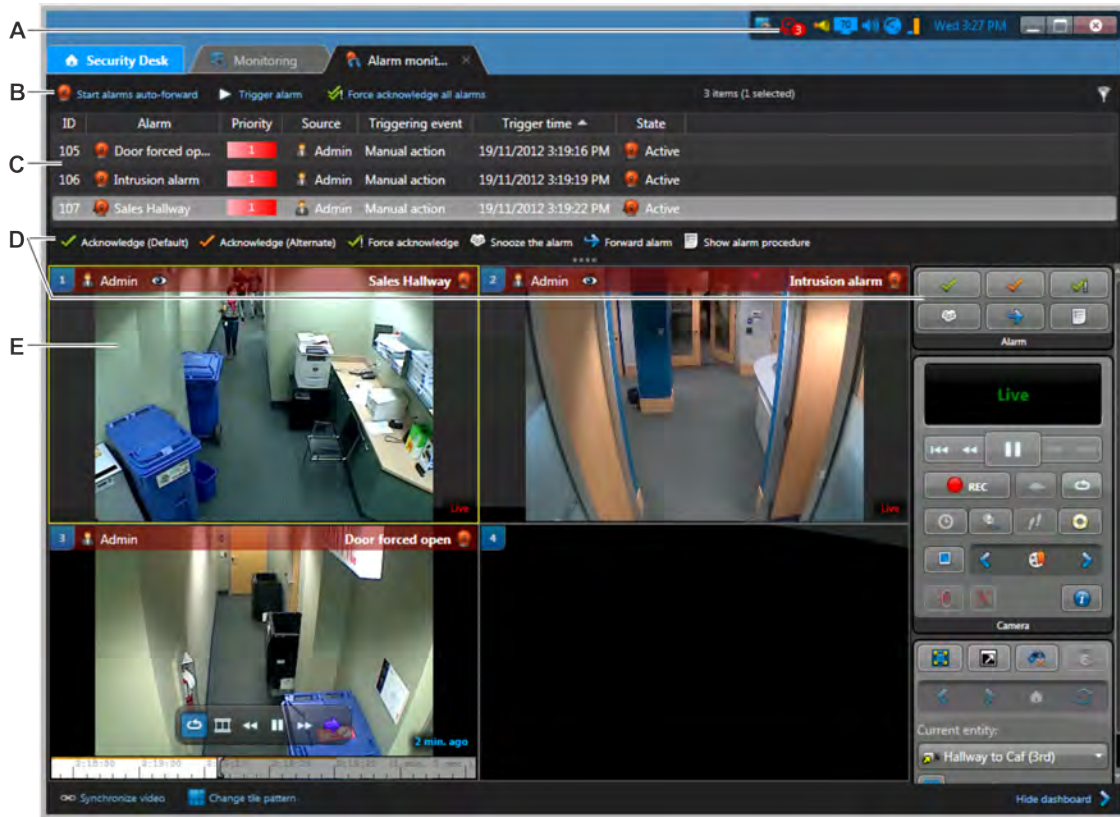
Entity	Columns	Description
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
Intrusion detection areas	Entity	Intrusion detection area name
	Entity path	List of all parent areas, starting from the system entity
	Health	Online, Offline, or Warning
	Arming state	<i>Master arm, Perimeter arm, Ready to arm, Arming, Disarmed, Disarmed (input trouble), or Armed (Alarm active)</i>
	Bypass	Active/inactive (represented by an icon)
	Alarm active	Active/inactive (represented by an icon)
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)
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

Entity	Columns	Description
	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 ()
Routes	Route	Route name, showing the two networks it joins
	Current configuration	<i>Unicast TCP, Unicast UDP, or Multicast</i>
	Detected capabilities	Unicast TCP, Unicast UDP, or Multicast NOTE: A <i>Redirector</i> is required on each network to be able to detect the capabilities.
	Status	OK, or warning message stating the reason of the problem NOTE: A <i>Redirector</i> is required on each network to be able to display the status.
Servers	Entity	Server name
	Health	Online, Offline, or Warning
	Roles	Roles assigned to this server
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

Overview of the Alarm monitoring task

Use the Alarm monitoring task to monitor and respond to *active alarms* in real time, as well as review past alarms.

The following figure shows the Alarm monitoring task.



A The alarm monitoring icon turns red when there is an active alarm. Double-click to open the Alarm monitoring task.

B Additional alarm commands.

- Start alarms auto-forward.
- Trigger alarm.
- (Administrators only) Force acknowledge all alarms.
- Set the alarm filter options.

C Current alarms are listed in the alarm list. To change the columns that are shown, right-click a column heading, and then click **Select columns**.

D Commands to control active alarms.

E Video of an alarm in a tile. The video is displayed with a red overlay with details of the alarm.

Related Topics

[Acknowledging alarms](#) on page 351

Overview of the Alarm report task

Use the Alarm report task to search for and investigate current and past alarms.

The following figure shows the Alarm report task.



- A Query filters.
- B [Export](#) or [print](#) the report.
- C The alarm report results are listed in the report pane.
- D (Only administrators) Forcibly acknowledge all active alarms.
- E Alarm widget.
- F Video of an alarm in a tile.
- G Run the report.

Related Topics

[Alarm widget](#) on page 31

[Investigating current and past alarms](#) on page 359

[How alarms are displayed in the Security Desk canvas](#) on page 348

Overview of the Enhanced cardholder access rights task

You can find out which cardholders and cardholder groups are currently granted or denied access to selected areas, doors, and elevators, using the *Enhanced cardholder access rights* report.

This report is helpful, because it allows you to see where a cardholder can go, and when, and determine if their access rule properties need to be adjusted. You can also use this report to find members of a cardholder group.

TIP: Perform your query on one cardholder or cardholder group at a time, so your report is more specific.

The screenshot shows the Security Desk interface with the following components:

- A:** Query filters on the left sidebar, including 'Doors - Areas - Elevators', 'Search', and a tree view of areas (Area 1, Area 2, Area 3, Dubai office, Montreal office, Paris office).
- B:** The report table with columns: Cardholder group, Cardholder, Area, Door side / Floor, Granted access by, and Denied access by. It shows 13 items selected.
- C:** The report table content, listing cardholders like Brandon Miller, Thomas Taylor, Michael Adams, Mike Gregor, and Miguel Castaneda.
- D:** Cardholder details for Mike Gregor and Michael Adams, including photos, names, email addresses, titles, hire dates, departments, office extensions, genders, home numbers, and cellphone numbers.
- E:** Cardholder details for Brandon Miller and Kathy Willson, including photos, names, email addresses, titles, hire dates, departments, office extensions, genders, home numbers, and cellphone numbers.
- F:** A green 'Generate report' button and a 'Query' button at the bottom left.

A Query filters.

- **Cardholder groups:** Restrict your search to specific cardholder groups.
- **Cardholders:** Restrict your search to specific cardholders.
- **Expand cardholder groups:** List the members of the selected cardholder groups in the report instead of the cardholder groups themselves.
- **Include perimeter entities:** Include the perimeter entities of the selected areas in the report.
- **Cardholder custom fields:** If custom fields are defined for the cardholders you are investigating, they can be included in this report.

B Export or print the report.

C All cardholders or cardholder groups that are granted or denied access at the selected areas and access points are listed in the report pane.

D View cardholder properties in a tile.

E  - View additional cardholder details.

D Run the report.

Related Topics

[How cardholders are displayed in the Security Desk canvas](#) on page 213

Enabling the Enhanced cardholder access rights task

To use the *Enhanced cardholder access rights* report, you must enable the report in Security Desk from the *SecurityDesk.plugins.xml* file.

To enable the Enhanced cardholder access rights task:

- 1 Open the *SecurityDesk.plugins.xml* file, located in *C:\Program files (x86)\Genetec Security Center 5.3* on a 64-bit computer, and in *C:\Program files\Genetec Security Center 5.3* on a 32-bit computer.
- 2 Set the **Genetec.AccessControl.Reporting.Casinos.dll** attribute to **true**.
Example: `<Assembly Name="Genetec.AccessControl.Reporting.Casinos.dll" Enabled="true" />`
- 3 Save the XML file, and then restart Security Desk.

The next time you open Security Desk, the *Enhanced cardholder access rights* task is available.

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 a type of role that manages and monitors access control units on the system.
access point	An access point is any entry (or exit) point to a physical area where access can be monitored and governed by access rules. An access point is typically a door side or an elevator floor.
access right	An access right is the basic right users must have over any part of the system before they can do anything with it. Other rights, such as viewing and modifying entity configurations, are granted through privileges. In the context of Synergis, an access right is the right granted to a cardholder to pass through an access point at a given date and time.
access rule	An access rule is a type of entity that defines a list of cardholders to whom access is either granted or denied based on a schedule. An access rule can be applied to a secured area or to an access point.
Access rule configuration	Access rule configuration is a type of maintenance task that reports on entities and access points affected by a given access rule.
Access troubleshooter	Access troubleshooter is a tool that helps you detect and diagnose access configuration problems. With this tool, you can find out about the following: <ul style="list-style-type: none">• 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 a type of role that is responsible for the discovery, status polling, and control of video units. An Archiver also manages the video archive, and performs motion detection when 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 <i>speaker</i> .
audio encoder	An audio encoder is a device or software that encodes audio streams using a compression algorithm. Synonym of <i>microphone</i> .
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 <i>broadcasts</i> a discovery request on a specific port, and the units listening on that port respond with a message that contains the connection information about themselves. The role then uses the information to configure the connection to the unit and enable communication.
AutoVu	AutoVu is the IP license plate recognition (LPR) system of Security Center that automates the reading and verification of vehicle license plates. AutoVu Sharp cameras capture license plate images, and send the data to Patroller or Security Center to verify against lists of vehicles of interest (hotlists) and vehicles with permits (permit lists). You can install AutoVu in a fixed configuration (e.g. on a pole in a parking lot), or in a mobile configuration (e.g. on a police car). You can use AutoVu for scofflaw and wanted vehicle identification, city-wide surveillance, parking enforcement, parking permit control, vehicle inventory, security, and access control.
AutoVu LPR Processing Unit	AutoVu LPR Processing Unit is the processing component of the SharpX system. The LPR Processing Unit is available with two or four camera ports, with one dedicated processor per camera (if using SharpX) or per two cameras (if using SharpX VGA). This ensures maximum, per-camera, processing performance. The LPR Processing Unit is sometimes referred to as the <i>trunk unit</i> because it is typically installed in a vehicle's trunk.

Auxiliary Archiver	Auxiliary Archiver is a type of role that supplements the video archive produced by the Archiver. Unlike the Archiver, the Auxiliary Archiver is not bound to any particular <i>discovery port</i> , 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 Genetec's proprietary connector box for AutoVu mobile solutions that use Sharp cameras. The breakout box provides power and network connectivity to the Sharp units and the in-vehicle computer.
broadcast	Broadcast is the communication between a single sender and all receivers on a network.
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) <i>digital certificate</i> ; (2) <i>SDK certificate</i> .
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 <i>City Parking Enforcement</i> 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 a component of the <i>fusion stream</i> . It is the <i>master key stream</i> that is encrypted with a <i>public key</i> . Only clients that own the corresponding <i>private key</i> can decrypt the master 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 Appliance 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 <i>identity certificate</i> or <i>encryption certificate</i> , 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 <i>main server</i> , and must be set up first. All other servers you add in Security Center are called <i>expansion servers</i> , 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 <i>In</i> and <i>Out</i> 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 <i>In</i> and <i>Out</i> 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 <i>digital certificate</i> or <i>public key certificate</i> , is an electronic document that contains a public and private key pair used in Security Center for <i>fusion stream encryption</i> . Information encrypted with the <i>public key</i> can only be decrypted with the matching <i>private key</i> .

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	Federation is the virtual system formed by joining multiple, independent Genetec IP security systems. Federation allows the users on your local system to view and control the entities belonging to independent remote systems, as if they were on your local system.
first-person-in rule	The first-person-in rule is the additional access restriction placed on a secured area that prevents anyone from entering the area until a

supervisor is on site. The restriction can be enforced when there is free access (on door unlock schedules) and when there is controlled access (on access rules).

Forensic search

Forensic search is a type of investigation task that searches for video sequences based on video analytics events.

four-port RS-485 module

A four-port RS-485 module is a RS-485 communication component of Synergis Master Controller with four ports (or channels) named A, B, C, and D. The number of interface modules you can connect to each channel depends on the type of hardware you have.

free access

A free access is an access point state where no credentials are necessary to enter a secured area. The door is unlocked. This is typically used during normal business hours, as a temporary measure during maintenance, or when the access control system is first powered up and is yet to be configured.

free exit

A free exit is an access point state where no credentials are necessary to leave a secured area. The person releases the door by turning the doorknob, or by pressing the REX button, and walks out. An automatic door closer shuts the door so it can be locked after being opened.

fusion stream

Fusion stream is Genetec's proprietary data structure for streaming multimedia. Each fusion stream is a bundle of data (video, audio, and metadata) streams and key streams related to a single camera. Fusion streams are created in response to specific client requests. The key streams are included only if the data streams are encrypted.

fusion stream encryption

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

G

G64

G64 is a Security Center format used by archiving roles (Archiver and Auxiliary Archiver) to store video sequences issued from a single camera. This data format supports audio, bookmarks, metadata overlays, timestamps, motion and event markers, and variable frame rate and resolution.

G64x

G64x is a Security Center format used to store video sequences from multiple cameras that are exported or backed up simultaneously. This data format supports audio, bookmarks, metadata overlays, timestamps, motion and event markers, variable frame rate and resolution, and watermarking.

Genetec Server

Genetec Server is the Windows service that is at the core of Security Center architecture, and that must be installed on every computer that is part of the Security Center's pool of servers. Every such server is a generic computing resource capable of taking on any role (set of functions) you assign to it.

Genetec Update Service	The Genetec Update Service is a web-based service that allows you to update your Security Center products when a new release becomes available.
Genetec Video Player	The Genetec Video Player is a media player that is used to view exported G64 and G64x video files from Security Desk, or on a computer that does not have Security Center installed.
geocoding	Geocoding is the process of finding associated geographic coordinates (latitude and longitude) from a street address.
Geographic information system	Geographic information system (GIS) is a system that captures spatial geographical data. Map Manager can connect to third-party vendors that provide GIS services in order to bring maps and all types of geographically referenced data to Security Center.
ghost camera	A ghost camera is an entity used as a substitute camera. This entity is automatically created by the Archiver when video archives are detected for a camera whose definition has been deleted from the Directory, either accidentally or because the physical device no longer exists. Ghost cameras cannot be configured, and only exist so users can reference the video archive that would otherwise not be associated to any camera.
ghost Patroller	A ghost Patroller is an entity automatically created by the LPR Manager when the AutoVu license includes the XML Import module. In Security Center, all LPR data must be associated to a Patroller entity or an LPR unit corresponding to a fixed Sharp camera. When you import LPR data from an external source via a specific LPR Manager using the XML Import module, the system uses the ghost entity to represent the LPR data source. You can formulate queries using the ghost entity as you would with a normal entity.
global antipassback	Global antipassback is a feature that extends the antipassback restrictions to areas controlled by multiple Synergis units.
Global Cardholder Synchronizer	Global Cardholder Synchronizer is a type of role that ensures the two-way synchronization of shared cardholders and their related entities between the local system (sharing participant) and the central system (sharing host).
global entity	A global entity is an entity that is shared across multiple independent Security Center systems by virtue of its membership to a global partition. Only cardholders, cardholder groups, credentials, and badge templates are eligible for sharing.
global partition	Global partition is a partition that is shared across multiple independent Security Center systems by the partition owner, called the sharing host.
H	
hardware integration package	A hardware integration package, or HIP, is an update that can be applied to Security Center. It enables the management of new functionalities (for

example, new video unit types), without requiring an upgrade to the next Security Center release.

Hardware inventory	Hardware inventory is a type of maintenance task that reports on the characteristics (unit model, firmware version, IP address, time zone, and so on) of access control, video, intrusion detection, and LPR units in your system.
hardware zone	A hardware zone is a zone entity in which the I/O linking is executed by a single access control unit. A hardware zone works independently of the Access Manager, and consequently, cannot be armed or disarmed from Security Desk.
Health history	Health history is a type of maintenance task that reports on health issues.
Health Monitor	Health Monitor is the central role that monitors system entities such as servers, roles, units, and client applications for health issues.
Health statistics	Health statistics is a type of maintenance task that gives you an overall view of the health of your system.
High availability	High availability is a design approach that enables a system to perform at a higher than normal operational level. This often involves failover and load balancing.
hit	A hit is a license plate read that matches a hit rule, such as a hotlist, overtime rule, permit, or permit restriction. A Patroller user can choose to reject or accept a hit. An accepted hit can subsequently be enforced.
hit rule	Hit rule is a type of LPR rule used to identify vehicles of interest (called "hits") using license plate reads. The hit rules include the following types: hotlist, overtime rule, permit, and permit restriction.
Hits	Hits is a type of investigation task that reports on hits reported within a selected time range and geographic area.
hot action	A hot action is an action mapped to a PC keyboard function key (Ctrl+F1 through Ctrl+F12) in Security Desk for quick access.
hotlist	A hotlist is a type of entity that defines a list of wanted vehicles, where each vehicle is identified by a license plate number, the issuing state, and the reason why the vehicle is wanted (stolen, wanted felon, Amber alert, VIP, and so on). Optional vehicle information might include the model, the color, and the vehicle identification number (VIN).
Hotlist and permit editor	Hotlist and permit editor is a type of operation task used to edit an existing hotlist or permit list. A new list cannot be created with this task, but after an existing list has been added to Security Center, users can edit, add, or delete items from the list, and the original text file is updated with the changes.
hotspot	Hotspot is a type of map object that represents an area on the map which requires special attention. Clicking on a hotspot displays associated fixed and PTZ cameras.

I

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 <i>digital certificate</i> or <i>public key certificate</i> , 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 <i>public key</i> 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. The supported identity providers for Stratocast accounts are Google, Microsoft (Windows Live ID), and Yahoo!
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.
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 <i>intrusion panels</i> (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 <i>System ID</i> (which identifies your system) and the <i>Validation key</i> (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 <i>long term</i> regulation uses the same principle as the <i>same position</i> regulation, but the parking period is over 24 hours. No more than one overtime rule may use the long term regulation in the entire system.

LPR	The LPR task is a type of administration task that allows you to configure LPR roles, units, hotlists, permits, overtime rules, and related entities and settings.
LPR camera	A LPR camera is a camera connected to an LPR unit that produces high resolution close-up images of license plates.
LPR Manager	LPR Manager is a type of role that manages and controls Patrollers and fixed Sharp units. The LPR Manager stores the data (reads, hits, GPS data, and so on) collected by the LPR units and Patrollers into a central database for reporting. The LPR Manager is also responsible for updating fixed Sharps and Patrollers in the field with hotfixes, hotlist updates, and so on.
LPR rule	LPR rule is a method used by Security Center and AutoVu for processing a license plate read. An LPR rule can be a hit rule or a parking facility.
LPR unit	A LPR unit is a type of entity that represents a hardware device dedicated to the capture of license plate numbers. An LPR unit is typically connected to an LPR camera and a context camera. These cameras can be incorporated to the unit or external to the unit.
M	
macro	A macro is a type of entity that encapsulates a C# program that adds custom functionalities to Security Center.
main server	Main server is the only server in a Security Center system hosting the Directory role. All other servers on the system must connect to the main server in order to be part of the same system. In an high availability configuration where multiple servers host the Directory role, it is the only server that can write to the Directory database.
man-in-the-middle	In computer security, man-in-the-middle (MITM) is a form of attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
manual capture	Manual capture is when license plate information is entered into the system by the user and not by the LPR.
manufacturer extension	Manufacturer extension is the manufacturer specific settings for access control units, video units, and intrusion detection units.
map	A map in Security Center is a two-dimensional diagram that helps you visualize the physical locations of your security equipment in a geographical area or a building space.
Map designer	Map designer is a type of administration task that allows you to create and edit maps that represent the physical locations of your equipment to Security Desk users.
map link	A map link is a map object that brings you to another map with a single click.

Map Manager	Map Manager is the central role that manages all mapping resources in Security Center, including imported map files, external map providers, and KML objects. It acts as the map server to all client applications that require maps.
map mode	Map mode is a Security Desk canvas operating mode where the main area of the canvas is used to display a geographical map, for the exclusive purpose of showing LPR events.
map object	Map objects are graphical representations of Security Center entities on your maps. They allow you to interact with your system without leaving your map.
map view	A map view is a defined display position and zoom level for a given map.
Maps	Maps is a type of operation task that heightens your situational awareness by providing the context of a map to your security monitoring and control activities.
master arm	Arming an intrusion detection area in such a way that all sensors attributed to the area would set the alarm off if one of them is triggered.
master key stream	In <i>fusion stream</i> encryption, each data stream is encrypted with a series of symmetric keys called <i>master key stream</i> . The symmetric keys are randomly generated by the Archiver 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 <i>Decision Support System</i> that provides organizations with a unified security platform that offers superior situational intelligence, visualization, and complete incident management capabilities. Mission Control guides operators through the incident monitoring and resolution process, allowing them to take control of undesirable situations, removing emotion from the response and ensuring compliance.

Mobile Admin	Mobile Admin is a web-based administration tool used to configure the Mobile Server.
Mobile app	Mobile app is the client component of Security Center Mobile installed on mobile devices. Mobile app users connect to Mobile Server to receive alarms, view live video streams, view the status of doors, and more, from Security Center.
Mobile Data Computer	Mobile Data Computer is a tablet computer or ruggedized laptop used in patrol vehicles to run the AutoVu Patroller application. The MDC is typically equipped with a touch-screen with a minimum resolution of 800 x 600 pixels and wireless networking capability.
Mobile License Plate Inventory	Mobile License Plate Inventory is the Patroller software installation that is configured for collecting license plates and other vehicle information for creating and maintaining a license plate inventory for a large parking area or parking garage.
Mobile Server	Mobile Server is the server component of Security Center Mobile that connects Mobile apps and Web Clients to Security Center. The Mobile Server connects to Security Center, and synchronizes the data and video between Security Center and supported Mobile client components.
monitor group	A monitor group is a type of entity used to designate analog monitors for alarm display. Besides the monitor groups, the only other way to display alarms in real time is to use the Alarm monitoring task in Security Desk.
monitor ID	Monitor ID is an ID used to uniquely identify a workstation screen controlled by Security Desk.
Monitoring	Monitoring is a type of operation task that allows you to monitor and respond to alarms and real time events pertaining to selected entities of interest.
motion detection	Motion detection is the feature that watches for changes in a series of video images. The definition of what constitutes motion in a video can be based on highly sophisticated criteria.
Motion search	Motion search is a type of investigation task that searches for motion detected in specific areas of a camera's field of view.
motion zone	A motion zone is a user defined areas within a video image where motion should be detected.
Move unit	Move unit tool is used to move units from one manager role to another. The move preserves all unit configurations and data. After the move, the new manager immediately takes on the command and control function of the unit, while the old manager continues to manage the unit data collected before the move.
multifactor authentication	Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

N

Navigator box	The Navigator box is Genetec's proprietary in-vehicle device that provides GPS coordinates and odometer readings to Patroller. Because it taps into the vehicle's odometry signal, it is more accurate than a standard GPS device. The Navigator box can be used with any type of AutoVu mobile deployment that requires positioning information, but it is required for City Parking Enforcement with Wheel Imaging.
network	The network entity is used to capture the characteristics of the networks used by your system so that proper stream routing decisions can be made.
network address translation	Network address translation is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device, for the purpose of remapping one IP address space into another.
network view	The network view is a browser view that illustrates your network environment by showing each server under the network they belong to.
Network view	The Network view task is a type of administration task that allows you to configure your networks and servers.
new wanted	A new wanted is a manually entered hotlist item in Patroller. When you are looking for a plate that does not appear in the hotlists loaded in the Patroller, you can enter the plate in order to raise a hit if the plate is captured.
notification tray	The notification tray contains icons that allow quick access to certain system features, and also displays indicators for system events and status information. The notification tray display settings are saved as part of your user profile and apply to both Security Desk and Config Tool.
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	Omnicast Federation is a type of role that connects an Omnicast 4.x system to Security Center and imports its entities, so that its cameras and events can be used in your local system.
output behavior	An output behavior is a type of entity that defines a custom output signal format, such as a pulse with a delay and duration.
overtime rule	An overtime rule is a type of entity that defines a parking time limit and the maximum number of violations enforceable within a single day. Overtime rules are used in city and university parking enforcement. For university parking, an overtime rule also defines the parking zone where these restrictions apply.
P	
parking facility	A parking facility is a type of entity that defines a large parking area as a number of sectors and rows for the purpose of inventory tracking.
parking lot	A parking lot is a polygon that defines the location and shape of a parking area on a map. By defining the number of parking spaces inside the parking lot, Security Center can calculate its percentage of occupancy during a given time period.
parking zone	Parking zone is the general concept used to designate the area where a given parking regulation (overtime rule, permit, or permit restriction) is enforced. When used in the context of university parking enforcement, the parking zone must be explicitly defined as a list of parking lots.
partition	A partition is a type of entity that defines a set of entities that are only visible to a specific group of users. For example, a partition could include all areas, doors, cameras, and zones in one building.
partition administrator	A partition administrator is an authorized user of a partition who has full administrative rights over that partition and its members. Partition administrators can add, modify, and delete all entities within their partitions, including roles, users, user groups, and child partitions.
Patroller	<ol style="list-style-type: none"> 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 <i>asymmetric encryption</i> , 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 <code>genetec.com</code> , or a path within that domain, such as <code>genetec.com/support/GTAC</code> . 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: <ul style="list-style-type: none">• 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: <i>Enabled</i> , <i>Disabled</i> , <i>Currently recording (unlocked)</i> , and <i>Currently recording (locked)</i> .
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.

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	Security Center Federation is a type of role that connects a remote, independent Security Center system to your local Security Center, so that its entities and events can be used by your local Security Desk users.
Security Center Mobile	Security Center Mobile is a feature of Genetec's unified platform that lets you remotely connect to your Security Center system over a wireless IP network. Supported Mobile client components include a platform-independent, unified Web Client, as well as various Mobile apps for smartphones and tablets.
security clearance	A security clearance is a numerical value used to further restrict the access to an area when a threat level is in effect. Cardholders can only access (enter or exit) an area if their security clearance is equal or higher than the minimum security clearance set on the area.
Security Desk	Security Desk is the unified user interface of Security Center. It provides consistent operator flow across all of the Security Center's main systems, Omnicast, Synergis, and AutoVu. Security Desk's unique task-based design lets operators efficiently control and monitor multiple security and public safety applications.
security token	An on-the-wire representation of claims that is cryptographically signed by the issuer of the claims, providing strong proof to any relying party as to the integrity of the claims and the identity of the issuer.
security token service	Secure token service (STS) is a claims provider implemented as a web service that issues security tokens. Active Directory Federation Services (ADFS) is an example of a security token service. Also known as an issuer.
self-signed certificate	A self-signed certificate is an identity certificate that is signed by the same entity whose identity it certifies.
server	A server is a type of entity that represents a server machine on which Genetec Server is installed.
server mode	The server mode is a special online operation mode restricted to Synergis units, in which the unit allows the Access Manager (the server) to make all access control decisions. The unit must stay connected to the Access Manager at all times to operate in this mode.
Server Admin	Server Admin is the web application running on every server machine in Security Center that allows you to configure the settings of Genetec Server. Server Admin also allows you to configure the Directory role on the main server.
sharing guest	Sharing guest is when Security Center system gives the rights to view and modify entities shared by another system.
sharing host	Sharing host is when Security Center system owns partitions that are shared with other Security Center systems.

Sharp EX	Sharp EX is the Sharp unit that includes an integrated image processor and supports two standard definition NTSC or PAL inputs for external cameras (LPR and context cameras).
SharpOS	SharpOS is the software component of a Sharp or SharpX unit. SharpOS is responsible for everything related to plate capture, collection, processing, and analytics. For example, a SharpOS update may include new LPR contexts, new firmware, Sharp Portal updates, and updates to the Sharp's Windows services (Plate Reader, HAL, updater service, and so on).
Sharp Portal	Sharp Portal is a web-based administration tool used to configure Sharp cameras for fixed or mobile AutoVu systems. From a web browser, you log on to a specific IP address (or the Sharp name in certain cases) that corresponds to the Sharp you want to configure. When you log on, you can configure options such as selecting the LPR context (e.g. Alabama, Oregon, Quebec, etc), selecting the read strategy (e.g. fast moving or slow moving vehicles), viewing the Sharp's live video feed, and more.
Sharp unit	Sharp unit is Genetec's proprietary LPR unit that integrates license plate capturing and processing components, as well as digital video processing functions, inside a ruggedized casing.
Sharp VGA	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 Dell™ PowerEdge™ R320 server that comes preloaded with Genetec security software, and Windows Embedded Standard 7. The SV-PRO is for small to mid-scale, single or multiple server installations, and can support both cameras and access control readers.

symmetric encryption

Symmetric encryption is a type of encryption where the same key is used for both encryption and decryption.

synchronous video

A synchronous video is a simultaneous live video or playback video from more than one camera that are synchronized in time.

Synergis

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

Synergis appliance

A Synergis appliance is an IP-ready security appliance manufactured by Genetec that is dedicated to access control functions. All Synergis

appliances come preinstalled with Synergis Softwire and can be enrolled as access control units in Security Center.

Synergis Appliance Portal

Synergis Appliance Portal is the web-based administration tool used to configure and administer the Synergis appliance, as well as upgrade its firmware.

Synergis Cloud Link

Synergis Cloud Link is Genetec's intelligent and PoE-enabled access control appliance that supports a variety of third-party interface modules over IP and RS-485. Synergis Cloud Link is seamlessly integrated with Security Center and is capable of making access control decisions independently of the Access Manager.

Synergis Master Controller

Synergis Master Controller (SMC) is Genetec's access control appliance that supports a variety of third-party interface modules over IP and RS-485. SMC is seamlessly integrated with Security Center and is capable of making access control decisions independently of the Access Manager.

Synergis Softwire

Synergis Softwire is the access control software developed by Genetec to run on a variety of IP-ready security appliances. Synergis Softwire lets these appliances communicate with third-party interface modules. A security appliance running Synergis Softwire can be enrolled as an access control unit in Security Center.

Synergis unit

A Synergis unit is a Synergis appliance that is enrolled as an access control unit in Security Center.

System

The System task is an administration task that allows you to configure roles, macros, schedules, and other system entities and settings.

system event

A system event is a predefined event that indicates the occurrence of an activity or incident. System events are defined by the system and cannot be renamed or deleted.

System status

System status is a type of maintenance task that monitors the status of all entities of a given type in real time, and allows you to interact with them.

T

tailgating

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

task

A task is the central concept on which the entire Security Center user interface is built. Each task corresponds to one aspect of your work as a security professional. For example, use a monitoring task to monitor system events in real-time, use an investigation task to discover suspicious activity patterns, or use an administration task to configure your system. All tasks can be customized and multiple tasks can be carried out simultaneously.

taskbar

A taskbar is a user interface element of the Security Center client application window, composed of the Home tab and the active task list.

	<p>The taskbar can be configured to appear on any edge of the application window.</p>
task cycling	<p>A task cycling is a Security Desk feature that automatically cycles through all tasks in the active task list following a fixed dwell time.</p>
task workspace	<p>A task workspace is an area in the Security Center client application window reserved for the current task. The workspace is typically divided into the following panes: canvas, report pane, dashboard, and Logical view.</p>
threat level	<p>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.</p>
tile	<p>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.</p>
tile ID	<p>The tile ID is the number displayed at the upper left corner of the tile. This number uniquely identifies each tile within the canvas.</p>
tile mode	<p>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.</p>
tile pattern	<p>The tile pattern is the arrangement of tiles within the canvas.</p>
tile plugin	<p>A tile plugin is a type of entity that represents an application that runs inside a Security Desk tile.</p>
Time and attendance	<p>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.</p>
timed antipassback	<p>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 <i>Presence timeout</i>. When the time delay has expired, the cardholder can once again pass into the area without generating a passback event.</p>
timeline	<p>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.</p>
transfer group	<p>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.</p>
Transmission Control Protocol	<p>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</p>

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

Unit replacement

Unit replacement is a tool that is used to replace a failed hardware device with a compatible one, while ensuring that the data associated to the old unit gets transferred to the new one. For an access control unit, the configuration of the old unit is copied to the new unit. For a video unit, the video archive associated to the old unit is now associated to the new unit, but the unit configuration is not copied.

unit synchronization

Unit synchronization is the process of downloading the latest Security Center settings to an access control unit. These settings, such as access rules, cardholders, credentials, unlock schedules, and so on, are required so that the unit can make accurate and autonomous decisions in the absence of the Access Manager.

University Parking Enforcement	University Parking Enforcement is a Patroller software installation that is configured for university parking enforcement: the enforcement of scheduled parking permits or overtime restrictions. The use of maps is mandatory. Hotlist functionality is also included.
unlock schedule	An unlock schedule defines the periods of time when free access is granted through an access point (door side or elevator floor).
unreconciled read	A unreconciled read is a MLPI license plate read that has not been committed to an inventory.
user	A user is a type of entity that identifies a person who uses Security Center applications and defines the rights and privileges that person has on the system. Users can be created manually or imported from an Active Directory.
user group	A user group is a type of entity that defines a group of users who share common properties and privileges. By becoming member of a group, a user automatically inherits all the properties of the group. A user can be a member of multiple user groups. User groups can also be nested.
user level	A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera PTZ, viewing the video feed from a camera, or to stay logged on when a threat level is set. The smaller the value, the higher the priority.
User management	The User management task is a type of administration task that allows you to configure users, user groups, and partitions.
V	
validation key	A validation key is a serial number uniquely identifying a computer that must be provided to obtain the license key.
Vault	Vault is a tool that displays your saved snapshots and exported G64, G64x, and GEK (encrypted) video files. From the Vault you can view the video files, encrypt and decrypt files, convert files to ASF, or package files with the Genetec Video Player.
vehicle identification number	A vehicle identification number (VIN) is an identification number that a manufacturer assigns to vehicles. This is usually visible from outside the vehicle as a small plate on the dashboard. A VIN can be included as additional information with license plate entries in a hotlist or permit list, to further validate a hit and ensure that it is the correct vehicle.
video analytics	Video analytics is the software technology that is used to analyze video for specific information about its content. Examples of video analytics include counting the number of people going through a door, license plate recognition, detection of unattended objects, or the direction of people walking or running.

video archive	Video archive includes both the recorded audio and video footage and the database that documents those recordings (source camera, timestamps, events, bookmarks, and so on).
video decoder	A video decoder is a device that converts a digital video stream into analog signals (NTSC or PAL) for display on an analog monitor. The video decoder is one of the many devices found on a video decoding unit.
video encoder	A video encoder is a device that converts an analog video source to a digital format, by using a standard compression algorithm, such as H.264, MPEG-4, MPEG-2, or M-JPEG. The video encoder is one of the many devices found on a video encoding unit.
video file	A video file is a file created by an archiving role (Archiver or Auxiliary Archiver) to store archived video. The file extension is G64 or G64x. You need Security Desk or the Genetec Video Player to view video files.
Video file explorer	Video file explorer is a type of investigation task that browses through your file system for video files (G64 and G64x) and allows you to play, convert to ASF, and verify the authenticity of these files.
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 Genetec™ customer, you have access to the Genetec™ Technical Information Site, where you can find information and search for answers to your product questions.

- **Genetec™ Technical Information Site:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

Before contacting GTAC or opening a support case, it is recommended to search the Technical Information Site for potential fixes, workarounds, or known issues.

To access the Technical Information Site, log on to [Genetec™ Portal](#) and click [Technical Information](#). Can't find what you're looking for? Contact documentation@genetec.com.

- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: [EN_GLM_ASSURANCE](#) and [EN_GLM_ADVANTAGE](#).

Additional resources

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

- **Forum:** The Forum is an easy-to-use message board that allows clients and Genetec™ staff to communicate with each other and discuss a variety of topics, ranging from technical questions to technology tips. You can log in or sign up at <https://gtapforum.genetec.com>.
- **Technical training:** In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to <http://www.genetec.com/support/training/training-calendar>.

Licensing

- For license activations or resets, please contact GTAC at <https://gtap.genetec.com>.
- For issues with license content or part numbers, or concerns about an order, please contact Genetec™ Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, please contact Genetec™ Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Please contact GTAC at <https://gtap.genetec.com> to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.