



# Security Desk Getting Started Guide 5.10

Document last updated: October 5, 2021

# Legal notices

---

©2021 Genetec Inc. All rights reserved.

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

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

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

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

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein.

Genetec™, AutoVu™, AutoVu MLC™, Citywise™, Community Connect™, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™, KiwiSecurity™, Omnicast™, Privacy Protector™, Sipelia™, Stratocast™, Streamvault™, Synergis™, Valcri™, their respective logos, as well as the Mobius Strip 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.

Patent pending. Genetec™ Security Center, Omnicast™, AutoVu™, Stratocast™, Genetec Citigraf™, Genetec Clearance™, and other Genetec™ products are the subject of pending patent applications, and may be the subject of issued patents, in the United States and in other jurisdictions worldwide.

All specifications are subject to change without notice.

## Document information

Document title: Security Desk Getting Started Guide 5.10

Original document number: EN.500.060-V5.10.2.0(1)

Document number: EN.500.060-V5.10.2.0(1)

Document update date: October 5, 2021

You can send your comments, corrections, and suggestions about this guide to [documentation@genetec.com](mailto:documentation@genetec.com).

# About this guide

---

This guide is for new users to Security Desk. It uses real-world scenarios to show you how to use the basic product features. You'll get a tour of the user interface, and then learn how to log on and off, view a camera, search for and export video, and manage alarms.

## 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:** Content in this guide that references information found on third-party websites was accurate at the time of publication, however, this information is subject to change without prior notice from Genetec Inc.

# Contents

---

## Preface

Legal notices . . . . .	ii
About this guide . . . . .	iii

## Chapter 1: Security Desk basics

About Security Desk . . . . .	2
Logging on to Security Center through Security Desk . . . . .	3
Home page overview . . . . .	7
UI component overview . . . . .	9
About the area view . . . . .	10
Searching for entities . . . . .	12
Searching for entities using the search tool . . . . .	12
Opening tasks . . . . .	14
Monitoring in Security Desk . . . . .	15
Monitoring task overview . . . . .	16
Reporting task workspace overview . . . . .	17
How to generate reports in Security Desk . . . . .	19

## Chapter 2: Canvas

About tiles . . . . .	22
Viewing entities in the canvas . . . . .	24
Unpacking content in tiles . . . . .	25
Changing tile patterns . . . . .	27
Default keyboard shortcuts . . . . .	28

## Chapter 3: Monitoring cameras

On-tile video controls . . . . .	35
Camera widget . . . . .	36
PTZ widget . . . . .	40
Zooming in and out of video . . . . .	42
Taking snapshots of video . . . . .	43
Editing video snapshots . . . . .	44
Adding bookmarks to video sequences . . . . .	45
Viewing bookmarked videos . . . . .	46
Report pane columns for the Bookmarks task . . . . .	46
Live and playback video modes . . . . .	47
Switching between video modes . . . . .	49
About the video timeline . . . . .	51
Performing targeted video searches . . . . .	52
Viewing video archives . . . . .	54
Video export formats . . . . .	57
Exporting video in G64x format . . . . .	58
Exporting video in G64, ASF, and MP4 formats . . . . .	63
The Export video dialog box . . . . .	66
Viewing exported video files . . . . .	68

Viewing exported files in the Video file explorer . . . . .	69
Sharing exported video files . . . . .	71
<b>Chapter 4: Monitoring access control entities</b>	
How access events are displayed in tiles . . . . .	73
Door widget . . . . .	74
Searching for cardholders and visitors using their credential . . . . .	75
Creating cardholders . . . . .	76
Assigning access rules to cardholders . . . . .	77
Assigning temporary access rules to cardholders . . . . .	79
Checking in new visitors . . . . .	80
Checking in returning visitors . . . . .	82
Checking out visitors . . . . .	83
Assigning credentials . . . . .	84
Requesting credential cards . . . . .	88
Printing credential cards in batches . . . . .	88
Printing paper credentials . . . . .	89
Assigning temporary cards . . . . .	90
Restoring original cards to cardholders and visitors . . . . .	90
Viewing properties of cardholder group members . . . . .	92
Viewing credential properties of cardholders . . . . .	93
Investigating visitor events . . . . .	94
Allowing access through doors . . . . .	96
Investigating door events . . . . .	98
<b>Chapter 5: Monitoring alarms</b>	
About alarms . . . . .	100
How alarms are displayed in the Security Desk canvas . . . . .	102
Alarm widget . . . . .	103
Enabling alarm monitoring in the Monitoring task . . . . .	105
Acknowledging alarms . . . . .	107
Filtering and grouping alarms in Security Center . . . . .	109
Forwarding alarms to other users automatically . . . . .	112
Forwarding alarms to other users manually . . . . .	113
Triggering alarms manually . . . . .	114
Investigating current and past alarms . . . . .	115
Overview of the Alarm monitoring task . . . . .	117
Overview of the Alarm report task . . . . .	118
Glossary . . . . .	119
Where to find product information . . . . .	144
Technical support . . . . .	145

# Security Desk basics

This section includes the following topics:

- ["About Security Desk"](#) on page 2
- ["Logging on to Security Center through Security Desk"](#) on page 3
- ["Home page overview"](#) on page 7
- ["UI component overview"](#) on page 9
- ["About the area view"](#) on page 10
- ["Searching for entities"](#) on page 12
- ["Opening tasks"](#) on page 14
- ["Monitoring in Security Desk"](#) on page 15
- ["Reporting task workspace overview"](#) on page 17
- ["How to generate reports in Security Desk"](#) on page 19

# About Security Desk

Security Desk is the unified user interface of Security Center. It provides consistent operator flow across all of the Security Center main systems, Omnicast™, Synergis™, and AutoVu™. The unique task-based design of Security Desk lets operators efficiently control and monitor multiple security and public safety applications.

In 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.

The screenshot displays the Security Desk Monitoring interface. At the top, there's a navigation bar with 'Security Desk' and 'Monitoring' tabs. Below this is a table with 26 items, showing event details such as 'Access denied: No access rule assigned' and 'Access granted' for 'Back door (A)'. The table columns include Event, Description, Event timestamp, Source, and Picture. Below the table is a search tree on the left showing a hierarchy of locations like 'Dubai office', 'Montreal office', and '4th Floor'. The main area features a 2x2 grid of video tiles. The top-left tile shows 'Access denied: No access rule assigned' with a video feed and a person's photo. The top-right tile shows 'Back door' with 'Door locked' status. The bottom-left tile shows 'Back door (A)' with 'Access granted' status. The bottom-right tile shows 'Back door (A)' with 'Access granted' status. On the right side, there are control panels for 'Door' (Closed/Locked) and 'Camera' (Live/Record). At the bottom, there are various utility buttons like 'Hide logical view', 'Monitored entities (2)', 'Synchronize video', 'Change tile pattern', 'Clear all', 'Open the Vault', 'Switch to map mode', and 'Hide dashboard'.

# Logging on to Security Center through Security Desk

---

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

## Before you begin

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

## What you should know

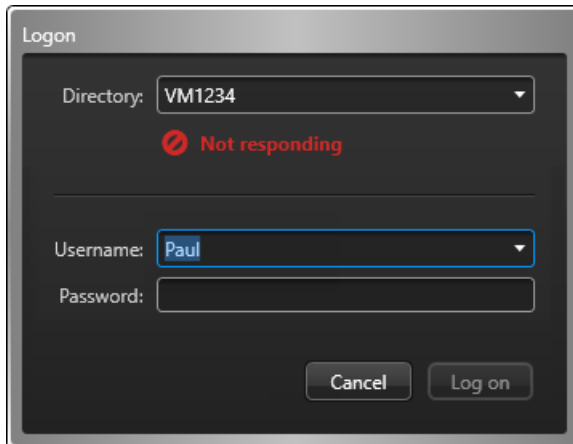
After you are logged on, you can log off and disconnect from the Directory without closing Security Desk. Logging off without closing the application is helpful if you plan to log on again using a different username and password.

### To log on to Security Center:

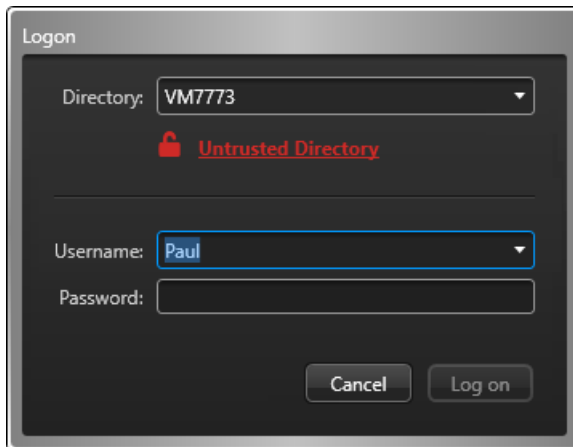
- 1 Open Security Desk.
  - a) Up to Windows 8, click **Start > All programs > Genetec Security Center 5.10 > Security Desk**
  - b) In Windows 10, click **Start > Genetec Security Center 5.10 > Security Desk**



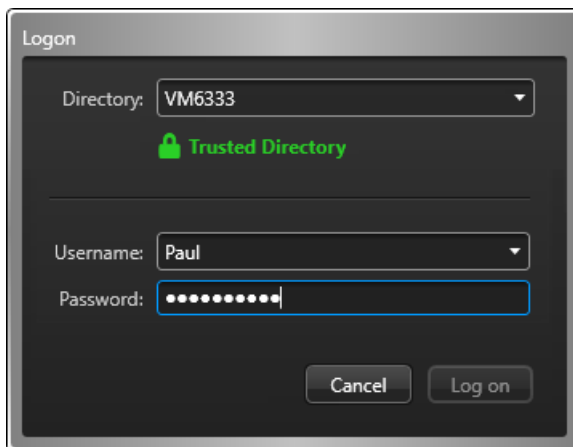
- In the *Logon* dialog box, enter the name of the **Directory**.  
If the Directory is not responding, check the spelling or contact your administrator.



If the Directory is not trusted, it could be the sign of a man-in-the-middle attack. Do not proceed unless your administrator confirms that it is safe to do so.



- Enter your Security Center username and password.



If single sign-on is deployed, you must click the **Sign in** button for your *identity provider*, or append your domain name to the end of your username, such as Username@DomainName. You will then be redirected to your identity provider for authentication.

- 4 To log on using your Windows user account, select **Use Windows credentials**. This option is only available if Active Directory is set up on your system.

The screenshot shows a 'Logon' dialog box with a dark background. At the top, it says 'Logon'. Below that is a 'Directory:' dropdown menu with 'VM6333' selected. Underneath is a green padlock icon and the text 'Trusted Directory'. The 'Username:' field contains 'GENETEC\pblart' and the 'Password:' field is filled with asterisks. A checkbox labeled 'Use Windows credentials' is checked. At the bottom, there are 'Cancel' and 'Log on' buttons.

- 5 Click **Log on**.
- 6 If you are required to log on with supervision, your supervisor must provide a username and password.

The screenshot shows the same 'Logon' dialog box. The 'Directory:' dropdown is still 'VM6333'. The 'Username:' dropdown now shows 'Paul'. The 'Password:' field is filled with asterisks. The 'Use Windows credentials' checkbox is now unchecked. Below these fields, there are 'Supervisor:' and 'Password:' fields, both containing asterisks. A message box at the bottom says 'Supervisor logon is required.' with a blue plus icon. 'Cancel' and 'Log on' buttons are at the bottom.

- 7 Click **Log on**.  
Security Desk opens.
- NOTE:** After a period of inactivity you might be locked out of Security Desk. You will have to re-enter your credentials to use the application again.
- 8 To log off, click the home (🏠) tab, and then click **Log off**.  
By default, you are asked to save your workspace when you log off Security Desk. You can change this behavior in the User Interaction section of the *Options* dialog box.

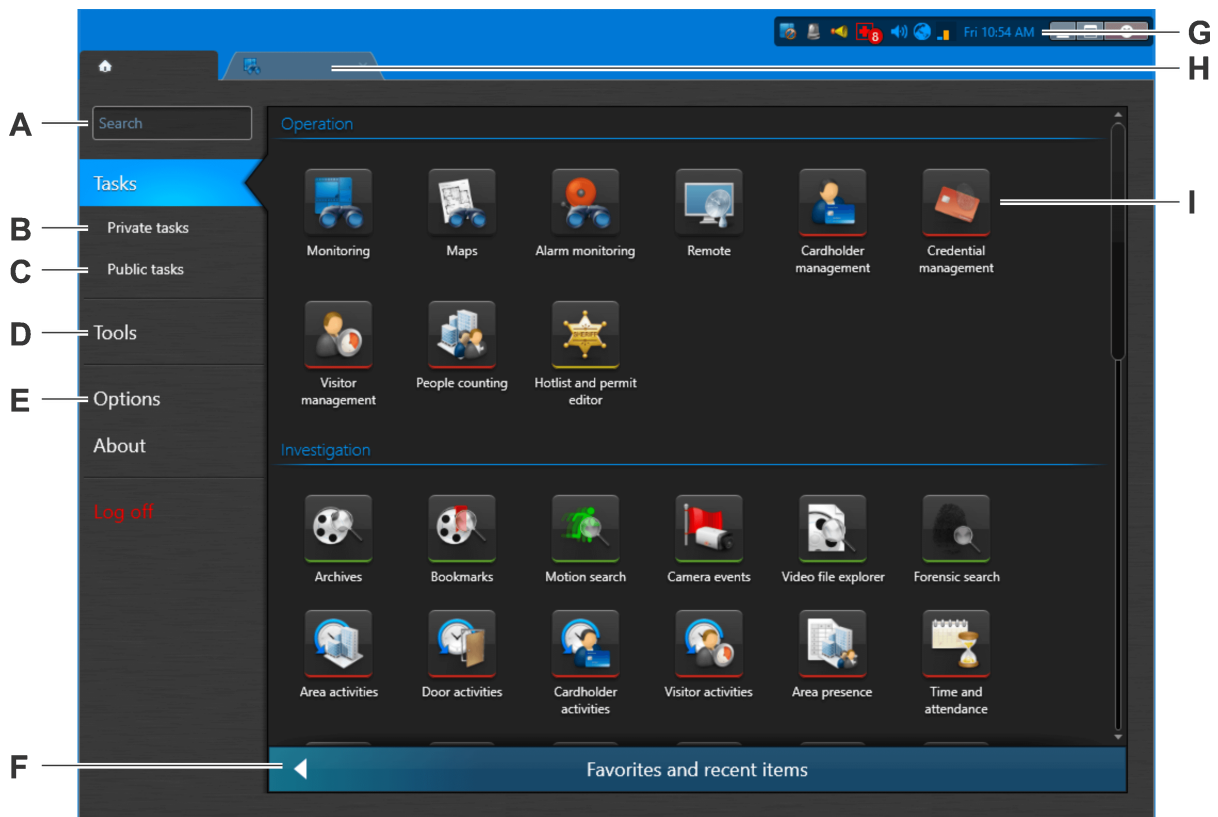
## Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.



# Home page overview

The home page is the main page in Security Center. Open the home page by clicking the home tab (🏠).



<b>A</b>	<b>Search box</b>	Type the name of the task you are looking for. All tasks containing that text in their category, name, or description, are shown.
<b>B</b>	<b>Private tasks</b>	Lists the saved tasks that you created and are only visible to your user.
<b>C</b>	<b>Public tasks</b>	Lists the saved tasks shared among multiple Security Center users.
<b>D</b>	<b>Tools</b>	Lists the standard Security Center tools, external tools, and applications you can start from your home page.
<b>E</b>	<b>Options</b>	Click to configure the options for your application.
<b>F</b>	<b>Favorites and Recent items</b>	Lists the tasks and tools you have used recently or added to your <b>Favorites</b> .
<b>G</b>	<b>Notification tray</b>	Displays important information about your system. Hover mouse over an icon to view system information, double-click to perform an action.
<b>H</b>	<b>Task tabs</b>	Shows the tasks you have open in individual tabs. Click to switch tasks.
<b>I</b>	<b>Tasks page</b>	Lists all tasks available to you. Select a task to open. If you have multiple instances of the task, you are asked to type a name.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.

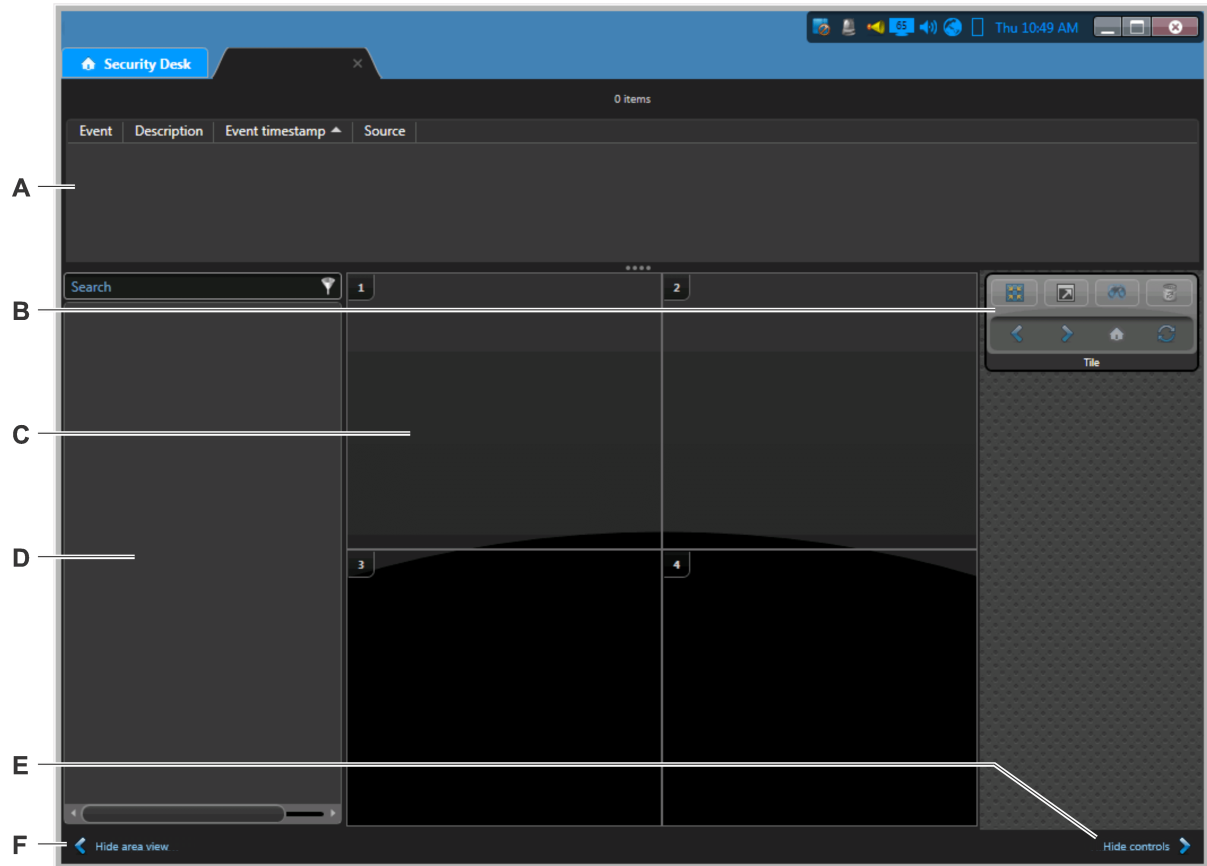


## Related Topics

[Opening tasks](#) on page 14

## UI component overview

Security Desk has a standard user interface in the *Monitoring* task and most reporting tasks, which has four main parts: the *Area view*, *Report pane*, *Canvas*, and *Controls*.



- 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 Controls** Contains widget commands related to the entity type displayed in the selected tile in the canvas.
- C Canvas** Allows you to view and control entities in *tile mode* or *map mode*.
- D Area view** Lists all the entities that are part of your system, which you can drag into the canvas.
- E Hide controls** Click to hide or show the controls.
- F Hide area view** Click to hide or show the area view.

Watch this video to learn more.



### Related Topics

[About the area view](#) on page 10

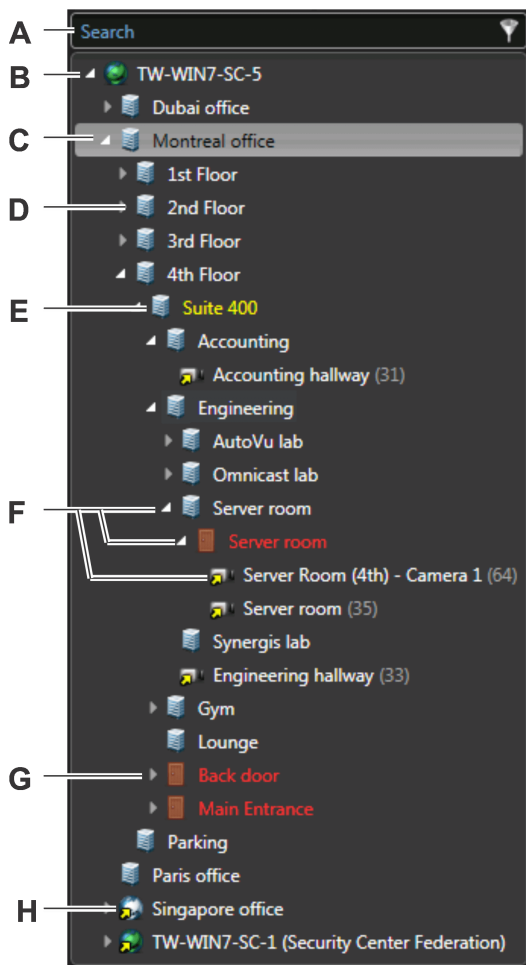
## About the area view

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.



<b>A</b>	<b>Search box</b>	Type in the <i>Search</i> box to find the entities containing that text in their category, name, or description.
<b>B</b>	<b>System entity</b>	The system entity (🌐) cannot be viewed in the canvas.
<b>C</b>	<b>Configure entity</b>	Right-click an entity in the area view, and then click <b>Configure entity</b> (⚙️) to jump to that entity's configuration page in Config Tool. You need the user privilege to modify entity properties to use this command.

<b>D</b>	<b>Area entity</b>	Area entities (  ) can represent a concept or physical location. It is a logical grouping.
<b>E</b>	<b>Yellow entity</b>	Whenever an entity name is displayed in yellow, it means that there is a problem with the settings.
<b>F</b>	<b>Arrow icons</b>	Click the arrows in the entity tree to show or hide child entities.
<b>G</b>	<b>Red entity</b>	Indicates that the entity is offline and the server cannot connect to it, or the server is offline.
<b>H</b>	<b>Federated entity</b>	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> .

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## Related Topics

[Searching for entities](#) on page 12

[Viewing entities in the canvas](#) on page 24

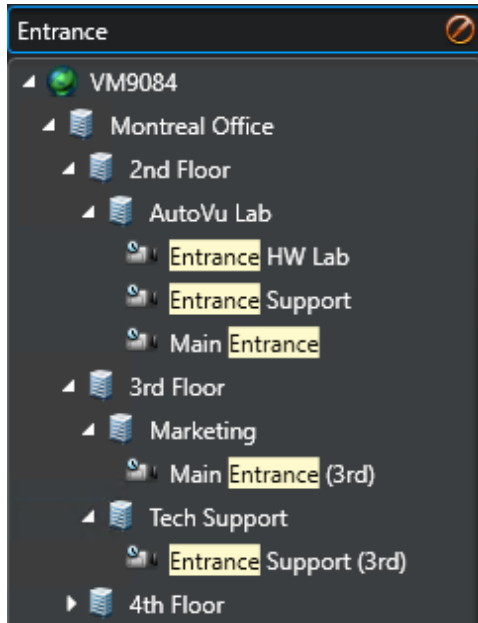


## Searching for entities

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.

## 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:

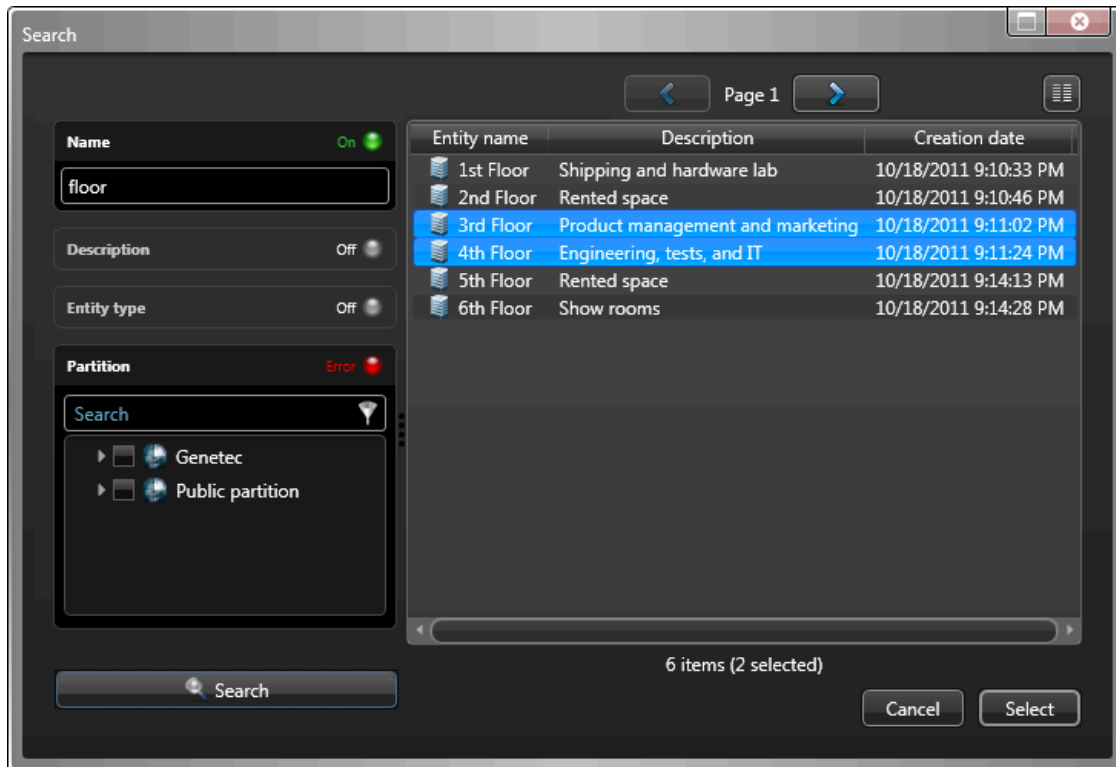
- 1 In the *Search* box in the selector, click **Apply a custom filter** (🔍).
- 2 In the *Search* window, use the filters to specify your search criteria.
  - To turn on a filter, click on the filter heading. Active filters are shown with a green LED (🟢).
  - To turn off a filter (🔴), click on the filter 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** (🔍).
- 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.

# 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 that can be duplicated. Single-instance tasks cannot be renamed.

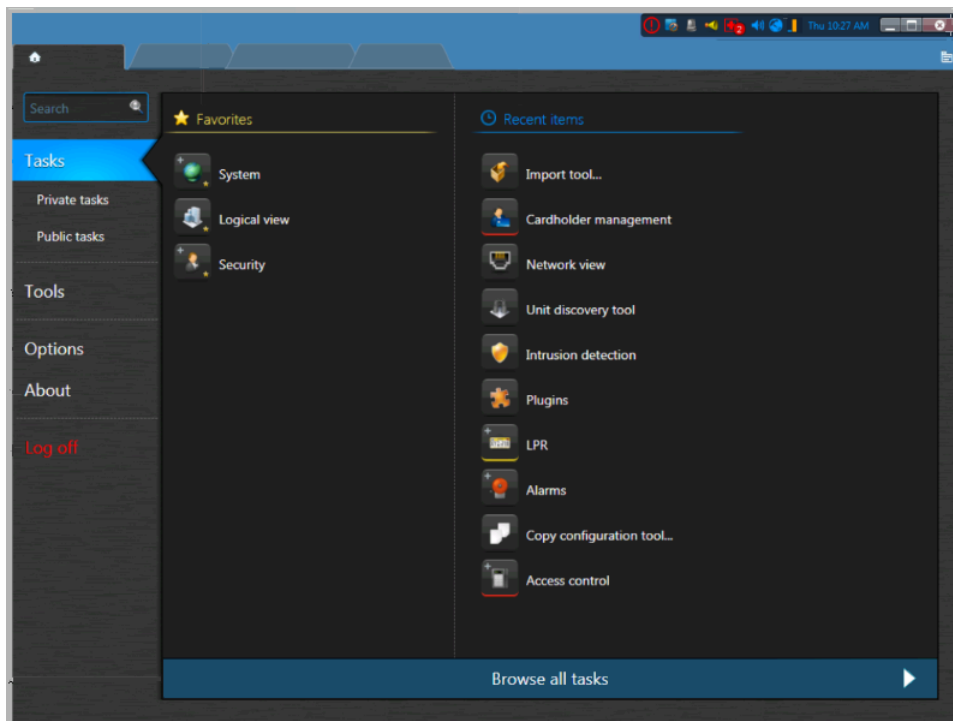
### To open a task:

- From the home page, do one of the following:
  - Enter 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** tab.
- Click the task.

**NOTE:** To open the task in the background, press Ctrl and click the task.

If only one instance of the task is allowed, the new task is created.

- 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.



## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.

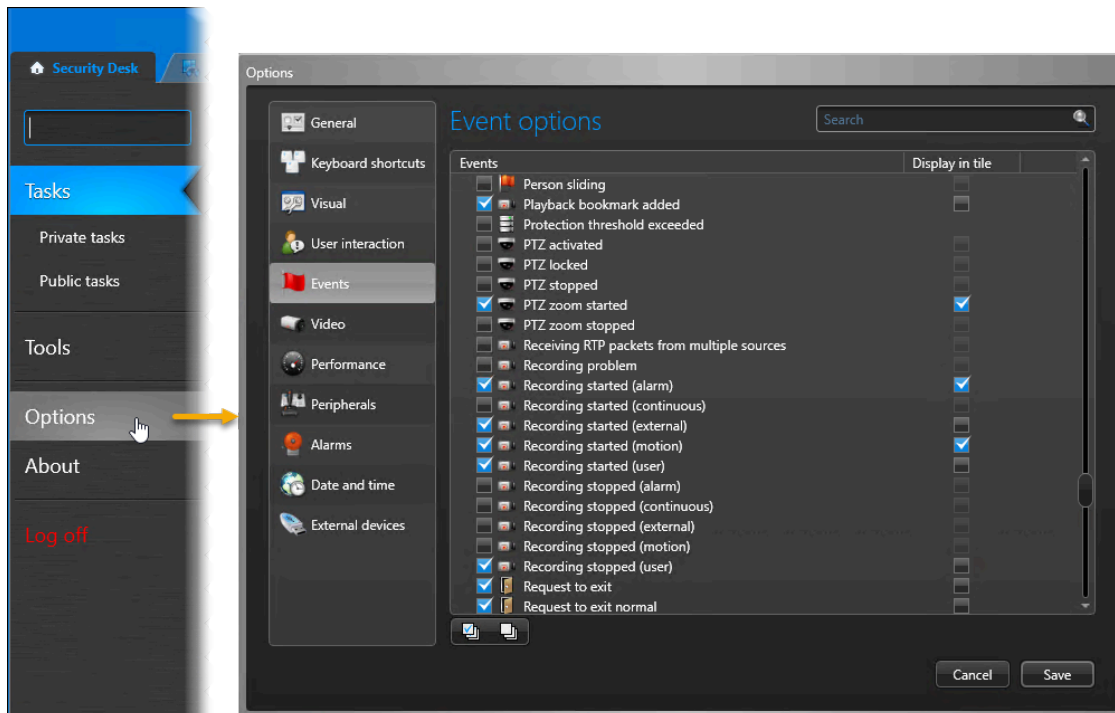


# Monitoring in Security Desk

You can monitor and respond to events, such as camera related events, in real time using the *Monitoring* task in Security Desk. When monitoring events, you monitor the entities that trigger those events.

## To monitor entities in Security Desk:

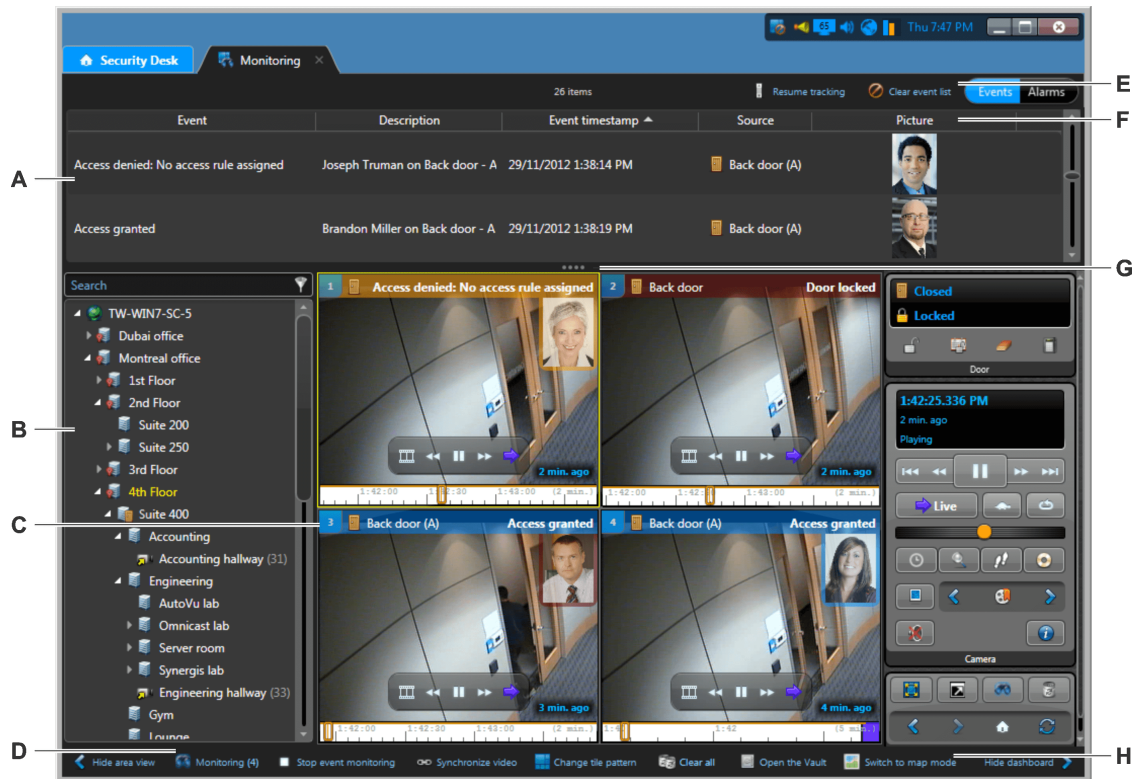
- 1 Select the event types to monitor as follows:
  - a) From the home page, click **Options > Events**.
  - b) In the **Event options** page, select which events to monitor.
  - c) In the **Display in tile** column, select the check boxes of the events you want to view in the Monitoring task canvas. If the check box is cleared, the event only appears in the event list.
  - d) Click **Save**.



- 2 In the area view of the Monitoring task, select the entities you want to monitor (cameras, doors, and so on).
  - 3 Drag the selected entities over the **Monitoring** (👁️) icon at the bottom of the Monitoring task.
- Events that occur in your system are displayed chronologically in the event list.

## Monitoring task overview

To quickly respond to events related to the entities you are monitoring, familiarize yourself with the Monitoring task user interface.

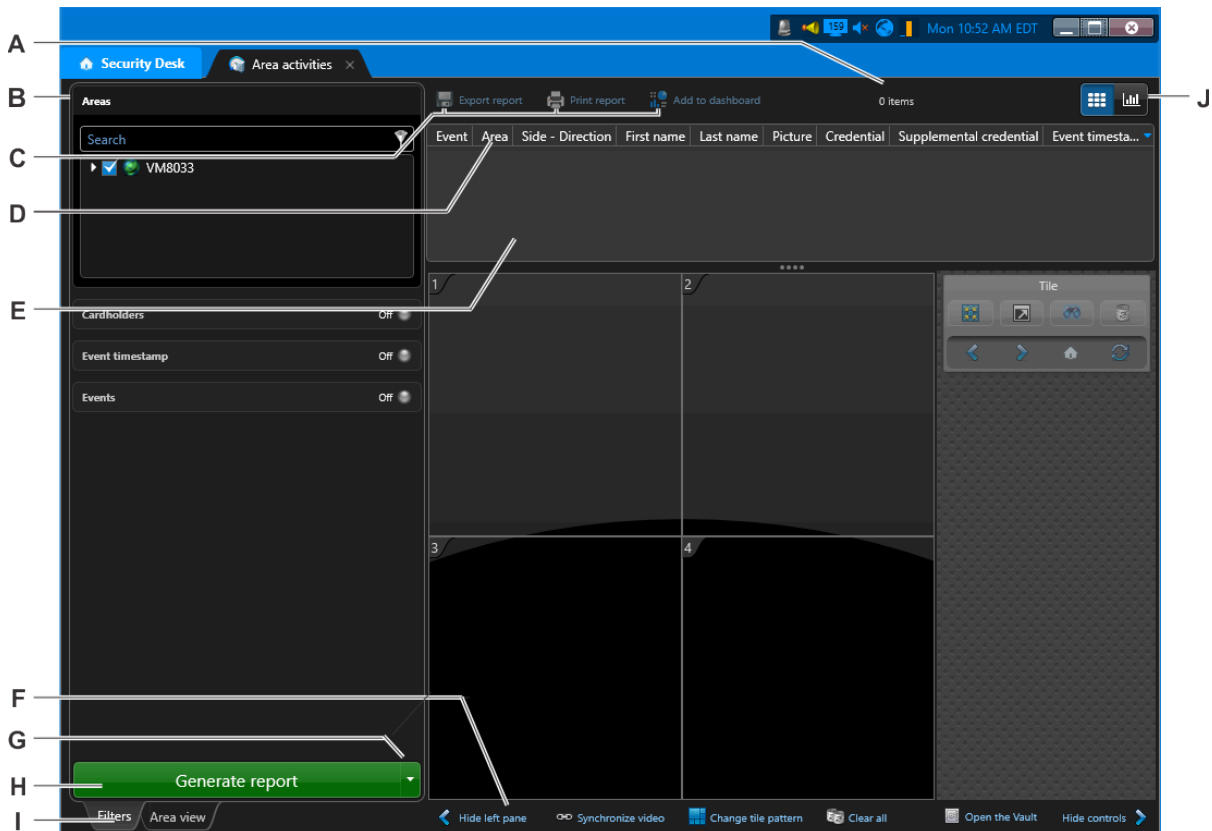


- A** Event list.
- B** Drag entities from the area view onto the canvas, or to the **Monitoring** (👁️) icon at the bottom of the window.
- C** Event monitoring is active on tiles with a blue tile ID. If alarm monitoring is active, the tile ID is red.
- D** Number of entities being monitored.
- E** Remove all events from the event list.
- F** Right-click to show, hide, or reorder the columns.
- G** Drag the grey dots downwards to view the event list.
- H** Switch to a map view.


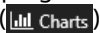


## Reporting task workspace overview

Reporting tasks are where you generate customized queries about 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.



<b>A</b>	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>B</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.
<b>C</b>	Export, print, or add to dashboard	Click to export your generated report, print it, or add the report to a dashboard.
<b>D</b>	Select columns	Right-click a column heading to select which columns to display in the report pane.
<b>E</b>	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).

<b>F</b>	Tile commands	<p>Commands related to canvas tiles:</p> <ul style="list-style-type: none"> <li>• <b>Synchronize video:</b> Synchronize the video displayed in the canvas.</li> <li>• <b>Clear all:</b> Empty all content from tiles.</li> <li>• <b>Change tile pattern:</b> Change the tile pattern in the canvas.</li> </ul>
<b>G</b>	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.
<b>H</b>	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.
<b>I</b>	Filters tab	<p>Use the Filters tab to customize and filter your searches. The Filters tab is only shown in reporting tasks.</p> <p><b>NOTE:</b> Click the Area view tab to show the area view, and select entities to view in the canvas.</p>
<b>J</b>	Tiles or Charts	<p>If the report supports tiles, open the chart view using the toggle button () at the top right of the task. Otherwise, open the chart view using the Charts button ().</p> <ul style="list-style-type: none"> <li>• If the report supports tiles: Click the Tiles button () to show the Tiles view below the report pane.</li> <li>• If the report supports charts: Click the Charts button () to show the Charts view below the report pane.</li> </ul>

### Related Topics

[How to generate reports in Security Desk](#) on page 19

# How to generate reports in Security Desk

You can create customized queries about the entities, activities, and events in your Security Center system for investigation or maintenance purposes by generating reports.

The following image shows the basic steps for generating a report, using the *Archive storage details* task as an example.

- 1 Set up query filters for the report.
- 2 Select a date and time. A green LED indicates a valid time range.  
**NOTE:** Depending on the reporting task you are using, this filter might be called **Event timestamp** or **Triggered on**.
- 3 Generate the report. The maximum number of report results you can receive in Security Center is 10,000.
- 4 Run and save the report directly to a file.
- 5 Save the results by exporting or printing the report.
- 6 Analyze the results in a chart view.
- 7 Query results are listed in the report pane. Double-click a result to view it in the canvas.
- 8 Respond to results by exporting or protecting important video files.

Watch this video to learn more about generating reports.





# Canvas

This section includes the following topics:

- ["About tiles"](#) on page 22
- ["Viewing entities in the canvas"](#) on page 24
- ["Unpacking content in tiles"](#) on page 25
- ["Changing tile patterns"](#) on page 27
- [" Default keyboard shortcuts "](#) on page 28

## 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.

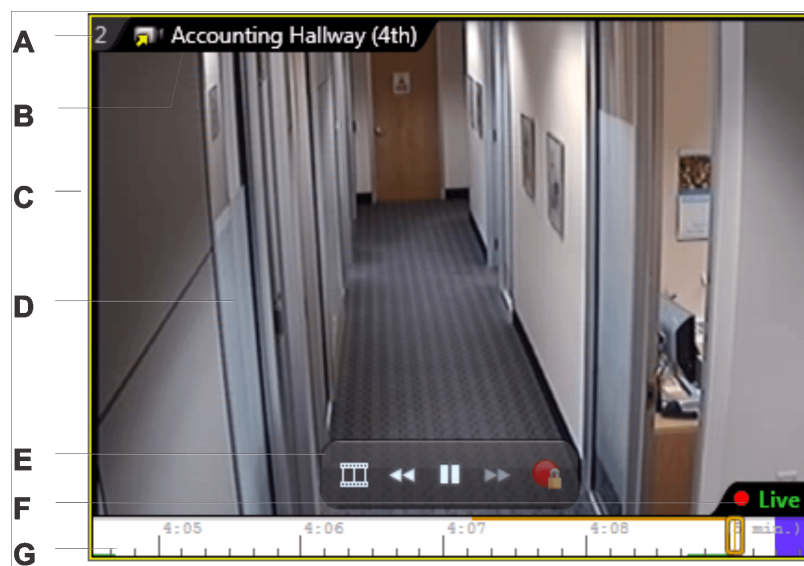
Tiles can display the following:

- Entities
- Event information
- Live and playback video
- Video images
- Cardholder and visitor pictures and information
- ALPR 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 to 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.



<b>A</b>	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>B</b>	Tile toolbar	Displays the entity name. When an event occurs, information corresponding to the event is also shown in the tile toolbar.

---

<b>C</b>	Yellow frame	Indicates that the tile is selected.
<b>D</b>	Video stream	The streaming video is displayed inside the tile. Double-click to expand the tile to the whole canvas.
<b>E</b>	On-tile video controls	Use the on-tile video controls while viewing video in a tile.
<b>F</b>	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.
<b>G</b>	Timeline	A timeline is a graphic illustration of a video sequence, showing where in time, motion and bookmarks are found. Thumbnails can also be added to the timeline to help the user select the segment of interest.  Use the timeline to control playback video.

---

**Related Topics**

[About the video timeline](#) on page 51

[On-tile video controls](#) on page 35

# 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 to a tile. This method only works if there are 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 *Controls* pane.
- 3 To clear entities from the canvas, do one of the following:
  - Right-click on a tile, and then click **Clear** (🗑️).
  - 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.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## 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.

**Limitation:** Limited to a maximum of 16 unpacked elements.

#### To unpack content in a tile:

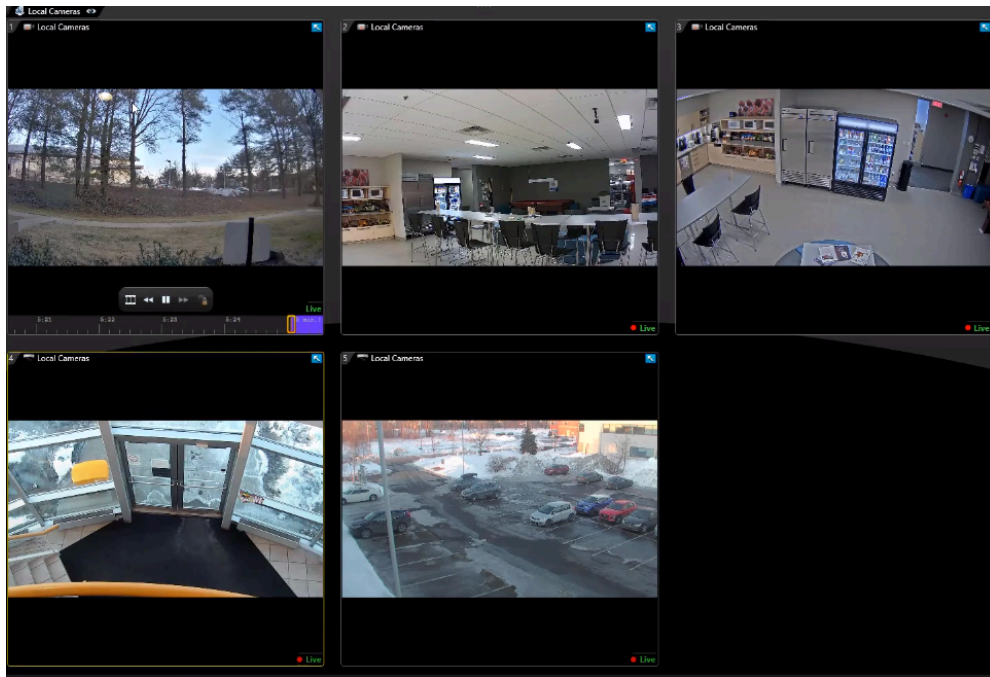
- 1 Select a tile that is displaying a composite entity.
- 2 Beside the entity name in the tile toolbar, click .
- 3 From the drop-down menu, click one of the following:



- 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. Because the tile is packed, only the first camera is displayed (Main Entrance), until you unpack the tile content.



Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.




# Changing tile patterns

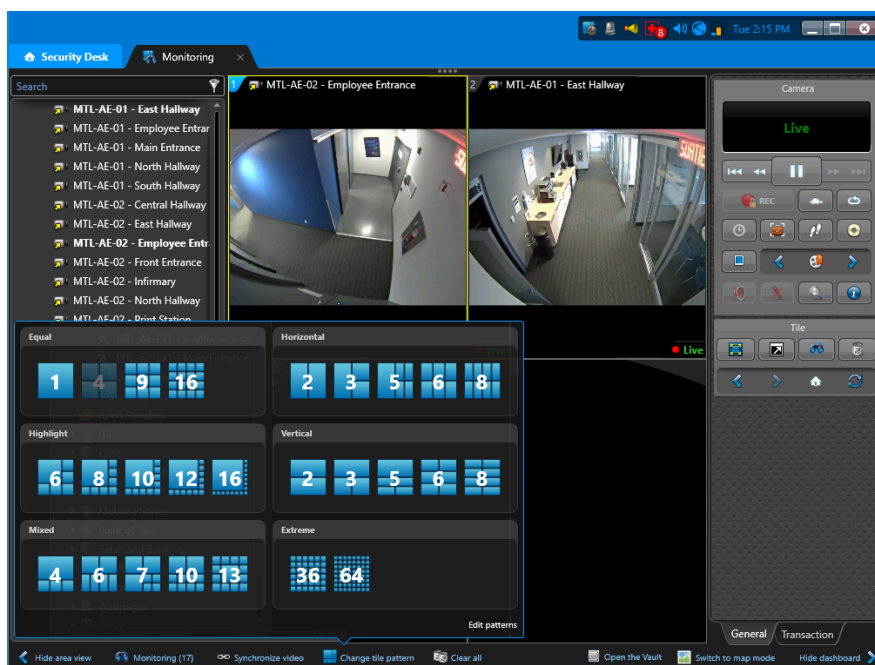
You can change the tile pattern of the canvas.

## 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.



## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.





## 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
<b>General commands</b>		
<b>Auto lock</b>	Lock the workstation.	Ctrl+Shift+L
<b>Controls</b>	Show/hide the controls.	F7
<b>Cycle through canvas only, report only, and both</b>	Show only the canvas, only the report pane, or both.	F9
<b>Exit application</b>	Close the application.	Alt+F4
<b>Full screen</b>	Toggle between displaying the application in windows and full screen mode.	F11
<b>Go to next content in cycle</b>	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
<b>Go to next content in cycle (all tiles)</b>	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
<b>Go to next page</b>	Switch to the next task tab.	Ctrl+Tab
<b>Go to previous content in cycle</b>	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
<b>Go to previous content in cycle (all tiles)</b>	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
<b>Go to previous page</b>	Switch to the previous task tab.	Ctrl+Shift+Tab
<b>Help</b>	Open the online help.	F1
<b>Home page</b>	Go to the home page.	Ctrl+Grave accent ( ` )
<b>Hot action x</b>	Execute hot actions 1-10, once you've configured them.	Ctrl+(F1-F10)
<b>Options</b>	Open the <i>Options</i> dialog box.	Ctrl+O
<b>Select columns</b>	Select which columns to show/hide in the report pane.	Ctrl+Shift+C
<b>Selector</b>	Show/hide the selector pane.	F6

Command	Description	Shortcut
<b>Start cycling</b>	Automatically switch between all loaded entities in Security Desk. By default, a 4 second dwell time for each entity is used.	Ctrl+Up arrow
<b>Start cycling (all)</b>	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
<b>Tiles only</b>	Show only the display tiles and task list. The selector pane, event pane, and controls are hidden. This is mainly used for the <i>Monitoring</i> task.	F10
<b>Tile context menu</b>	Open the tile context menu for the selected tile in the canvas. <b>NOTE:</b> This keyboard shortcut cannot be modified from the <i>Options</i> dialog box.	Shift+F10 or Context menu key Press Tab to cycle through the menu options, and then press Enter.
<b>Alarm commands</b>		
<b>Acknowledge (Default)</b>	Acknowledge the selected alarm in the <i>Alarm report</i> task.	Spacebar
<b>Acknowledge all (Default)</b>	Acknowledge all alarms in the <i>Alarm report</i> task.	Ctrl+Shift+Spacebar
<b>Show alarm page</b>	Open the <i>Alarm monitoring</i> task.	Ctrl+A
<b>Snooze alarm (all)</b>	Put all alarms to sleep for 30 seconds. When an alarm is snoozing, it is temporarily removed from the canvas.	Alt+Ctrl+Shift+S
<b>Snooze the alarm</b>	Put the alarm to sleep for 30 seconds. When the alarm is snoozing, it is temporarily removed from the canvas.	S
<b>Camera commands</b>		
<b>Add a bookmark</b>	Add a bookmark to video in the selected tile (for live video only).	B
<b>Add bookmark (all)</b>	Add bookmarks to video in all selected tiles (for live video only).	Ctrl+Shift+B
<b>Copy statistics of the currently selected video tile</b>	Copy the statistics of the selected tile.	Ctrl+Shift+X
<b>Export video</b>	Export video from the selected tile.	Ctrl+E
<b>Export video from all tiles</b>	Export video from all the tile in the canvas.	Ctrl+Shift+E
<b>Forward</b>	Forward the video playback.	Period (.)
<b>Forward all</b>	Forward the video playback of all cameras that are displayed in the canvas.	Ctrl+Shift+Period (.)

Command	Description	Shortcut
<b>Instant replay</b>	View an instant video replay in the selected tile.	I
<b>Jump backward</b>	Jump backwards in the recorded video according to the seek time specified in the <i>Options</i> dialog box.	Ctrl+Shift+N
<b>Jump backward all</b>	Jump backwards in the recorded video according to the seek time specified in the <i>Options</i> dialog box, for all cameras that are displayed in the canvas.	Alt+Ctrl+Shift+N
<b>Jump forward</b>	Jump forward in the recorded video according to the seek time specified in the <i>Options</i> dialog box.	Ctrl+Shift+M
<b>Jump forward all</b>	Jump forward in the recorded video according to the seek time specified in the <i>Options</i> dialog box, for all cameras that are displayed in the canvas.	Alt+Ctrl+Shift+M
<b>Next frame</b>	When your playback video is paused, go to the next video frame.	M
<b>Next frame all</b>	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
<b>Play/Pause</b>	Pause or play the video recording.	G
<b>Play/Pause all</b>	Pause or play the video recording for all cameras that are displayed in the canvas.	Ctrl+Shift+G
<b>Previous frame</b>	When your playback video is paused, go to the previous video frame.	N
<b>Previous frame all</b>	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
<b>Rewind</b>	Rewind the video playback.	Comma (,)
<b>Rewind all</b>	Rewind the video playback for all cameras that are displayed in the canvas.	Ctrl+Shift+Comma (,)
<b>Show diagnostic timeline</b>	Show the timeline of the video stream diagnosis.	Ctrl+Shift+T
<b>Show video stream diagnosis</b>	Show/hide the video stream diagnosis, where you can troubleshoot your video stream issues.	Ctrl+Shift+D
<b>Show video stream statistics on the tile</b>	Show/hide the statistics summary of the video in the selected tile.	Ctrl+Shift+A
<b>Show video stream status</b>	Show/hide the status summary of the video stream connections and redirections in the selected tile.	Ctrl+Shift+R
<b>Slow motion</b>	Switch the playback to slow motion.	Shift+En dash (-)
<b>Slow motion (all)</b>	Switch the playback to slow motion for all cameras that are displayed in the canvas.	Ctrl+Shift+En dash (-)

Command	Description	Shortcut
<b>Switch to live</b>	Switch to live video.	L
<b>Switch to live (all)</b>	Switch to live video for all cameras that are displayed in the canvas.	Ctrl+Shift+V
<b>Switch to playback</b>	Switch to playback video.	P
<b>Toggle recording</b>	Start/stop recording video for the selected tile.	R
<b>Toggle recording (all)</b>	Start/stop recording video for all cameras that are displayed in the canvas.	Alt+Ctrl+Shift+R
<b>Visual tracking</b>	Enable/disable visual tracking for the selected tile.	Alt+F
<b>Visual tracking (all)</b>	Enable/disable visual tracking for all cameras that are displayed in the canvas.	Ctrl+Shift+F
<b>PTZ commands</b>		
<b>Go to preset</b>	Jump to a PTZ preset you select.	<PTZ preset>+Shift+Insert
<b>Pan left</b>	Pan the PTZ camera image to the left.	Left arrow
<b>Pan right</b>	Pan the PTZ camera image to the right.	Right arrow
<b>Tilt down</b>	Tilt the PTZ camera image down.	Down arrow
<b>Tilt up</b>	Tilt the PTZ camera image up.	Up arrow
<b>Zoom in</b>	Zoom in the PTZ camera image.	Hold the Plus sign (+)
<b>Zoom out</b>	Zoom out the PTZ camera image.	Hold the En dash (-) key
<b>Door commands</b>		
<b>Unlock</b>	Unlock the selected door.	U
<b>Unlock (all)</b>	Unlock all the doors that are displayed in the canvas.	Ctrl+Shift+U
<b>Task commands</b>		
<b>Rename task</b>	Rename the selected task.	F2
<b>Save as</b>	Save a task under a different name and scope (private or public).	Ctrl+T
<b>Save workspace</b>	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
<b>Saved tasks</b>	Open the <i>public tasks</i> page from the home page.	Ctrl+N
<b>Tile commands</b>		
<b>Back</b>	Switch to the previous tile content.	Alt+Left arrow

Command	Description	Shortcut
<b>Change tile pattern</b>	Change the tile pattern in the canvas.	Ctrl+P
<b>Clear</b>	Clear a specific tile in the canvas.	<Tile ID>+Backspace
<b>Clear all</b>	Clear all the tiles in the canvas.	Ctrl+Backspace
<b>Cycle next pattern</b>	Cycle to the next tile pattern.	W
<b>Cycle previous pattern</b>	Cycle to the previous tile pattern.	Q
<b>Display camera sequence</b>	Display a camera sequence in a specific tile.	<Camera sequence ID>+Ctrl+ENTER
<b>Display entity</b>	Display an entity in a specific tile.	<Entity ID>+ENTER
<b>Forward</b>	Switch to the next tile content.	Alt+Right arrow
<b>Home</b>	<ul style="list-style-type: none"> <li>• <b>Map mode:</b> Jump to the home web page associated with the map.</li> <li>• <b>Tile mode:</b> Return to the first content you dragged into the tile.</li> </ul>	Alt+HOME
<b>Maximize tile</b>	Maximize the selected tile to the whole canvas. Press E again to shrink the tile.	E
<b>Maximize tile fullscreen</b>	Maximize the selected tile to full screen mode. Press Alt +ENTER again to shrink the tile.	Alt+ENTER
<b>Monitor alarms</b>	Enable/disable alarm monitoring for the selected tile. When alarm monitoring is enabled, alarms automatically appear in the tile.	Alt+A
<b>Monitor all alarms</b>	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
<b>Monitor events</b>	Enable/disable event monitoring for the selected tile. When event monitoring is enabled, events automatically appear in the tile.	Alt+T
<b>Pack/unpack</b>	Pack/unpack the area or camera sequence in the selected tile.	Alt+U
<b>Refresh</b>	Refresh the page, or reload the selected tile.	F5
<b>Select next tile</b>	Select the next tile in the canvas.	Y
<b>Select previous tile</b>	Select the previous tile in the canvas.	T
<b>Start task cycling</b>	Automatically switch between all loaded tasks in Security Desk. By default, a 4 second dwell time for each task is used.	Ctrl+Q

Command	Description	Shortcut
<b>Stop task cycling</b>	Stop the task cycling rotation.	ESC
<b>Toggle monitoring (all)</b>	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

# Monitoring cameras

This section includes the following topics:

- ["On-tile video controls"](#) on page 35
- ["Camera widget"](#) on page 36
- ["PTZ widget"](#) on page 40
- ["Zooming in and out of video"](#) on page 42
- ["Taking snapshots of video"](#) on page 43
- ["Editing video snapshots"](#) on page 44
- ["Adding bookmarks to video sequences"](#) on page 45
- ["Live and playback video modes"](#) on page 47
- ["Switching between video modes"](#) on page 49
- ["About the video timeline"](#) on page 51
- ["Performing targeted video searches"](#) on page 52
- ["Viewing video archives"](#) on page 54
- ["Video export formats"](#) on page 57
- ["Exporting video in G64x format"](#) on page 58
- ["Exporting video in G64, ASF, and MP4 formats"](#) on page 63
- ["The Export video dialog box"](#) on page 66
- ["Viewing exported video files"](#) on page 68
- ["Sharing exported video files"](#) on page 71

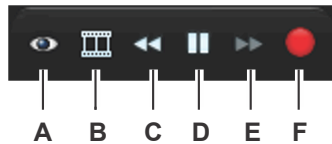
## On-tile video controls

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:



<b>A</b>	<ul style="list-style-type: none"> <li>Go to PTZ preset Only available for PTZ cameras with defined preset positions. Commands the PTZ camera to go to the specified preset position.</li> <li>Go to digital zoom preset Only available for fixed cameras with defined digital zoom presets. Commands the fixed camera to go to the specified digital zoom preset.</li> </ul>
<b>B</b>	Show/hide thumbnail images
<b>C</b>	Rewind (reverse playback)
<b>D</b>	Pause
<b>E</b>	Forward
<b>F</b>	<p>The command depends on whether you are viewing live or playback video:</p> <ul style="list-style-type: none"> <li>Live video: Recording state</li> <li>Playback video: Switch to live video</li> </ul> <p>If the camera is also controlled by an Auxiliary Archiver, you can manually start recording on the Auxiliary Archiver by right-clicking the recording state button, selecting <b>Auxiliary recording</b>, and then clicking the record button (●) next to the Auxiliary Archiver role name.</p> <p><b>NOTE:</b> Various buttons and button colors can be displayed depending on the task you are performing. For more information, see <a href="#">Camera widget</a> on page 36.</p>

### Related Topics

[Camera widget](#) on page 36

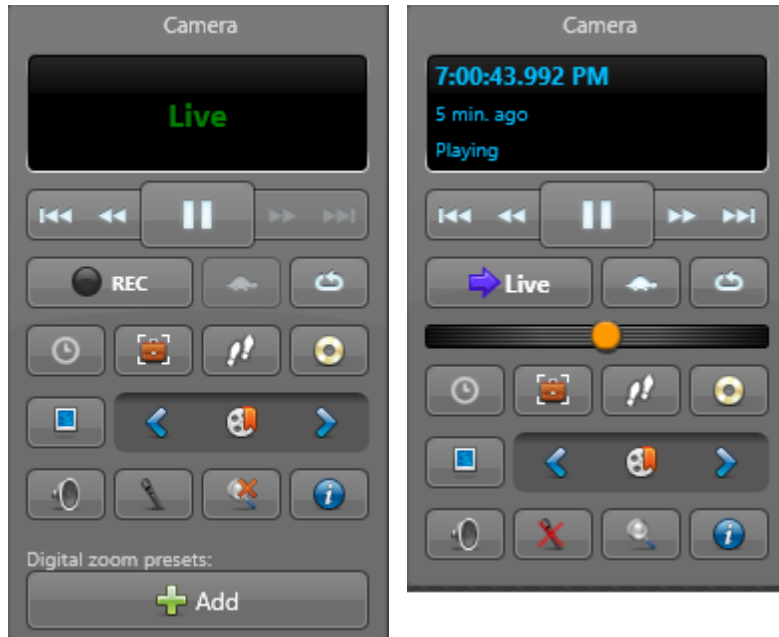


## Camera widget







The *Camera* widget appears in the *Controls* pane 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 is selected in a tile.



The camera widget commands are described below:

Button	Command	Description
	<b>Jump backward</b> <sup>1</sup>	Jump backward. Each click of this button forces the recording playback to jump backwards by 15 seconds. You can configure this value from the <i>Options</i> dialog box.
	<b>Rewind</b> <sup>1</sup>	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.
	<b>Previous frame</b> <sup>1</sup>	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.
	<b>Pause</b> <sup>1</sup>	Pause the playback at the current frame.
	<b>Play</b> <sup>1</sup>	Play back the recording at normal speed (1x).
	<b>Next frame</b> <sup>1</sup>	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
	<b>Forward</b> <sup>1</sup>	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).
	<b>Jump forward</b> <sup>1</sup>	Jump forward. Each click of this button forces the recording playback to jump forward by 15 seconds. You can configure this value from the <i>Options</i> dialog box.
	<b>Switch to live</b> <sup>1</sup>	Switch the displayed images from playback to live video.
	<b>Recording on</b>	(Solid red) The camera is currently recording. Click to stop recording.
	<b>Recording on</b>	(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.
	<b>Recording on (locked by system)</b>	The camera is currently recording, and is controlled by a system configuration. You cannot click to stop recording.
	<b>Recording off</b>	The camera is not currently recording. Click to start recording. The recording stops automatically after five minutes. You can also stop the recording manually.  If the camera is also controlled by an Auxiliary Archiver, you can manually start recording on the Auxiliary Archiver by right-clicking the recording state button, selecting <b>Auxiliary recording</b> , and then clicking the record button (●) next to the Auxiliary Archiver role name.
	<b>Recording off (locked by system)</b>	The camera is not currently recording, and is controlled by a system configuration. You cannot click to start recording.
	<b>Recording problem</b>	There is a problem recording the camera. The problem might be due to an error writing to disk, an error writing to the Archiver database, or the fact that the camera is not streaming video when it should. If you see this error, contact your system Administrator to resolve the issue.
	<b>Slow motion</b> <sup>1</sup>	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.
	<b>Loop playback</b>	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.
	<b>Speed slider</b>	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.
	<b>Speed slider (limited)</b>	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.

Button	Command	Description
	<b>Jog wheel</b>	Replaces the speed slider when the video is paused. Use it for frame by frame playback both forwards and backwards.
	<b>Go to specific time</b> <sup>1</sup>	Open a browser window, and jump to a precise date and time in the recording.
	<b>Quick search</b>	Opens the <i>Quick search</i> dialog box.
	<b>Enable visual tracking</b> <sup>1</sup>	Follow an individual or object that is moving across different cameras from the same tile.
	<b>Export video</b> <sup>1</sup>	Create stand-alone video files that can be played without being connected to the Security Center Directory.
	<b>Save a snapshot</b> <sup>1</sup>	Save the current video frame as an image file.
	<b>Previous bookmark</b> <sup>1</sup>	Jump to the previous bookmark.
	<b>Add a bookmark</b> <sup>1</sup>	Add a bookmark to the video.
	<b>Next bookmark</b> <sup>1</sup>	Jump to the next bookmark.
	<b>Listen</b> <sup>1</sup>	Enable the speaker. This button is only available when the camera supports audio.
	<b>Stop listening</b> <sup>1</sup>	Disable the speaker. This button is only available when the camera supports audio.
	<b>Talk</b> <sup>1</sup>	Enable the microphone. This button is only available when the camera supports audio.
	<b>Stop talking</b>	Disable the microphone. This button is only available when the camera supports audio.
	<b>Toggle digital zoom</b>	Apply a 2x digital zoom to the image. Further digital zoom adjustments can then be performed within the tile.
	<b>Show stream properties</b>	Display the properties of the selected video stream.
	<b>Digital zoom presets</b>	When digital zoom is applied to the selected tile, click this button to add a digital zoom preset for the current camera image position.

<sup>1</sup> If you hold Ctrl+Shift when clicking the command, the command applies to all cameras displayed in the canvas.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## Related Topics

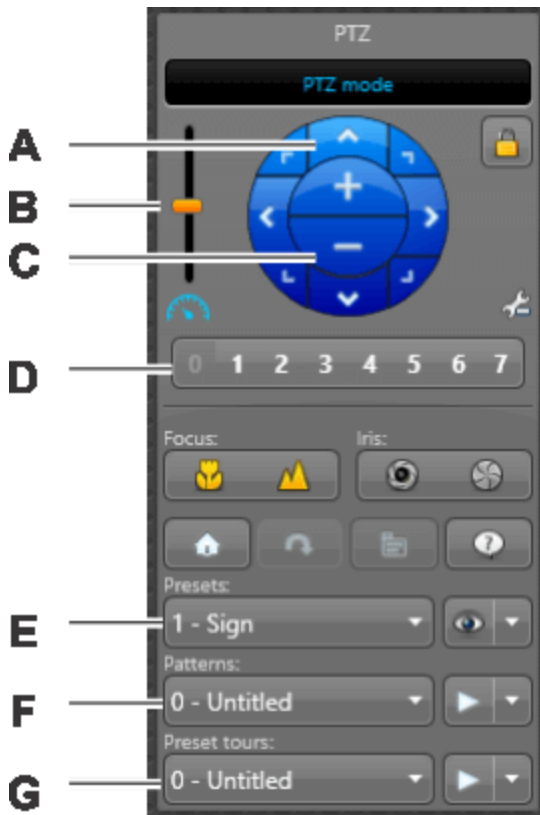
[Switching between video modes](#) on page 49

[Performing targeted video searches](#) on page 52  
[Exporting video in G64x format](#) on page 58  
[Exporting video in G64, ASF, and MP4 formats](#) on page 63  
[Adding bookmarks to video sequences](#) on page 45  
[Zooming in and out of video](#) on page 42














## PTZ widget

The *PTZ* widget is used to perform pan, tilt, and zoom operations on the displayed camera. It appears in the *Controls* pane when the selected tile displays a PTZ-enabled camera (📹).

**IMPORTANT:** Not all PTZ cameras support all PTZ commands. If one or more of the PTZ buttons are greyed out, the PTZ camera you are working with does not support that command.



Button/Letter	Command	Description
<b>A</b>	<b>Direction arrows</b>	Pan the PTZ motor using the eight direction arrows.
<b>B</b>	<b>Speed slider</b>	Adjust the speed of the PTZ motor.
<b>C</b>	<b>Zoom in/out</b>	Zoom in and out using the plus (+) and minus (-) commands.
<b>D</b>	<b>Quick access buttons</b>	Move the PTZ motor to one of the eight quick access PTZ presets.
<b>E</b>	<b>Presets</b>	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.
<b>F</b>	<b>Patterns</b>	Select a PTZ pattern from the drop-down list to start a PTZ pattern (series of presets or recorded PTZ movements), record a new pattern, or rename the pattern.
<b>G</b>	<b>Preset tours</b>	Select an auxiliary from the drop-down list to start or stop an auxiliary command, or rename the command.
🔒	<b>Lock PTZ</b>	Lock the PTZ motor so only you have control of the PTZ.

Button/Letter	Command	Description
	<b>Toggle to advanced mode</b>	Open the PTZ Advanced mode menu.
	<b>Focus near</b>	Focus the PTZ near.
	<b>Focus far</b>	Focus the PTZ far.
	<b>Open iris</b>	Manually control the iris (open iris).
	<b>Close iris</b>	Manually control the iris (close iris).
	<b>PTZ home</b>	Go to the PTZ home (default) position.
	<b>Flip</b>	Flip the PTZ motor 180 degrees.
	<b>Menu on/off</b>	Open the PTZ menu. This option is only for analog PTZ cameras.
	<b>Specific commands</b>	Use commands that are specific to that camera model.
	<b>Go to preset</b>	Jump to the preset position selected in the drop-down list. <ul style="list-style-type: none"> <li>• <b>Save:</b> Save the preset selected in the drop-down list, using the current PTZ position.</li> <li>• <b>Clear preset:</b> Clear the PTZ position from the preset.</li> </ul>
	<b>Start pattern</b>	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"> <li>• <b>Rename:</b> Rename the selected preset, pattern, or auxiliary.</li> <li>• <b>Record pattern:</b> Record a new PTZ pattern.</li> <li>• <b>Clear pattern:</b> Clear the pattern.</li> </ul>
	<b>Start auxiliary command</b>	Start a PTZ auxiliary command (for example, a wiper blade).
	<b>Stop auxiliary command</b>	Stop the PTZ auxiliary command.
ABC	<b>Rename</b>	Rename the selected preset, pattern, or auxiliary.

## Zooming in and out of video

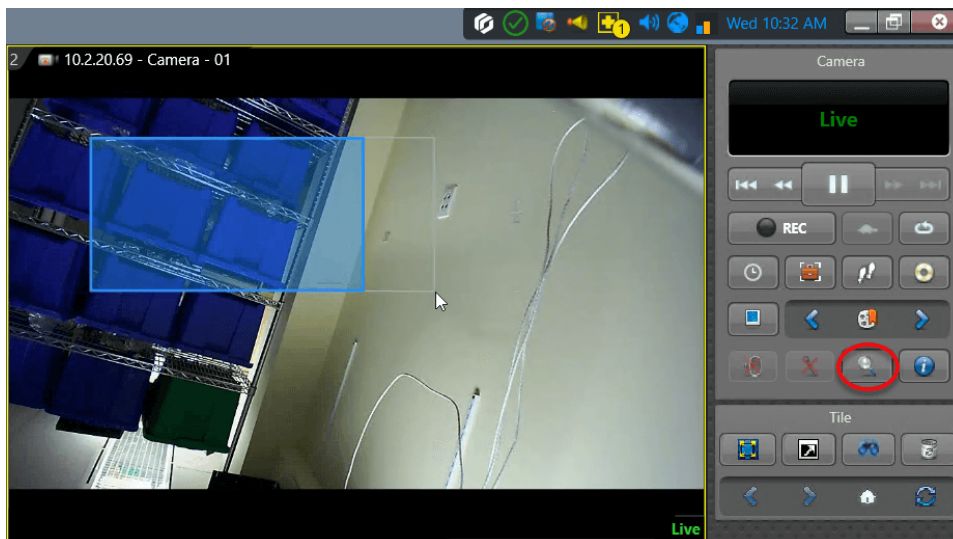
To get a better view of the finer details of what you are monitoring, you can zoom in on the live or playback video that is displayed in a tile, regardless of whether you are using fixed cameras or PTZ cameras.

### 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.

### Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



# 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.



## What you should know

- All snapshots are saved with the following naming convention: *CameraName (Date Time).png*. By default, snapshots are saved as PNG file in the following location: *C:\Users\Username\AppData\Local\Genetec Inc \Vault*.
- If you plan to use the snapshot for incident investigation, note that only JPEG files include EXIF tags that provide chain of custody information.

### 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, 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 2 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**.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.





# 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 From the home page, click **Tools > Vault**.
- 2 From the Vault, open the *Image editor* by doing the following:
  - Select the snapshot and click **Edit** (.
  - Right-click the snapshot and click **Edit**.
- 3 Edit the snapshot using the following editing tools:
  - Rotate the image
  - Flip the image
  - Crop the image ()
  - Adjust the transparency ()
  - Adjust the brightness and contrast ()
  - Hide or blur sections of the image using the **Mask** tool ()
  - Zoom the image in or out by holding the **Ctrl** key, and scrolling using your mouse wheel

After the image is zoomed in, you can pan and scroll the image. Pan the image by holding the **Ctrl** key, and clicking and dragging your mouse. Scroll vertically using your mouse wheel. Scroll horizontally by holding the **Shift** key, and using your mouse wheel.
- 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.

# 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

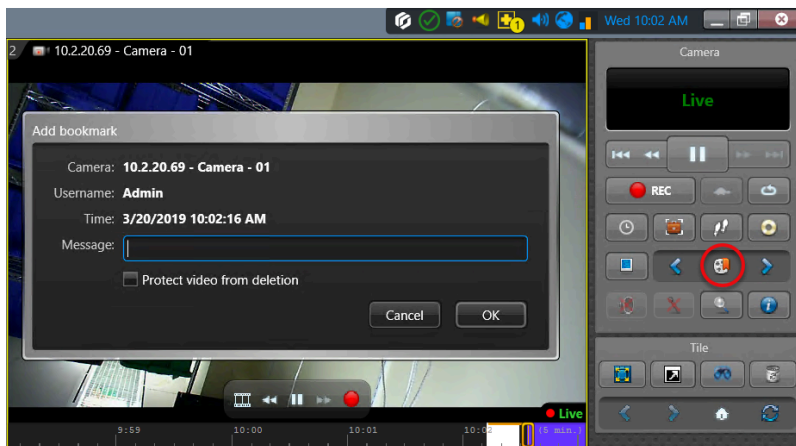
- A bookmark is an indicator of an event or incident that is used to mark a specific point in time in a recorded video sequence. A bookmark also contains a short text description that can be used to search for and review the video sequences at a later time.
- If a camera is not currently recording, adding a bookmark forces it to begin recording.
- If you add a bookmark to an exported video clip, the bookmark is only stored in the exported video clip and not the original archived video.

### 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 of the protection.  
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.



## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## Viewing bookmarked videos

To view a video sequence that was previously bookmarked, you can generate a report of 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 predefined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
  - **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.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## Report pane columns for the Bookmarks 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 Bookmarks report using Web Client, not all of the report columns are available.



- **Camera:** Camera name.
- **Custom fields:** Predefined custom fields for the entity. The columns only appear if custom fields are defined for the entity and were made visible to you when they were created or last configured.
- **Event timestamp:** Date and time that the event occurred.
- **Message:** Bookmark message (might be blank if no message was written).
- **Source (entity):** The name of the system the camera belongs to.
- **Thumbnails:** Thumbnail images of the recorded video during the selected time range. Thumbnails only appear for video that was recorded by an Archiver or Auxiliary Archiver, not if the video was recorded on the edge. Thumbnails are not available for video archives in Cloud storage.

## Live and playback video modes

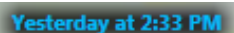

When viewing a camera in the canvas, you can alternate between *live* and *playback* video modes from the timeline or from the camera widget in the *Controls* pane.

Using the camera widget, you can pause, rewind, or instantly replay video. 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:

- Green with red dot (  ) - The camera is currently recording.
- Green (  ) - 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.

-  Date/Time stamp overlay in *relative* mode.
-  Date/Time stamp overlay in *absolute* mode.

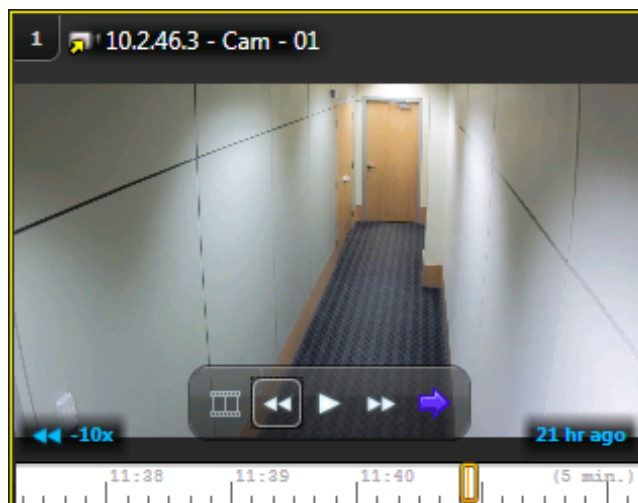
### How the video mode is determined

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 to 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)

### Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



### Related Topics

[Switching between video modes](#) on page 49

## Switching between video modes

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

### 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:

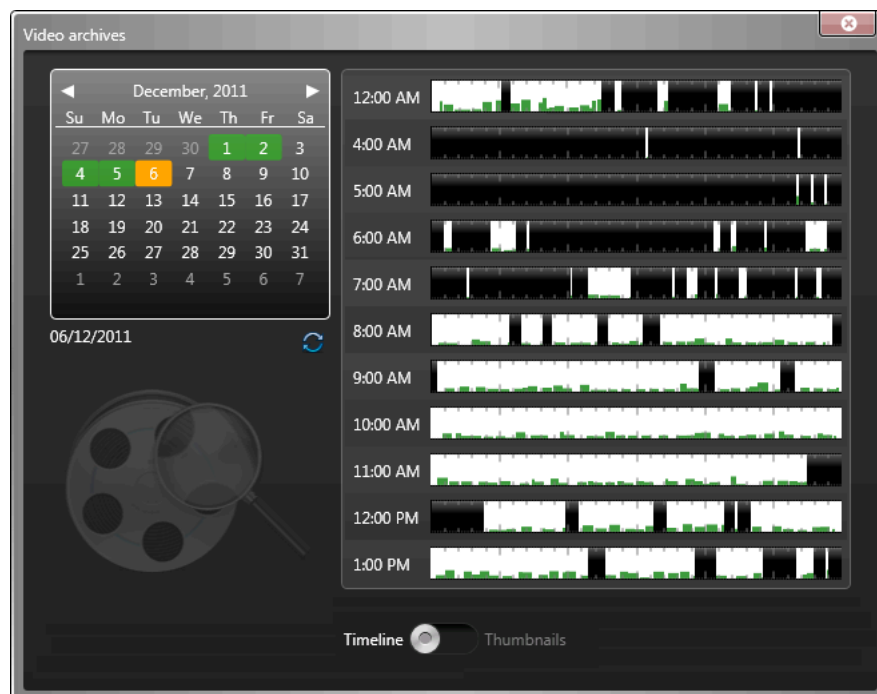
- On the timeline, click and drag the playback cursor to the left.
 

**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:
  - a. In the camera widget, click **Go to specific time** (🕒).
  - b. 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.



- c. (Optional) Switch between *Timeline* and *Thumbnails* view.
- d. 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** ().

### Related Topics

[Live and playback video modes](#) on page 47

## 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.



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

### Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.






## Performing targeted video searches

If a camera recorded an event and you know where the event occurred in the camera's field of view, such as a bag removed from a table, you can use *Quick search* on the playback video to find the exact video sequence containing the evidence.

### What you should know

*Quick search* only supports playback video.

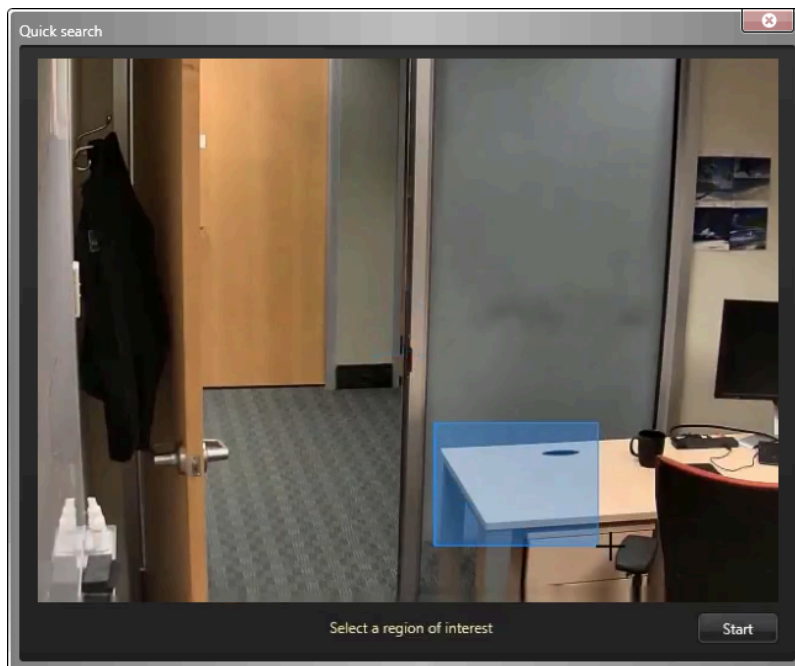
#### To perform a targeted video search:

- 1 From the home page, open the *Monitoring* task.
- 2 From the area view, drag the camera you want to search from to a tile.
- 3 In the camera widget, click **Quick search** .

The selected camera is displayed in the *Quick search* dialog box.

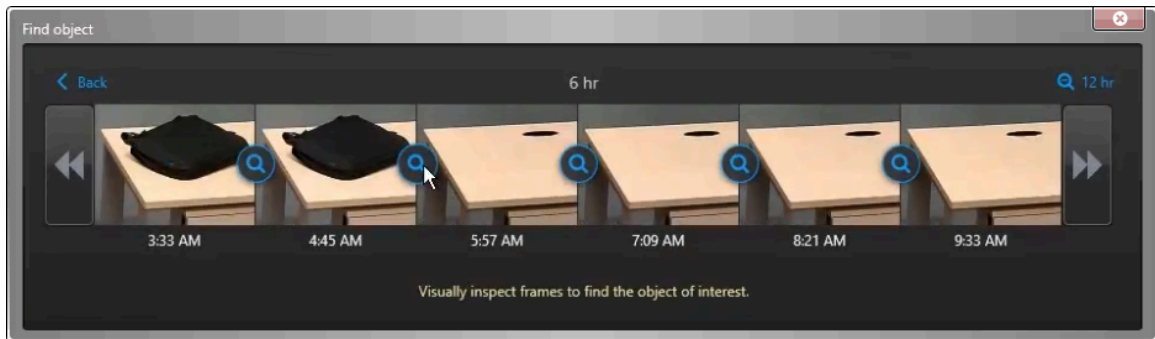
- 4 Draw a rectangle around the area you want to target your search.

For example, if you are trying to find out who removed an object from a table, circle the corner of the table where the object was supposed to be left.






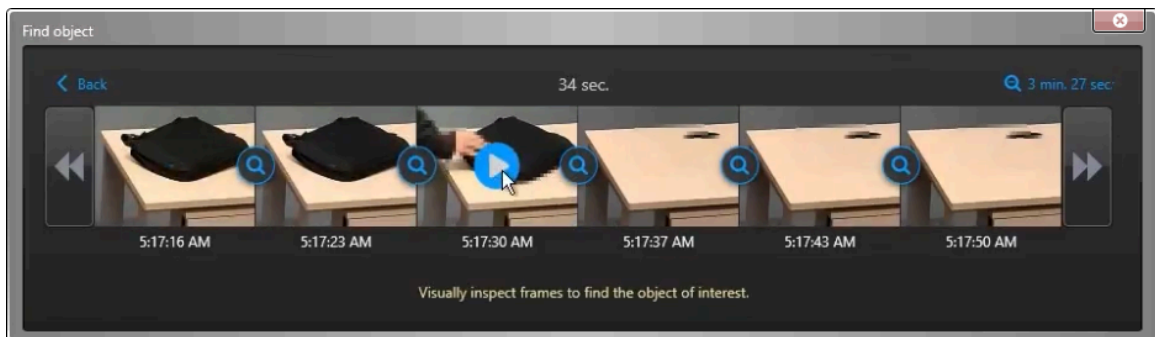
5 Click **Start**.

An overview of the last six hours of video recording is displayed as a series of thumbnails cropped to the area you selected.



**NOTE:** No thumbnails are displayed when there is no recorded video. If you know that recorded video exists but do not see any thumbnails, Security Desk might not be configured correctly. Ask your system administrator to resolve this issue for you.

- 6 Visually inspect the thumbnails and click the  button between the two frames when the object was removed.
- 7 If none of the frames correspond to the moment you are looking for, click  or  to move backward or forward in the timeline.
- 8 Continue the search process until you find the exact moment when the incident took place.
- 9 When you find the exact moment you are looking for, click the corresponding frame to start the playback from that moment.



- 10 (Optional) [Export the video sequence as evidence.](#)

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## Viewing video archives

Using the Archives report, you can find and view video archives on your system by camera and time range.

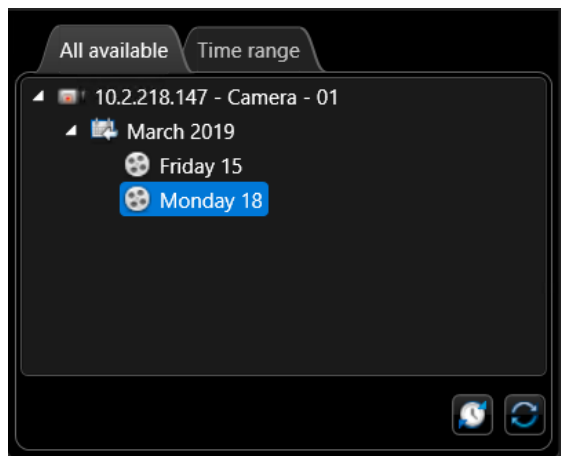
### What you should know


If an important security event occurs, you can do the following in the Archives report:

- Search for available *video archives* from a specific time range or from a specific camera during a given date.
- Search through the video archives to review a video recording.
- Export a video recording to share with colleagues or law enforcement.
- Retrieve cloud archives from long-term storage.

#### To view a video archive:

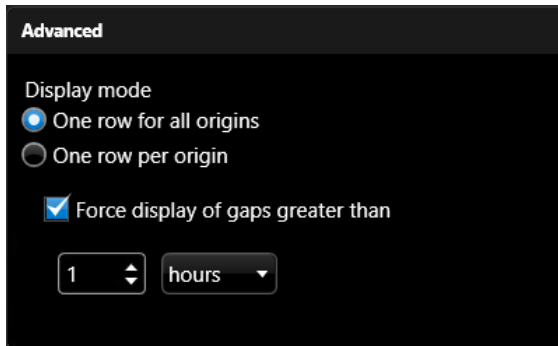
- 1 From the Security Desk home page, open the *Archives* task.
- 2 Click the **Filters** tab and select the cameras that you want to investigate.
- 3 Search for video archives by date or by time range:
  - To search for video archives by date:
    - a. Click the **All available** tab, and then select the cameras that you want to investigate. All days that include video archives for the selected cameras are listed by month and day.



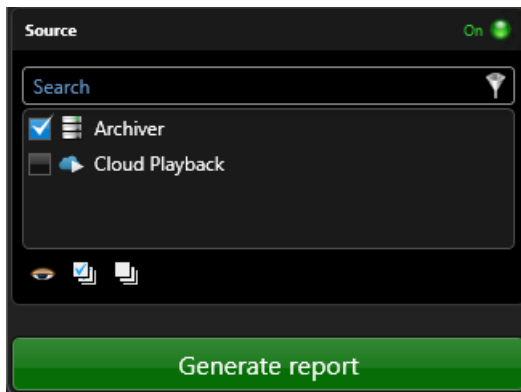
- b. To show the time range for each day that video archives are found for, click .
  - c. Select a date.
- To search for archives by time range:
    - a. Click the **Cameras** filter and select the cameras to investigate.
    - b. Click the **Time range** tab and set the time range.

- 4 Select advanced display mode options.

**NOTE:** The **Force display of gaps greater than** field can be configured for seconds, minutes, hours, or days.



- 5 Search a specific source.



Possible sources include:

- Archiver roles
- Auxiliary Archiver roles
- Cloud Playback role
- Omnicast™ Federation™ roles
- Security Center Federation™ roles

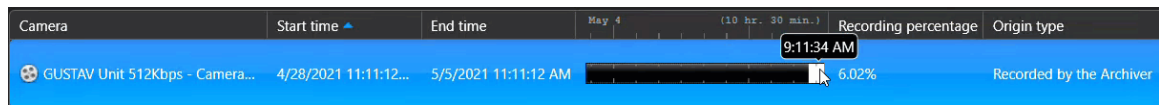
## 6 Click **Generate report**.

The related video recordings are listed in the report pane:

- 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, and the *Preview* column header is replaced with a timeline ruler.

**NOTE:** If the report results include cameras in different time zones and your system displays time based on each device's time zone, the timeline ruler is hidden.

- If you searched by time range, you can hold the Ctrl key and use the mouse wheel to zoom in or out on the timeline ruler.



**NOTE:** You cannot zoom outside of the original query time span. To view a larger time span, generate a new query.

The *Preview* column shows where video is available within the sequence for each camera. You can hover over this timeline to see specific timestamps.

## 7 To view the video sequence in a tile, double-click or drag an item from the report pane to the canvas. The selected sequence starts playing.

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

- A valid certificate if the video stream is encrypted.
- The required privilege to see that particular camera. The camera might be blocked and require a special privilege to see its archives.

## 8 To control the video recording, use the *Camera* widget.

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

## 10 To retrieve video archives from long-term cloud storage, select the item in the report pane and click **Retrieve cloud archives** (☁️).

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## Related Topics

[Exporting video in G64x format on page 58](#)

[Exporting video in G64, ASF, and MP4 formats on page 63](#)

[Camera widget on page 36](#)

# 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 G64x, G64, ASF, and MP4.

## G64x and G64 formats

G64x and G64 are Security Center video formats that support audio, bookmarks, date-time information, metadata overlays, and motion indicators. All event markers are included in the exported file, except metadata markers. These formats also support variable frame rate and variable image resolution.

**NOTE:** The G64 format is deprecated and has been superseded by G64x. Only use G64 to ensure compatibility with Security Center 5.2 and earlier, and Omnicast™ 4.8 and earlier.

If present, G64x files automatically inherit the *digital signature* from the original video. There can only be one signature per file. If an exported video sequence has multiple signatures, a separate file is generated for each signature. Additionally, G64x is the only format that can be re-exported, if that option is selected during export.

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. These G64 files will carry a digital signature if the original video was signed.

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 associated with the video sequence and digital signatures are 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, overlays, and digital signatures are not currently supported.

# Exporting video in G64x format

---

To create stand-alone G64x video files that you can play without connecting to Security Center, you can export from any task in Security Desk that displays live or playback video.

## Before you begin

- Review the available [video export formats](#).
- Ensure that you have the *Export video* privilege.

## What you should know

- When you export a G64x video, the system can include additional file information, such as camera name, creation date, and camera coordinates, which can be useful for investigation. To view additional file information, right-click 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.

- If you have video watermarking enabled, digital signatures and encryption in the video source are excluded from your exported file.

### To export video:

- 1 From the Security Desk home page, open any task that can display live or playback video.

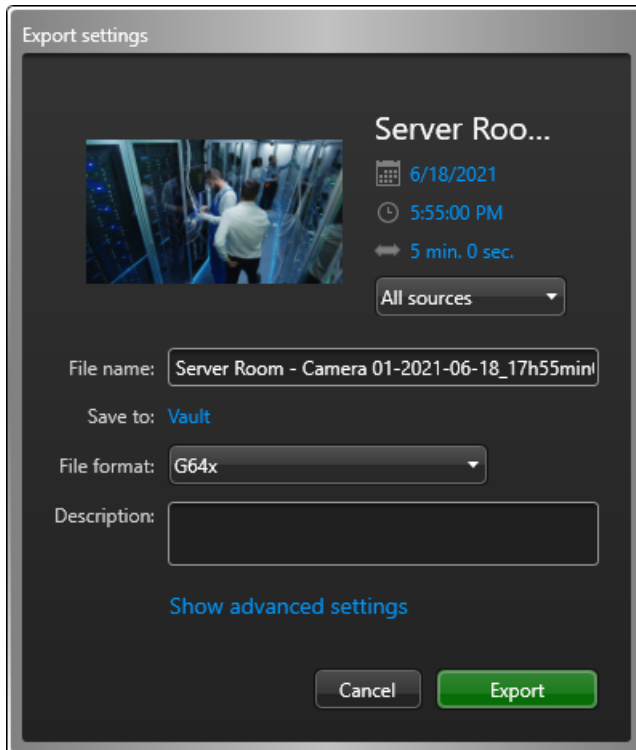
## 2 Select the video to export.

- After generating a report, select one or more items from the report pane, and click **Export video** (📺).
- Open video in a tile, right-click the tile, and click **Camera > Export video**.
- In the *Camera* widget, click **Export video** (📺).

You can export video from the selected tile or from all tiles.

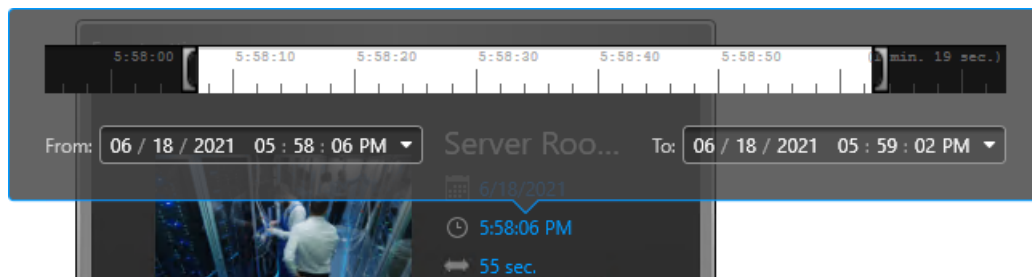
**NOTE:** Privacy protection is not removed from video streams during export. To export protected streams without blurring or anonymization, users with the *Remove privacy protection* privilege must remove privacy protection from the required streams before they click **Export video**.

The *Export settings* dialog box opens:



## 3 Set the date, time, and duration of the selected video sequences:

- Click the date, time, or duration setting.
- Enter the date and time for the start and end of the sequence, or drag the time range markers (⏮ ⏭) to the desired length of time.



**NOTE:** You can set a maximum time range of 24 hours.



- (Optional) To export a video sequence from a specific source, click **All sources** and select the source to export from.
- If required, update the name of the video file in the **Filename** field.  
By default, the file name includes the camera name, the date, and the duration of the video sequence.



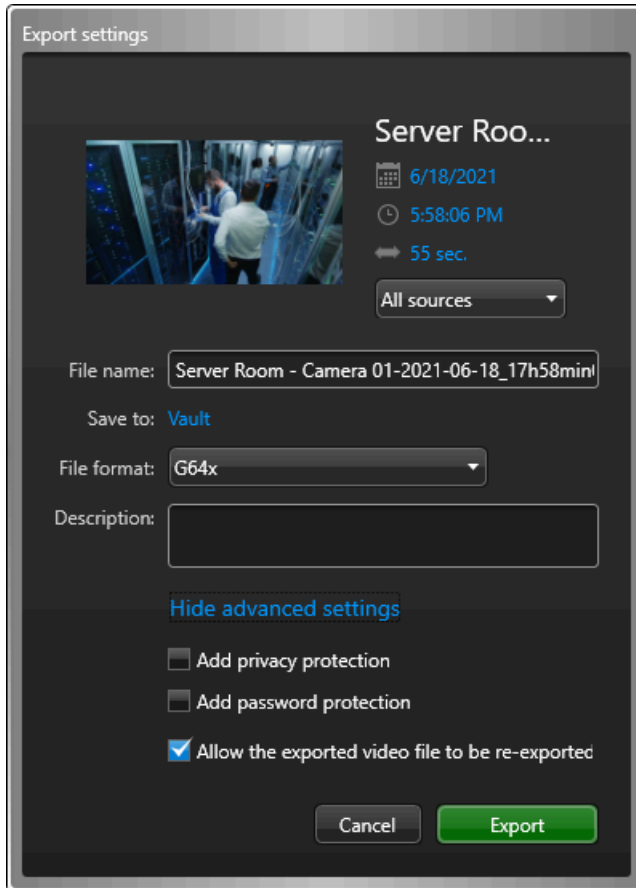
- 6 (Optional) To save the video file in a specific subfolder of the Vault, click **Vault** and create or select a subfolder.
- 7 In the **File format** list, select **G64x**.
- 8 In the **Description** field, enter a description for the exported video if necessary.  
The description is shown in the *Audit trails* and file properties in the Vault.

**NOTE:** A description is mandatory for users without the *Single user export* privilege.

For all other users, the field is only available if the G64x format is selected, and the **Include additional properties on export/snapshot** option is enabled in the user configuration.

- 9 If you are exporting video from all tiles, do the following:
  - a) Select a **Playback mode**.
    - **All at once:** Play back the sequences in the same tiles that they were displayed in when exported.
    - **Sequential:** Play back the video in-sequence within a single tile.
  - b) To change the playback order of the video sequences, select a video sequence and use the  and  buttons.

10 If required, click **Show advanced settings** and configure as needed:



- a) If you have a KiwiVision™ Privacy Protector™ license, select **Add privacy protection** to pixelate motion in the exported video. This privacy protection is always applied using default settings.
- b) Select **Add password protection** and enter a password to encrypt the video file. The password must be entered to open the exported video.

**NOTE:** Password protected video files cannot be re-exported.

- c) Select **Allow the exported video file to be re-exported** to enable all or part of the exported video to be reexported in the same or a different format.

Video files can be re-exported in Security Desk or the Genetec™ Video Player.

11 Click **Export**.

If you do not have the *Single user export* privilege, the *Authorization* window opens, and a second user with the *Export video* privilege must enter their credentials to authorize the 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.

If another export process is running, your export is queued and starts when the previous export has finished. When your export is complete, the video files are created in the export folder that you specified, and the files are available in the Vault.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## After you finish

Do one of the following:

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

# Exporting video in G64, ASF, and MP4 formats

---

To create stand-alone G64, ASF, and MP4 video files that you can play without connecting to Security Center, you can export from any task in Security Desk that displays live or playback video.

## Before you begin

- Review the available [video export formats](#).
- Ensure that you have the *Export video* privilege.

## What you should know

- When you export a G64, ASF, or MP4 video, the system does not include additional file information, such as camera name, creation date, and camera coordinates, which can be useful for investigation. To include additional file information, [export the file as G64x](#).
- If you lack the *Single user export* privilege, a second user with the *Export video* privilege must authorize the export.
- If another export process is running, your export is queued and starts when the current export has finished.

### To export video:

- 1 From the Security Desk home page, open any task that can display live or playback video.

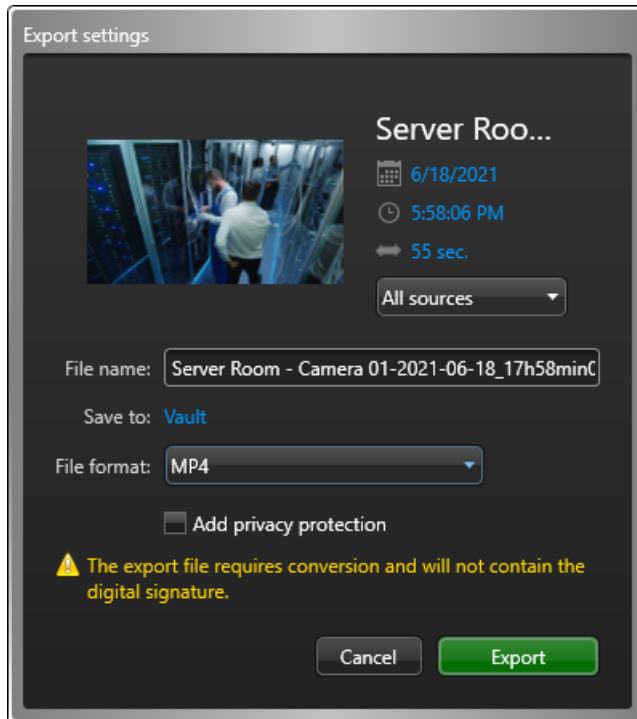
## 2 Select the video to export.

- After generating a report, select one or more items from the report pane, and click **Export video** (📺).
- Open video in a tile, right-click the tile, and click **Camera > Export video**.
- In the *Camera* widget, click **Export video** (📺).

You can export video from the selected tile or from all tiles.

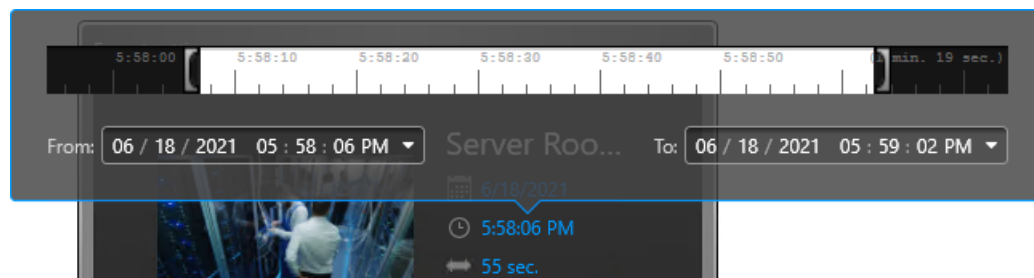
**NOTE:** Privacy protection is not removed from video streams during export. To export protected streams without blurring or anonymization, users with the *Remove privacy protection* privilege must remove privacy protection from the required streams before they click **Export video**.

The *Export settings* dialog box opens:




## 3 Set the date, time, and duration of the selected video sequences:

- Click the date, time, or duration setting.
- Enter the date and time for the start and end of the sequence, or drag the time range markers (⏮ ⏭) to the desired length of time.



**NOTE:** You can set a maximum time range of 24 hours.

4 (Optional) To export a video sequence from a specific source, click **All sources** and select the source to export from.

- 5 If required, update the name of the video file in the **Filename** field.  
By default, the file name includes the camera name, the date, and the duration of the video sequence.  
**NOTE:** Multiple video sequences exported at the same time are each saved as a separate file with a unique file name.
- 6 (Optional) To save the video file in a specific subfolder of the Vault, click **Vault** and create or select a subfolder.
- 7 In the **File format** list, select **G64 (compatibility mode)**, **ASF**, or **MP4**.
- 8 (Optional) If you have a KiwiVision™ Privacy Protector™ license, select **Add privacy protection** to pixelate motion in the exported video. This privacy protection is always applied using default settings.
- 9 Click **Export**.  
If you do not have the *Single user export* privilege, the *Authorization* window opens, and a second user with the *Export video* privilege must enter their credentials to authorize the 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.  
If another export process is running, your export is queued and starts when the previous export has finished. When your 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

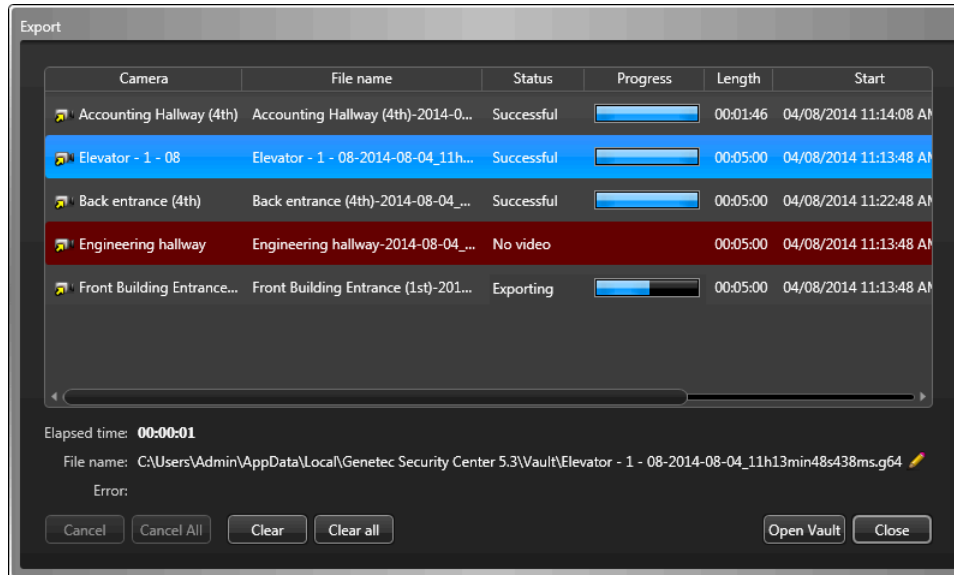
Do one of the following:

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

## 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.
  - **Canceled:** The export operation has been canceled 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.

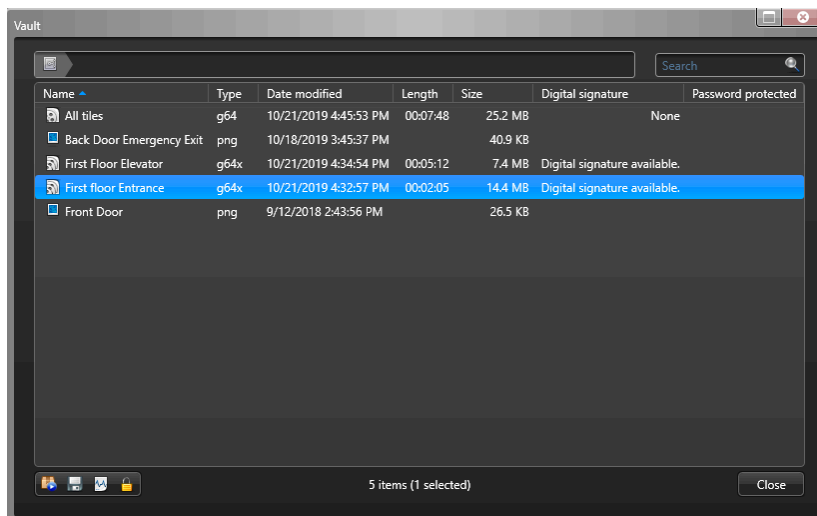
### What you should know

- 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 to play the file correctly.
- When you export a G64x video, the system can include additional file information, such as camera name, creation date, and camera coordinates, which can be useful for investigation. To view additional file information, right-click 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 view an exported video file from the Vault:

- 1 From the home page, click **Tools > Vault**.



The Vault displays all exported files.

- 2 Double-click the file you want to view.  
(G64x only) If the file is password-protected, enter the password.

One of the following happens:

- If it is a G64x file, the file opens in Security Desk and plays in the canvas of the *Monitoring* task.
- If it is an ASF or MP4 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 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.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## 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 if 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.
- **Digital signature:** Indicates whether or not the video file is digitally signed.
- **Encryption:** Indicates whether the video file is encrypted. If the file is encrypted, you must decrypt it before you can view it.
- **Date modified:** Date the video file was last modified.

- 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.



# 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.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



# Monitoring access control entities

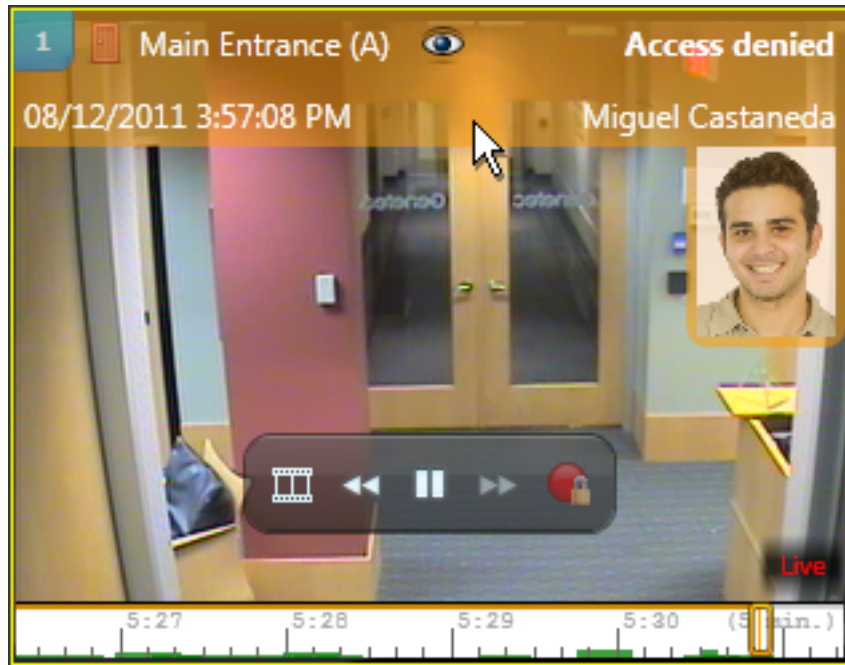
This section includes the following topics:

- ["How access events are displayed in tiles"](#) on page 73
- ["Door widget"](#) on page 74
- ["Searching for cardholders and visitors using their credential"](#) on page 75
- ["Creating cardholders"](#) on page 76
- ["Checking in new visitors"](#) on page 80
- ["Checking out visitors"](#) on page 83
- ["Assigning credentials"](#) on page 84
- ["Assigning temporary cards"](#) on page 90
- ["Viewing properties of cardholder group members"](#) on page 92
- ["Viewing credential properties of cardholders"](#) on page 93
- ["Investigating visitor events"](#) on page 94
- ["Allowing access through doors"](#) on page 96
- ["Investigating door events"](#) on page 98

## 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.



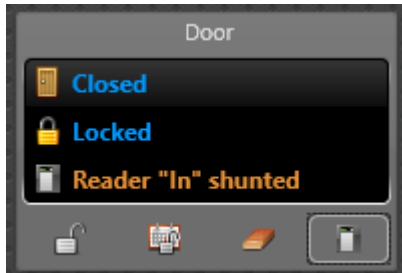
### How antipassback works

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*.

## 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 state (closed or opened), the lock state (locked, unlocked, unlocked and in maintenance mode, or unsecured), and the reader state (if it is shunted).



The door widget commands are described below:

Button	Command	Description
	<b>Unlock<sup>1</sup></b>	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).
	<b>Override unlock schedules</b>	Unlock the door indefinitely for maintenance purposes, or keep the door locked or unlocked for a predetermined period.
	<b>Cancel</b>	Cancel the unlock schedule override.
	<b>Forgive antipassback violation</b>	Forgive an antipassback violation. This button is only available when there is an antipassback violation.
	<b>Reader (Shunt or Activate)</b>	Select the reader to either Shunt (deactivate) or Activate. This button is only available when your access control equipment supports reader shunting.

<sup>1</sup> If you hold Ctrl+Shift when clicking the command, the command applies to all doors displayed in the canvas.

### Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



# 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.

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.





# 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. For more information, see the *Security Center Administrator Guide*.
- If you require different groups of cardholders with different access rights, create cardholder groups in Config Tool. For more information, see the *Security Center Administrator Guide*.
- To modify the security clearance of a cardholder, you must be granted the *Change cardholder options* and *Modify security clearance* privileges.

### To create a cardholder:

- 1 Open the *Cardholder management* task, and click **New** (+).
- 2 At the top of the dialog box, enter the cardholder's first name and last name.
- 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 credentials to work, and for them to have access to any area, their status must be *Active*.
  - **Activation:** Set an activation for their profile:
    - **Never:** (Only available after a cardholder is deactivated) The date and time that you clicked **New** (+) to create the cardholder.
    - **Specific date:** Activates on a specific date and time.
  - **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 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 an item** (+). In the dialog box that opens, select the cardholder groups, and click **OK**.

- 8 Enter the cardholder's email address.  
A valid email address is necessary if you want to assign *mobile credentials* to the cardholder.
- 9 Enter the cardholder's mobile phone number.
- 10 (Optional) If custom fields are defined for cardholders, such as department, phone numbers, and so on, enter the additional cardholder information.

- 11 (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.
  - **Can escort visitors:** Indicates whether or not the cardholder can act as a visitor host.
  - **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, enter 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 users who have been granted access to the partition can see the cardholder.

- 12 Click **Save**.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## Related Topics

[Assigning access rules to cardholders](#) on page 77

[Assigning temporary access rules to cardholders](#) on page 79

## 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 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. If you need to grant temporary or short term access to a cardholder, create a temporary access rule.

**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 listing the access rules that are not yet assigned to this cardholder opens.
- 3 Do one of the following:
    - Select the rule you want to add, and click **Add**.
    - [Create and assign a temporary access rule](#).
  - 4 Select the access rule from the list.

The schedule that applies to the access rule is shown in a grid on the right. Each time block represents 30 minutes. Green areas indicate periods when access is granted by the rule. Red areas indicate periods when access is denied by the rule. Grey areas are times not specified by the schedule; therefore, access is denied. If it is a temporary access rule (🕒), the activation and expiration times are indicated. Areas, doors, and elevators that the rule is associated with are listed at the bottom.

The screenshot shows the 'Access rules' configuration for cardholder Charles Brymer. The 'IT Training' rule is selected. The interface includes a list of rules on the left, a grid for access rights overview, and a tooltip showing a 30-minute time block. The grid shows access granted (green) from 12:00 to 4:00 on Monday through Friday. The tooltip shows a 30-minute time block starting at 4:00 on Monday.

- 5 To view a partial (hatched) time block in minutes, click and hold the left mouse button.
  - 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**.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



**Related Topics**[Assigning credentials](#) on page 84[Creating cardholders](#) on page 76

## Assigning temporary access rules to cardholders

To accommodate seasonal cardholders, such as students who are enrolled during a semester, or permanent cardholders who need short term access to a restricted area, you can create and assign temporary access rules.

### What you should know

A temporary access rule is an access rule that has an activation and an expiration time. Temporary access rules are suited for situations where permanent cardholders need to have temporary or seasonal access to restricted areas. These access rules are automatically deleted seven days after they expire to avoid cluttering the system.

**NOTE:** From the *Cardholder management* task, you can only assign a temporary access rule to one cardholder at a time. To assign a temporary access rule to multiple cardholders or cardholder groups, you must update the access rule properties from Config Tool.

**To assign a temporary access rule 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 listing the access rules that are not yet assigned to this cardholder opens.
- 3 Do one of the following:
  - Select an existing temporary access rule (🔑) and click **Add**.
  - Click **Temporary access rule** (+).

The temporary access rule creation wizard opens.
- 4 In the *Basic information* page, enter the rule name and description, then click **Next**.
- 5 In the *Access rule information* page, do one of the following:
  - Click **Use an existing access rule as template**, then select from the **Access rule** drop-down list, the access rule you want to use as template.
  - The schedule and the associated entities will be copied to your temporary access rule.
  - Click **Specify custom access parameters**, and specify the following:
    - **Access to:** Expand the area view and select the entities you want to grant access to.
    - **Activation:** Activation date and time, or when the rule schedule starts to apply.
    - **Expiration:** Expiration date and time, or when the rule schedule stops to apply.
    - **Schedule:** Choose when this access rule is active.
- 6 Click **Next** > **Create**.
- A temporary access rule (🔑) is created and assigned to your cardholder.
- 7 Click **Save**.

### After you finish

(Optional) Assign the temporary access rule you created to other cardholders.

**Related Topics**[Creating cardholders](#) on page 76

## 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. You can either pre-register visitors for later check-in, or create a visitor and check them in immediately.

### 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 **New** (+).
- 3 At the top of the dialog box, enter the visitor's first name and last name.
- 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* date is the same as the check-in date. You can set the activation date to a date in the future, which allows you to create visitor profiles in advance.

  - **Status:** For a visitor's credentials to work, their status must be *Active*. You can set their status to *Active* immediately by clicking **Check in** (👤), and then **Save**.
  - **Activation:** Set an activation for their profile:
    - **Never:** The default value. Use this option when you plan to check in a visitor manually or you don't know when the visitor will be arriving.
    - **Specific date:** Expires on a specific date and time.
  - **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 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 define which access rules apply to the visitor.

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

**NOTE:** Only cardholder groups configured for visitors are listed. A visitor can belong to more than one cardholder group.

- b) To assign additional cardholder groups, click **Advanced** (+), then click **Add an item** (+). In the dialog box that opens, select the cardholder groups, and click **OK**.

## 9 Enter the visitor's email address.

## 10 Enter the visitor's mobile phone number.

## 11 (Optional) Assign one or two hosts (or escorts) to the visitor:

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

- a) Click the **Visitor host** list and select a cardholder as the visitor's host.

A dialog box opens displaying the message *Do you wish to automatically enable the Escort required option?*

- b) Click **Yes** to turn on the **Escort required** option.

When the option is on, the visitor is not allowed to access certain areas unless their assigned hosts also present their credentials after them within a certain delay.

- c) (Optional) To assign a second host, click **Advanced** (+), then click **Add an item** (+). In the dialog box that opens, select a cardholder to assign as host and click **OK**.

**NOTE:** The order in which the hosts present their credentials is not important.

12 (Optional) Enter a date and time into the **Expected arrival** field.

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

14 (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 users who have been granted access to the partition can see the visitor.

## 15 Do one of the following:

- To pre-register a visitor to be checked in later, click **Save**.
- To check in the visitor immediately, click **Save and check in**.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## 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 **New** (+).
- 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 opens, 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 check-in, expiration, or expected arrival 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 needed, and then do one of the following:
  - To pre-register a visitor to be checked in later, click **Save**.
  - To check in the visitor immediately, click **Save and check in** (👤).

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



### After you finish

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

#### Related Topics

[Assigning credentials](#) on page 84

## 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 find the visitor name.

**NOTE:** You can check out multiple visitors at the same time by holding down the shift key and selecting the visitors you want to check out.

- 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.

### Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



### Related Topics

[Investigating visitor events](#) on page 94



# Assigning credentials

---

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

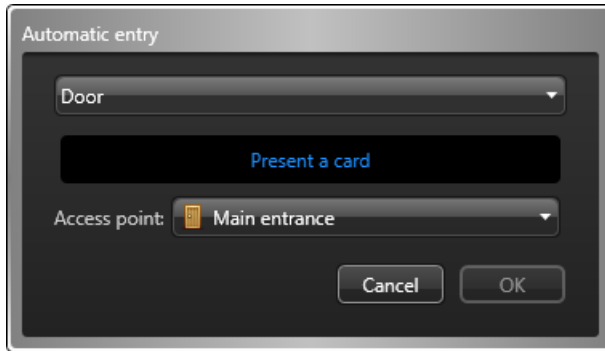
## What you should know

Cardholders and visitors can be assigned multiple *credentials*. You can assign credentials while you are creating a new cardholder or visitor (except for *mobile credentials*), or after they have been created. In this procedure, it is assumed you have already created the cardholders.

### To assign credentials:

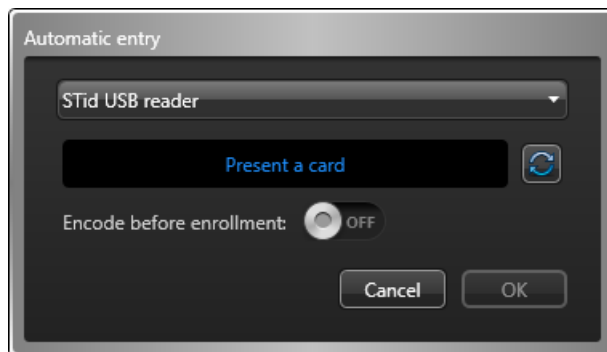
- 1 Do one of the following:
  - For cardholders, open the *Cardholder management* task, select a cardholder, and then click **Modify** (✎).
  - For visitors, open the *Visitor management* task, select a visitor, and then click **Modify** (✎).
- 2 In the *Credential* section, click **Add a credential** (+).
- 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.
  - **License plate:** Enter a cardholder's license plate number. Use this method if a Sharp camera is being used to trigger a vehicle access barrier. In this case, the cardholder's vehicle license plate can be used as a credential.
  - **Request card:** Request a credential card for the cardholder or visitor. Use this method if you do not have a printer on site.
  - **Mobile credential:** Request a mobile credential for the cardholder or visitor. You must have a mobile credential provider set up and mobile credential readers installed. The cardholder must have a valid email address configured.
  - **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.



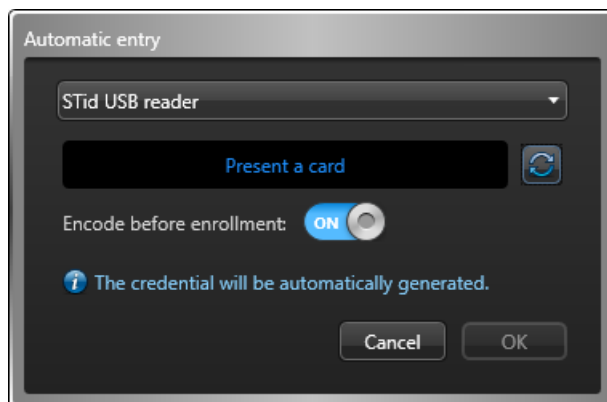
If you have a smart card encoding reader set up, do one of the following:

- To read a pre-encoded card, set the option **Encode before enrollment** to **OFF**. When the reader LED turns green (ready to read), place the smart card on the reader. The reader LED turns yellow and then green with a short beep before turning off.



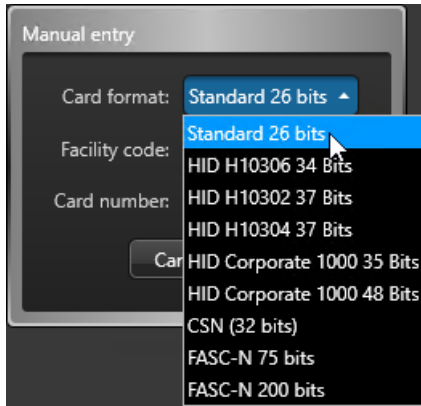
- To generate and encode on your card a random 128-bit MIFARE DESFire credential before enrolling it, set the option **Encode before enrollment** to **ON**. When the reader LED turns red (ready to encode), place the smart card on the reader for approximately 2 seconds. The reader LED turns yellow and then green with a short beep before turning off. If you hear a long beep and the LED stays red, try again.

**NOTE:** Your Security Center license must support smart card encoding.



The dialog box closes automatically after an eligible card is presented. If the card has not been enrolled, it is enrolled automatically. If the card was already assigned to someone, it is rejected.

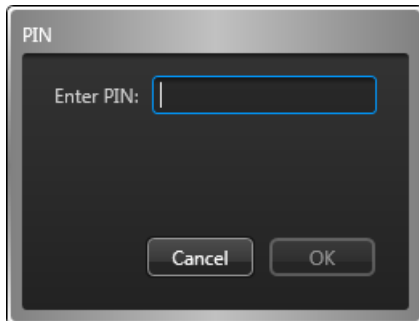
- 5 If you select **Manual entry**, you must then select a card format, enter the required data fields, and click **OK**.



**CAUTION:** Enter your card data carefully because the system cannot validate whether the data you entered correspond to a physical card or not.

If the card has not been enrolled, it is enrolled automatically. If the card was already assigned to someone, it is rejected.

- 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**, do the following:

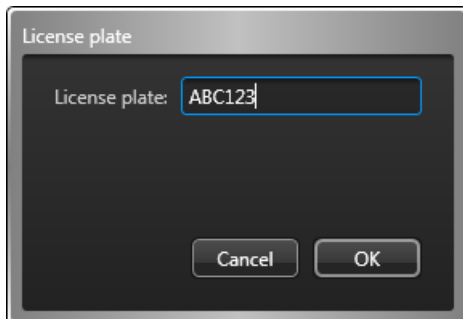


- a) Enter the PIN as a numerical value.

**NOTE:** Do not 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 If you select **License plate**, you must then do the following:

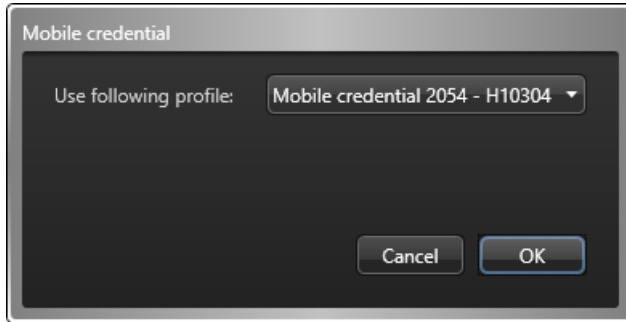


- a) Enter the license plate number.

**NOTE:** You do not need to enter spaces that appear in the license plate number. The system treats "ABC123" and "ABC 123" as the same plate.

- b) Click **OK**.

- 9 If you select **Mobile credential**, you must then do the following:



- a) Select the credential profile (if there is more than one).  
You can assign one mobile credential from each profile to the cardholder.
- b) Click **OK**.

**NOTE:** An email invitation is sent to the cardholder with a link to download the mobile credential app. The cardholder must accept the invitation for the credential to be *activated* on their phone. If the cardholder declines the invitation or if the invitation times out, the credential remains *unused*, and the mobile credential provider can assign it to the next cardholder who needs one. Security Center does not know that the requested mobile credential has not been accepted by the cardholder until the same mobile credential is assigned to someone else, at which time, Security Center automatically removes it from the current cardholder.

**IMPORTANT:** A mobile credential that has been activated (paired to a phone) can never be reused on another phone. If a cardholder loses their phone or needs to change their phone, they must inform the Security Center operator who must delete the credential or flag it as *lost*. After that, the operator must log on to the credential provider's portal and *revoke* the mobile credential.

- 10 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 license plate, a license plate 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.

- 11 (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 more 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.

- 12 Click **Save**.

You must save all your changes before you can print the badge.

- 13 To print the badge, click **Print badge** next to the badge preview.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.






## 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.

## Printing credential cards in batches

To save time when printing credential cards, you can print them in batches.

### What you should know

All the credentials you select must be associated with a badge template.

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

#### To print credential cards in batches:

- 1 From the home page, open the *Credential management* task.

- 2 Select the credentials you want to print:
  - Hold Ctrl and click specific credentials in the list.
  - Hold Shift and select a range of credentials in the list.
- 3 Click **Print**.

The selected credentials are printed in the order in which they are listed in the *Credential management* task.

## 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 usually associated with 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 creating a new cardholder or visitor, or after they are 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)**.
- 4 In the **Badge printing** dialog box, select a badge from the list.
 

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.

#### 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** 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.

### Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## 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.



# 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), 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:** Specify a time range during which the cardholder profile activates.
  - **Expiration date:** Specify a time range during which the cardholder or visitor profile expires.
  - **Unused cardholders:** Search for cardholder or visitors for whom no assigned credentials have produced an *access granted* event within a certain time range.

**NOTE:** For the report to generate results, all Access Manager roles must be active and online.

  - **Status:** The status of the cardholder or visitor's profile: *Active*, *Expired*, or *Inactive*.
  - **First name:** Cardholder or visitor's first name.
  - **Last name:** Cardholder or visitor's last name.
  - **Email address:** Cardholder or visitor's email address.
  - **Mobile phone number:** Cardholder or visitor's mobile phone number.
  - **Description:** Restrict the search to entries that contain this text string.
  - **Picture:** Whether or not the cardholder or visitor has a picture assigned.
  - **Partition:** Partition that the entity is a member of.
  - **Cardholder groups:** Restrict the search to specific cardholder groups.
  - **Credential name:** Credential's name.
  - **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, card numbers, or license plates.
  - **Custom fields:** Restrict the search to a predefined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
  - **Can escort visitors:** Indicates whether or not the cardholder can act as a visitor host (can be switched on or off).
- 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 .

### Related Topics

[How to generate reports in Security Desk](#) on page 19

# 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:
  - **Unused credentials:** Search for credentials that have not produced an *access granted* event within a certain time range.  
**NOTE:** For the report to generate results, all Access Manager roles must be active and online.
  - **Credential:** Specify whether or not the credential is assigned.
  - **Cardholders:** Restrict the search to specific cardholders, cardholder groups, or visitors.
  - **Credential information:** Restrict the search to specific card formats, facility codes, card numbers, or license plates.
  - **Status:** The status of the cardholder or visitor's profile: *Active, Expired, Inactive, Lost, Stolen*.
- 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 .

## Related Topics

[How to generate reports in Security Desk](#) on page 19


## 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.

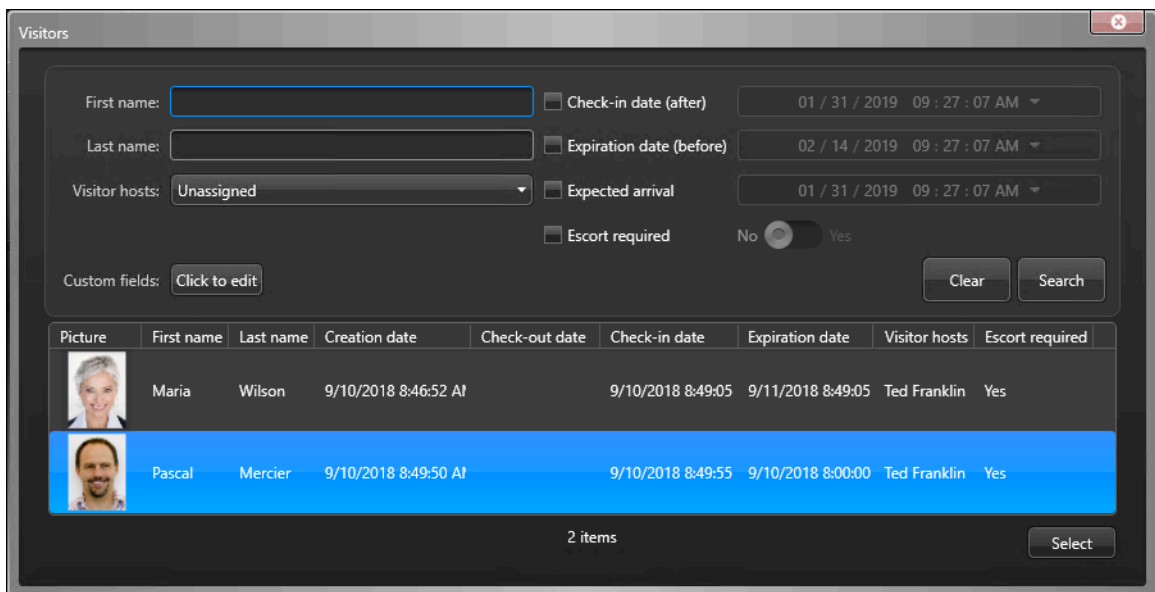
### What you should know



In Security Desk, you can see all the areas and doors that a visitor accessed during their stay. If you want to check for 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 in one of the following ways:
  - Type a visitor's first name or last name, and then click **Search**.
  - Select the visitor's activation, expiration, or expected arrival date, and then click **Search**.
  - Select the visitor's host, 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.



Picture	First name	Last name	Creation date	Check-out date	Check-in date	Expiration date	Visitor hosts	Escort required
	Maria	Wilson	9/10/2018 8:46:52 AM		9/10/2018 8:49:05	9/11/2018 8:49:05	Ted Franklin	Yes
	Pascal	Mercier	9/10/2018 8:49:50 AM		9/10/2018 8:49:55	9/10/2018 8:00:00	Ted Franklin	Yes

- 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 predefined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
  - **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 or for global time units, such as the previous week or the previous 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 connected to the entity, the door, elevator, or area icons are displayed, depending on the type of visitor event.

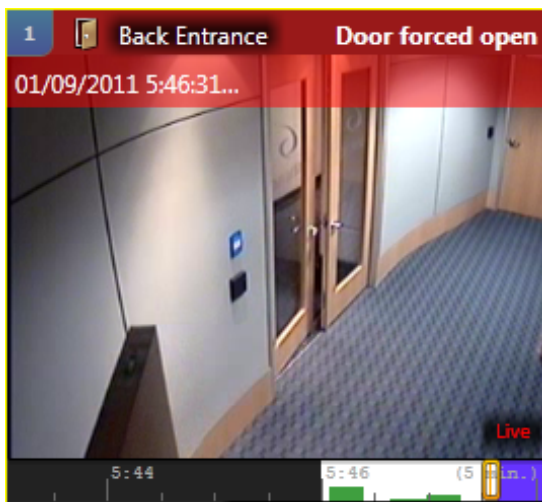
9 To control the tiles, use the widgets in the *Controls* pane.

## 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

- For the **Override unlock schedules** button in the *Door* widget to be enabled, you must have the *Modify door properties* privilege.
- 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 with 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:

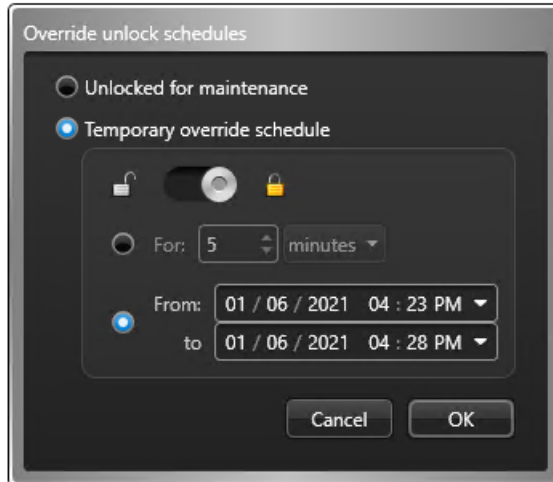
- 1 From the *Monitoring* task, select a tile that is displaying a door. The *Door* widget is displayed in the *Controls* pane.

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 of the following:



- **Unlocked 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 a specified period of time, either immediately or in the future. With this option, the door returns to its normal state after the time expires.

3 Click **OK**.

## 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.

# 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 specific cardholders, cardholder groups, or visitors.
  - **Credential:** Restrict the search to specific credentials.
  - **Custom fields:** Restrict the search to a predefined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
  - **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 or for global time units, such as the previous week or the previous 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

Using the *Door Activities* report, you can see how many access denied events have occurred in the last week, or since your last shift. You can also search for other critical events, such as *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 verify that maintenance staff has completed work at a particular door, you can investigate on that door by selecting the *Door maintenance completed* event.

## Related Topics

[How to generate reports in Security Desk](#) on page 19

# Monitoring alarms

This section includes the following topics:

- ["About alarms"](#) on page 100
- ["How alarms are displayed in the Security Desk canvas"](#) on page 102
- ["Alarm widget"](#) on page 103
- ["Enabling alarm monitoring in the Monitoring task"](#) on page 105
- ["Acknowledging alarms"](#) on page 107
- ["Filtering and grouping alarms in Security Center"](#) on page 109
- ["Forwarding alarms to other users automatically"](#) on page 112
- ["Forwarding alarms to other users manually"](#) on page 113
- ["Triggering alarms manually"](#) on page 114
- ["Investigating current and past alarms"](#) on page 115
- ["Overview of the Alarm monitoring task "](#) on page 117
- ["Overview of the Alarm report task "](#) on page 118

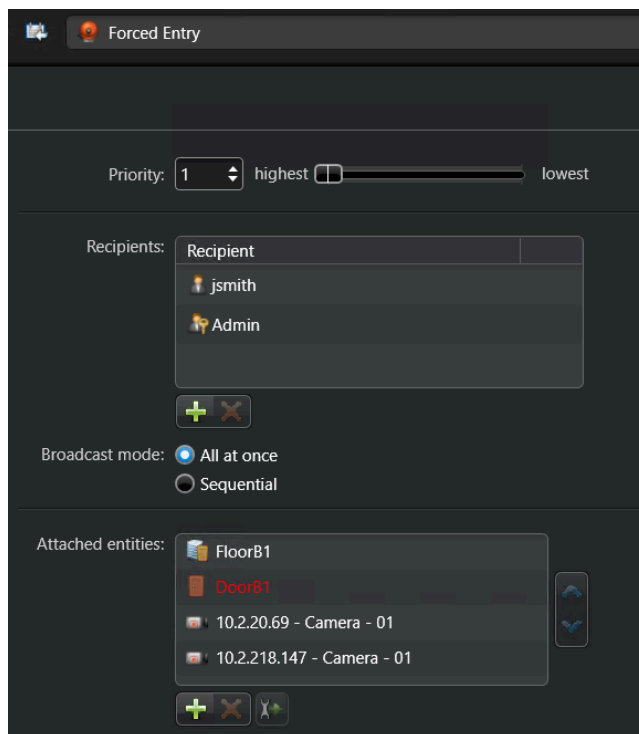


## About alarms

An alarm entity describes a particular type of 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 the situation, who must be notified, how it must be displayed to the user, and so on.

The basic properties of an alarm are:

- **Name:** Alarm name.
- **Priority:** Priority of the alarm (1-255), based on the urgency of the situation. Higher priority alarms are displayed first in Security Desk.
- **Recipients:** Users, user groups, and analog monitor groups who are notified when the alarm occurs, and are responsible for responding to the alarm situation.
- **Broadcast mode:** How the alarm recipients are notified about the alarm.
  - **All at once:** (Default) All recipients are notified at the same time, immediately after the alarm is triggered.
  - **Sequential:** The recipients are notified individually, each after a specified delay (in seconds) calculated from the time the alarm is triggered. If the recipient is a user group, all members of the user group are notified at the same time.
- **Attached entities:** Entities that help describe the alarm situation (for example, cameras, area, doors, alarm procedure, and so on). When the alarm is received in Security Desk, the attached entities can be displayed one after another in a sequence or all at once in the *canvas*, to help you review the situation. If a composite entity is attached to the alarm, the entities that compose it are also attached to the alarm. For example, if a door entity is attached to the alarm, the cameras associated to the door are also attached to the alarm.



### Alarm priority

In Security Desk, alarms are displayed in the *Alarm monitoring* task and the *Monitoring* task by order of priority (this is evaluated every time a new alarm is received). The highest priority alarm is displayed in tile #1,

followed by the second highest in tile #2, and so on. When two alarms have the same priority value, priority is given to the newest one.

When a new alarm is received in Security Desk with a priority level identical or higher than the current alarms displayed, it pushes the other alarms down the tile list.

When an alarm is *acknowledged* in Security Desk, it frees a tile for lower priority alarms to move up.

## Video recording on alarms

When an alarm is triggered that has cameras attached to it, you can make sure that the video related to the alarm is recorded and available for future alarm investigations.

The amount of time that the video is recorded for (called the *guaranteed recording span*) is defined by two settings:

- **The alarm recording duration:** Number of seconds that the Archiver records video for after the alarm is triggered. This option (*Automatic video recording*) is set in the alarm *Advanced* tab.
- **The recording buffer:** Number of seconds that the Archiver records video for before the alarm was triggered, to make sure that whatever triggered the alarm is also recorded. This option (*Time to record before an event*) is set in the Archiver *Camera default settings* tab, or for each camera individually.

If an alarm is triggered from a camera event (for example *Object removed*), then the camera that caused the event is also attached to the alarm and starts recording.

**IMPORTANT:** The recordings are dependent on the archiving schedules. If recording is disabled when the alarm is triggered, no video is recorded.

## How alarms are displayed in the Security Desk canvas

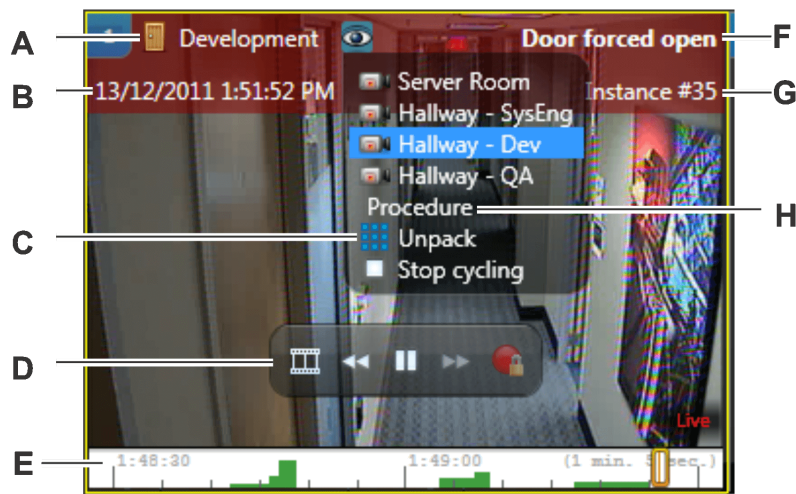
You can view active and past alarms in the canvas in the *Alarm monitoring* task, the *Alarm report* task, and the *Monitoring* task.

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.

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.



<b>A</b>	Source of the alarm
<b>B</b>	Alarm timestamp
<b>C</b>	Allows you to view all attached entities at once
<b>D</b>	On-tile video controls
<b>E</b>	Timeline
<b>F</b>	Alarm name
<b>G</b>	Alarm instance number
<b>H</b>	Displays the alarm procedure if it is defined

### Related Topics

[Unpacking content in tiles](#) on page 25

## 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 a triggered alarm requires an acknowledgment 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 acknowledgment 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
	<b>Acknowledge (Default)</b> <sup>1</sup>	Acknowledge the alarm. The alarm is no longer active, and is removed from the canvas and the alarm list.
	<b>Acknowledge (Alternate)</b> <sup>1</sup>	Set the alarm to the <i>alternate</i> acknowledged state. The reasons for using this acknowledgment 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.
	<b>Forcibly acknowledge</b> <sup>1</sup>	Force the alarm to be acknowledged. This is helpful for clearing alarms that are currently under investigation and their acknowledgment condition is not yet cleared.
	<b>Investigate</b>	Investigate the alarm. This action lets other users in the system know that you have seen the alarm without acknowledging it, so the alarm is not removed from the active alarm list.
	<b>Snooze alarm</b> <sup>1</sup>	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 <i>Options</i> dialog box.
	<b>Forward alarm</b> <sup>1</sup>	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.
	<b>Show alarm procedure</b>	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.

<sup>1</sup> 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 112

[Forwarding alarms to other users manually](#) on page 113

## 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

When tiles are armed to monitor alarms in the *Monitoring* task, alarms are no longer displayed as pop-up windows in the notification tray. For more information about configuring alarms as pop-ups, see the *Security Center User Guide*.

#### To enable alarm monitoring in the Monitoring task:

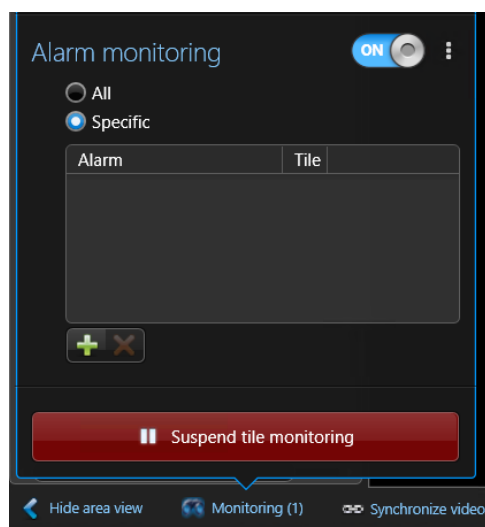
- 1 Open the *Monitoring* task.
- 2 At the bottom of the *Monitoring* task, click **Monitoring** (🔊).
- 3 Switch the **Alarm monitoring** option to **ON**.

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.
- 5 If you selected **Specific**, do the following:
  - 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. If you cannot see the **Events/Alarms** toggle button, drag the top of the canvas down to expose the alarm list that appears at the top of the screen.

You can pause tile monitoring at any time by clicking **Suspend tile monitoring**.

### Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



# Acknowledging alarms

---

You can view and acknowledge the alarms from the *Alarm monitoring* and the *Monitoring* task.

## Before you begin




To view and acknowledge alarms from the *Monitoring* task, you [must enable alarm monitoring for that Monitoring task](#).

## What you should know

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 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 acknowledgment required:** Show alarms where their acknowledgment 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 colored overlay that provides the alarm details.
- 4 In the widget, 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 acknowledgment 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.
- **Investigate** (🔍): Investigate the alarm. This action lets other users in the system know that you have seen the alarm without acknowledging it, so the alarm is not removed from the active alarm list.
- **Forcibly acknowledge** (👉): Force the alarm to be acknowledged. This is helpful for clearing alarms that are currently under investigation and their acknowledgment condition is not yet cleared.
- **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 acknowledgment condition is not yet cleared.
- **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.
- **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.
- **Edit context** (✎): Add or modify the alarm annotation.

**NOTE:** All actions on the alarms are logged in the activity trail.

## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## Related Topics

[How alarms are displayed in the Security Desk canvas](#) on page 102

[Overview of the Alarm monitoring task](#) on page 117

## Filtering and grouping alarms in Security Center

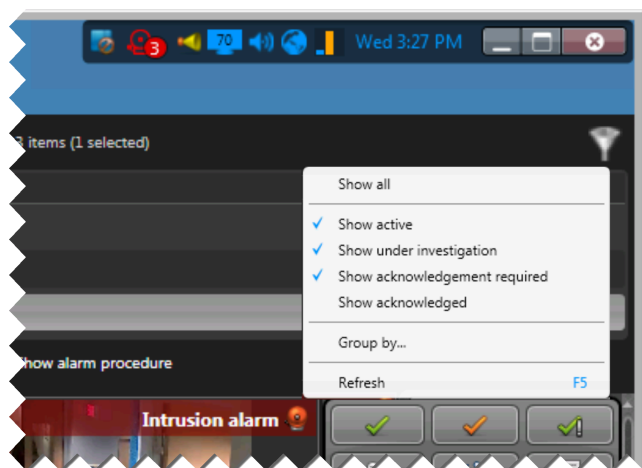
You can filter and group alarms to control how they appear in the *Alarm monitoring* task and the *Monitoring* task.

### 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** toggle button, drag the top of the canvas down to expose the alarm list that appears at the top of the screen.



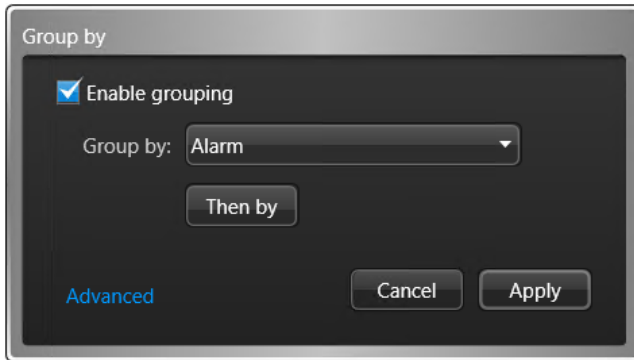
- 2 Select or clear the following filters:
  - **Show all:** Display all alarms (no filter).
  - **Show active:** Show active alarms.
  - **Show under investigation:** Show alarms that are currently under investigation.
  - **Show acknowledgment required:** Show alarms where their acknowledgment conditions are cleared but they must still be acknowledged.
  - **Show acknowledged:** Show acknowledged alarms.

### To group alarms:

- 1 In the *Alarm monitoring* task or the *Monitoring* task, right-click a column heading 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 **Events/Alarms** button, drag the top of the canvas down to expose the alarm list that appears at the top of the screen.



- In the *Group by* dialog box, select **Enable grouping**.

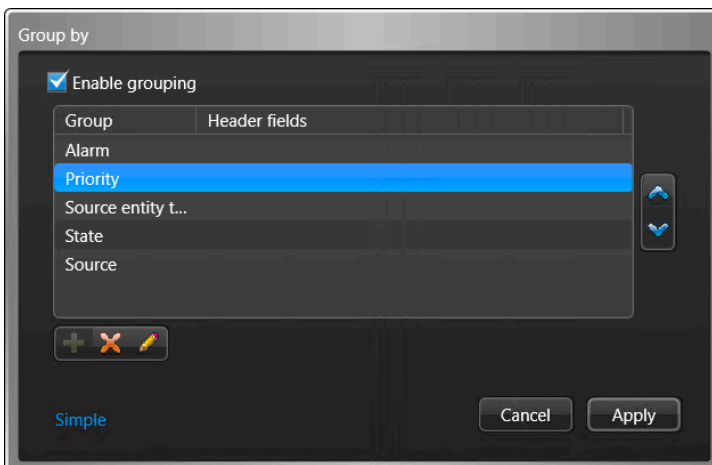


- From the drop-down list, select the highest level of grouping you would like to apply to the alarms.

You can group the alarms by:

- **Alarm:** Alarm entity name.
- **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:** Source entity that triggered the alarm. It is the event source if the alarm is triggered by an event-to-action, or the user, if the event is triggered manually. The source is not shown if you do not have permission to access the source entity.
- **Source entity type:** The source entity type that triggered the alarm, when the alarm is triggered by an event-to-action. It shows **User** when the alarm is triggered 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 (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 that is under investigation, meaning that someone has seen it but not necessarily able to take care of it.
  - **Acknowledgment required:** Alarm with an acknowledgment condition that was cleared and that is ready to be acknowledged.

- To apply additional grouping levels, select **Then by**.
- Click **Advanced**.
- To change the grouping order, select a group, and then use the  and  arrows.



- 7 To show alarm information in the header of the group, do the following:
  - a) Select a group, and then click **Edit the item** (✎).
  - b) Select the alarm columns you want to show.
  - c) To change the column order of appearance, use the ⬆️ and ⬇️ arrows.
  - d) Click **OK**.
- 8 Click **Apply**.

### Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



# 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**.

## 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.
- The alarm cannot be set to maintenance mode.
- 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.

## Investigating current and past alarms

---

You can search for and investigate current and past alarms, using the *Alarm report* task.

### What you should know

In Security Desk, you can investigate all of the alarms that were triggered during the last week or since your last shift. You can also investigate major events that happened in your system (by only selecting critical alarms), who acknowledged a specific alarm, and why. You can also review the video associated to an alarm, which can then be exported and sent 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:
  - **Alarms:** Select the types of alarms you want to investigate. Alarms can be locally defined (🔴), or imported from federated systems (🟡).
  - **Acknowledged by:** Users who acknowledged the alarm.
  - **Acknowledged on:** Alarm acknowledgment time range.
  - **Acknowledgment type:**

Select one of the following acknowledgment 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.
  - **Context:** Restrict the search to alarms with a specific text in the annotation. The search is case insensitive.
  - **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 that is under investigation.
    - **Acknowledgment required:** Alarm with an acknowledgment condition that was cleared is ready to be acknowledged.
  - **Triggered on:** Alarm trigger time range.
  - **Triggering event:** Events used to trigger the alarm.
  - **Custom fields:** Restrict the search to a predefined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
- 3 Click **Generate report**.
 

The 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.



## Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



## Related Topics

[How to generate reports in Security Desk](#) on page 19

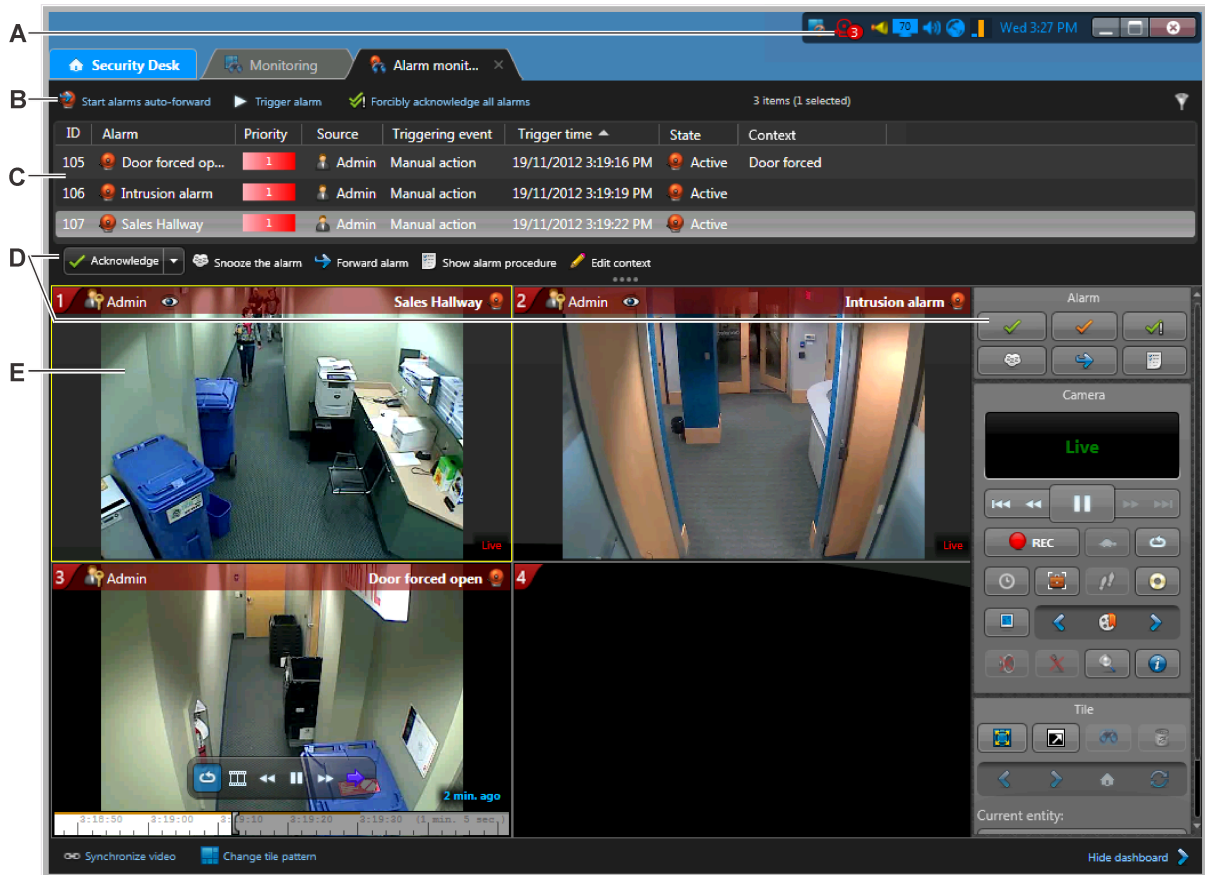
[How alarms are displayed in the Security Desk canvas](#) on page 102

[Alarm widget](#) on page 103

# 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.
- 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**.

Right-click an alarm to go to the configuration page of the alarm or its source entity.

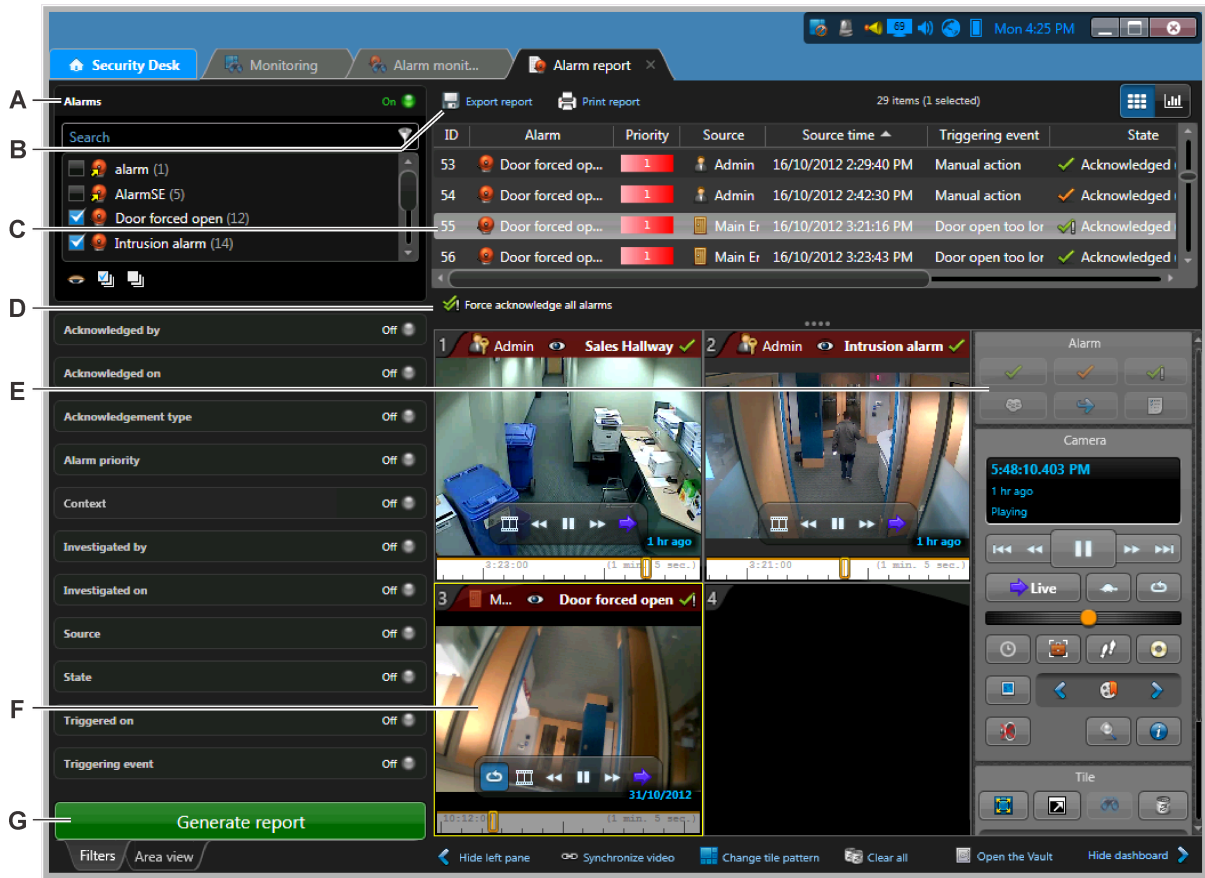
**D** Commands to control active alarms. Click the **Acknowledge** drop-down list to see all available commands.

**E** Video of an alarm in a tile. The video is displayed with a colored overlay with details of the alarm.



# 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** Click  to export or  to print the report.

**C** The alarm report results are listed in the report pane.

Right-click an alarm to go to the configuration page of the alarm or its source entity.

**D** 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 103

[Alarm widget](#) on page 103

[Investigating current and past alarms](#) on page 115

[How alarms are displayed in the Security Desk canvas](#) on page 102

# Glossary

<b>authorized user</b>	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.
<b>Access control health history</b>	The <i>Access control health history</i> task is a maintenance task that reports on events related to the health of access control entities. Unlike the events in the <i>Health history</i> report, the events in the <i>Access control health history</i> report are not generated by the Health Monitor role, identified by an event number, or categorized by severity.
<b>access control unit</b>	An access control unit entity 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.
<b>Access control unit events</b>	The <i>Access control unit events</i> task is a maintenance task that reports on events pertaining to selected access control units.
<b>Access Manager</b>	The Access Manager role manages and monitors access control units on the system.
<b>access point</b>	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.
<b>access right</b>	An access right is the basic right users must have over any part of the system before they can do anything with it. Other rights, such as viewing and modifying entity configurations, are granted through privileges. In the context of a Synergis™ system, an access right is the right granted to a cardholder to pass through an access point at a given date and time.
<b>access rule</b>	An access rule entity defines a list of cardholders to whom access is either granted or denied based on a schedule. Access rules can be applied to secured areas and doors for entries and exits, or to intrusion detection areas for arming and disarming.
<b>Access rule configuration</b>	The <i>Access rule configuration</i> task is a maintenance task that reports on entities and access points affected by a given access rule.
<b>Access troubleshooter</b>	Access troubleshooter is a tool that helps you detect and diagnose access configuration problems. With this tool, you can find out about the following:

- Who is allowed to pass through an access point at a given date and time
- Which access points a cardholder is allowed to use at a given date and time
- Why a given cardholder can or cannot use an access point at a given date and time

<b>action</b>	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.
<b>active alarm</b>	An active alarm is an alarm that has not yet been acknowledged.
<b>Active Directory</b>	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.
<b>Activity trails</b>	The <i>Activity trails</i> task is a maintenance task that reports on the user activity related to video, access control, and ALPR 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.
<b>Advanced Systems Format</b>	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.
<b>agent</b>	An agent is a subprocess created by a Security Center role to run simultaneously on multiple servers for the purpose of sharing its load.
<b>alarm</b>	An alarm entity describes a particular type of 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 the situation, who must be notified, how it must be displayed to the user, and so on.
<b>alarm acknowledgement</b>	An alarm acknowledgement is a user's response to an alarm. In Security Center, the default and the alternative acknowledgement are the two variants of alarm acknowledgements. Each variant is associated to a different <i>event</i> so that specific actions can be programmed based on the alarm response selected by the user.
<b>Alarm monitoring</b>	The <i>Alarm monitoring</i> task is an operation task that you can use to monitor and respond to alarms (acknowledge, forward, snooze, and so on) in real time, and to review past alarms.
<b>Alarm report</b>	The <i>Alarm report</i> task is an investigation task that you can use to search and view current and past alarms.

<b>analog monitor</b>	An analog monitor entity 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.
<b>antipassback</b>	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.
<b>Archiver</b>	The Archiver role is responsible for the discovery, status polling, and control of video units. The Archiver also manages the video archive and performs motion detection if it is not done on the unit itself.
<b>Archiver events</b>	The <i>Archiver events</i> task is a maintenance task that reports on events pertaining to selected Archiver roles.
<b>Archives</b>	The <i>Archives</i> task is an investigation task that you can use to find and view video archives by camera and time range.
<b>Archive storage details</b>	The <i>Archive storage details</i> task is a 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. Using this task, you can also change the protection status of these video files.
<b>archive transfer</b>	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.
<b>area</b>	In Security Center, an area entity represents a concept or a physical location (room, floor, building, site, and so on) used for grouping other entities in the system.
<b>Area activities</b>	The <i>Area activities</i> task is an investigation task that reports on access control events pertaining to selected areas.
<b>Area presence</b>	The <i>Area presence</i> is an investigation task that provides a snapshot of all cardholders and visitors currently present in a selected area.
<b>area view</b>	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.
<b>asset</b>	An asset entity represents any valuable object with an RFID tag attached, thus allowing it to be tracked by an asset management software.
<b>asynchronous video</b>	Asynchronous video is simultaneous playback video from more than one camera that are not synchronized in time.

<b>audio decoder</b>	An audio decoder is a device or software that decodes compressed audio streams for playback. Synonym of <i>speaker</i> .
<b>audio encoder</b>	An audio encoder is a device or software that encodes audio streams using a compression algorithm. Synonym of <i>microphone</i> .
<b>Audit trails</b>	The <i>Audit trails</i> task is a maintenance task that reports on the configuration changes of the selected entities in the system. The report also indicates the user who made the changes.
<b>automatic enrollment</b>	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.
<b>automatic license plate recognition</b>	Automatic license plate recognition (ALPR) is an image processing technology used to read license plate numbers. ALPR converts license plate numbers cropped from camera images into a database searchable format.
<b>AutoVu™</b>	The AutoVu™ automatic license plate recognition (ALPR) system automates license plate reading and identification, making it easier for law enforcement and for municipal and commercial organizations to locate vehicles of interest and enforce parking restrictions. Designed for both fixed and mobile installations, the AutoVu™ system is ideal for a variety of applications and entities, including law enforcement, municipal, and commercial organizations.
<b>Auxiliary Archiver</b>	The Auxiliary Archiver role supplements the video archive produced by the Archiver role. Unlike the Archiver role, the Auxiliary Archiver role 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 role cannot operate independently; it requires the Archiver role to communicate with video units.
<b>Badge designer</b>	The Badge designer is the tool that you can use to design and modify badge templates.
<b>badge template</b>	A badge template is an entity used to configure a printing template for badges.
<b>bookmark</b>	A bookmark is an indicator of an event or incident that is used to mark a specific point in time in a recorded video sequence. A bookmark also contains a short text description that can be

	used to search for and review the video sequences at a later time.
<b>Bookmarks</b>	The <i>Bookmarks</i> task is an investigation task that searches for bookmarks related to selected cameras within a specified time range.
<b>broadcast</b>	Broadcast is the communication between a single sender and all receivers on a network.
<b>camera</b>	A camera entity represents a single video source in the system. The video source can either be an IP camera, or an analog camera that connects to the video encoder of a video unit. Multiple video streams can be generated from the same video source.
<b>camera blocking</b>	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.
<b>Camera configuration</b>	The <i>Camera configuration</i> task is a maintenance task that reports on the properties and settings of local cameras in your system (manufacturer, resolution, frame rate, stream usage, and so on).
<b>Camera events</b>	The <i>Camera events</i> task is an investigation task that reports on events pertaining to selected cameras within a specified time range.
<b>camera sequence</b>	A camera sequence is an entity that defines a list of cameras that are displayed one after another in a rotating fashion within a single tile in Security Desk.
<b>canvas</b>	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.
<b>Card and PIN</b>	Card and PIN is an access point mode that requires a cardholder to present their card, and then enter a personal identification number (PIN).
<b>cardholder</b>	A cardholder entity represents a person who can enter and exit secured areas by virtue of their credentials (typically access cards) and whose activities can be tracked.
<b>Cardholder access rights</b>	The <i>Cardholder access rights</i> task is a maintenance task that reports on which cardholders and cardholder groups are granted or denied access to selected areas, doors, and elevators.



<b>Cardholder activities</b>	The <i>Cardholder activities</i> task is an investigation task that reports on cardholder activities, such as access denied, first person in, last person out, antipassback violation, and so on.
<b>Cardholder configuration</b>	The <i>Cardholder configuration</i> is a maintenance task that reports on cardholder properties, such as first name, last name, picture, status, custom properties, and so on.
<b>cardholder group</b>	A cardholder group is an entity that defines the common access rights of a group of cardholders.
<b>Cardholder management</b>	The <i>Cardholder management</i> task is an operation task. You can use this task to create, modify, and delete cardholders. With this task, you can also manage a cardholders' credentials, including temporary replacement cards.
<b>cash register</b>	A cash register entity represents a single cash register (or terminal) in a point of sale system.
<b>certificate</b>	Designates one of the following: (1) <i>digital certificate</i> ; (2) <i>SDK certificate</i> .
<b>Config Tool</b>	Config Tool is the Security Center administrative application used to manage all Security Center users and to configure all Security Center entities such as areas, cameras, doors, schedules, cardholders, patrol vehicles, ALPR units, and hardware devices.
<b>Conflict resolution utility</b>	The Conflict resolution utility is a tool that helps you resolve conflicts caused by importing users and cardholders from an Active Directory.
<b>controlled exit</b>	A controlled exit is when credentials are necessary to leave a secured area.
<b>controller module</b>	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.
<b>Copy configuration tool</b>	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.
<b>credential</b>	A credential entity 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.
<b>Credential activities</b>	The <i>Credential activities</i> task is an investigation task that reports on credential related activities, such as access denied due to expired, inactive, lost, or stolen credentials, and so on.
<b>credential code</b>	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.
<b>Credential configuration</b>	The <i>Credential configuration</i> task is a maintenance task that reports on credential properties, such as status, assigned cardholder, card format, credential code, custom properties, and so on.
<b>Credential management</b>	The <i>Credential management</i> task is an operation task. You can use this task to create, modify, and delete credentials. With this task, you can also 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.
<b>Credential request history</b>	The <i>Credential request history</i> task is an investigation task that reports on which users requested, canceled, or printed cardholder credentials.
<b>custom event</b>	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.
<b>custom field</b>	A custom field is a user-defined property that is associated with an entity type and is used to store additional information that is useful to your organization.
<b>database server</b>	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.
<b>debounce</b>	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 (in milliseconds).
<b>degraded mode</b>	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 HID VertX interface modules can operate in degraded mode.
<b>dependent mode</b>	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.
<b>dewarping</b>	Dewarping is the transformation used to straighten a digital image taken with a fisheye lens.

<b>digital signature</b>	A digital signature is cryptographic metadata added to video frames by the Archiver or Auxiliary Archiver to ensure their authenticity. If a video sequence is manipulated by adding, deleting, or modifying frames, the signature of the modified content will differ from the original, indicating that the video sequence has been tampered with.
<b>Directory</b>	The Directory role identifies a Security Center system. It manages all entity configurations and system-wide settings. 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.
<b>Directory Manager</b>	The Directory Manager role manages the Directory failover and load balancing to produce the high availability characteristics in Security Center.
<b>Directory server</b>	A Directory server is any one of the multiple servers simultaneously running the Directory role in a high availability configuration.
<b>discovery port</b>	A discovery port is a port used by certain Security Center roles (Access Manager, Archiver, ALPR Manager) to find the units they are responsible for on the LAN. No two discovery ports can be the same on one system.
<b>door</b>	A door entity 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.
<b>Door activities</b>	The <i>Door activities</i> task is an investigation task that generates reports on door-related activities, such as access denied, door forced open, door open too long, hardware tamper, and so on.
<b>door contact</b>	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.
<b>door side</b>	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.
<b>Door troubleshooter</b>	The <i>Door troubleshooter</i> task is a maintenance task that lists all the cardholders who have access to a particular door side or elevator floor at a specific date and time.

<b>Driver Development Kit</b>	Driver Development Kit is a SDK for creating device drivers.
<b>duress</b>	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.
<b>edge recording</b>	Edge recording is the process of recording and storing recorded videos on the peripheral device, 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 (SD card) or on a network attached storage volume (NAS volume).
<b>electric door strike</b>	An electric door strike is an electric device that releases the door latch when current is applied.
<b>elevator</b>	An elevator is an entity that provides access control properties to elevators. For an elevator, each floor is considered an access point.
<b>Elevator activities</b>	The <i>Elevator activities</i> task is an investigation task that reports on elevator related activities, such as access denied, floor accessed, unit is offline, hardware tamper, and so on.
<b>enforce</b>	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.
<b>entity</b>	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.
<b>entity tree</b>	An entity tree is the graphical representation of Security Center entities in a tree structure, illustrating the hierarchical nature of their relationships.
<b>event</b>	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. Every event has an entity as its main focus, called the event source.
<b>event-to-action</b>	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.
<b>expansion server</b>	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.

<b>failover</b>	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 if the primary server becomes unavailable, either through failure or through scheduled downtime.
<b>federated entity</b>	A federated entity is any entity that is imported from an independent system through one of the Federation™ roles.
<b>federated system</b>	A federated system is a independent system (Omnicast™ or Security Center) that is unified under your local Security Center through a Federation™ role, so that the local users can view and control its entities as if they belong to their local system.
<b>Federation™</b>	The Federation™ feature joins multiple, independent Genetec™ IP security systems into a single virtual system. With this feature, users on the central Security Center system can view and control entities that belong to remote systems.
<b>Forensic search</b>	The <i>Forensic search</i> task is an investigation task that searches for video sequences based on video analytics events stored in Bosch units.
<b>four-port RS-485 module</b>	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.
<b>free access</b>	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.
<b>free exit</b>	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.
<b>G64</b>	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.
<b>Genetec™ Server</b>	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.

<b>Genetec™ Video Player</b>	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.
<b>ghost camera</b>	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.
<b>Geographic Information System</b>	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.
<b>Global Cardholder Synchronizer</b>	The Global Cardholder Synchronizer role ensures the two-way synchronization of shared cardholders and their related entities between the local system (sharing guest) where it resides and the central system (sharing host).
<b>global entity</b>	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.
<b>global partition</b>	Global partition is a partition that is shared across multiple independent Security Center systems by the partition owner, called the sharing host.
<b>hardware integration package</b>	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.
<b>Hardware inventory</b>	The <i>Hardware inventory</i> task is a 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 ALPR units in your system.
<b>hardware zone</b>	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.
<b>Health history</b>	The <i>Health history</i> task is a maintenance task that reports on health issues.
<b>Health Monitor</b>	The Health Monitor role monitors system entities such as servers, roles, units, and client applications for health issues.

<b>Health statistics</b>	The <i>Health statistics</i> task is a maintenance task that gives you an overall view of the health of your system by reporting on the availability of selected system entities such as roles, video units, and doors.
<b>High availability</b>	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.
<b>hot action</b>	A hot action is an action mapped to a PC keyboard function key (Ctrl+F1 through Ctrl+F12) in Security Desk for quick access.
<b>hotspot</b>	A hotspot is a map object that represents an area on the map which requires special attention. Clicking on a hotspot displays associated fixed and PTZ cameras.
<b>identity provider</b>	An identity provider is a trusted, external system that administers user accounts, and is responsible for providing user authentication and identity information to relying applications over a distributed network.
<b>Import tool</b>	The Import tool is the tool that you can use to import cardholders, cardholder groups, and credentials from a comma-separated values (CSV) file.
<b>inactive entity</b>	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.
<b>incident</b>	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.
<b>Incidents</b>	The <i>Incidents</i> task is an investigation task that you can use to search, review, and modify incident reports created by Security Desk users.
<b>interface module</b>	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.
<b>interlock</b>	An interlock (also known as sally port or airlock) is an access restriction placed on a secured area that permits only one perimeter door to be open at any given time.
<b>intrusion detection area</b>	An intrusion detection area entity represents a zone (sometimes called an area) or a partition (group of sensors) on an intrusion panel.
<b>Intrusion detection area activities</b>	The <i>Intrusion detection area activities</i> task is an investigation task that reports on activities (master arm, perimeter arm, duress, input trouble, and so on) in selected intrusion detection areas.

<b>intrusion detection unit</b>	An intrusion detection unit entity represents an intrusion device (intrusion panel, control panel, receiver, and so on) that is monitored and controlled by the Intrusion Manager role.
<b>Intrusion detection unit events</b>	The <i>Intrusion detection unit events</i> task is an investigation task that reports on events (AC fail, battery fail, unit lost, input trouble, and so on) related to selected intrusion detection units.
<b>Intrusion Manager</b>	The Intrusion Manager role monitors and controls intrusion detection units. It listens to the events reported by the units, provides live reports to Security Center, and logs the events in a database for future reporting.
<b>intrusion panel</b>	An <i>intrusion panel</i> (also known as <i>alarm panel</i> or <i>control panel</i> ) 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.
<b>I/O configuration</b>	The <i>I/O configuration</i> task is a maintenance task that reports on the I/O configurations (controlled access points, doors, and elevators) of access control units.
<b>I/O linking</b>	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).
<b>IP camera</b>	An IP camera is a video encoder unit incorporating a camera.
<b>IPv4</b>	IPv4 is the first generation Internet protocol using a 32-bit address space.
<b>IPv6</b>	IPv6 is a 128-bit Internet protocol that uses eight groups of four hexadecimal digits for address space.
<b>Keyhole Markup Language</b>	Keyhole Markup Language (KML) is a file format used to display geographic data in an Earth browser such as Google Earth and Google Maps.
<b>license key</b>	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).
<b>license plate inventory</b>	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).
<b>load balancing</b>	Load balancing is the distribution of workload across multiple computers.



<b>logical ID</b>	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.
<b>macro</b>	A macro is an entity that encapsulates a C# program that adds custom functionalities to Security Center.
<b>main server</b>	The 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 to be part of the same system. In a high availability configuration where multiple servers host the Directory role, it is the only server that can write to the Directory database.
<b>map link</b>	A map link is a map object that brings you to another map with a single click.
<b>map mode</b>	Map mode is a Security Desk canvas operating mode that replaces tiles and controls with a geographical map showing all active, georeferenced events in your system. Switching to Map mode is a feature that comes with AutoVu™, Genetec Mission Control™, or Record fusion, and requires a license for one of these major features.
<b>map object</b>	Map objects are graphical representations on your maps of Security Center entities or geographical features, such as cities, highways, rivers, and so on. With map objects, you can interact with your system without leaving your map.
<b>map view</b>	A map view is a defined section of a map.
<b>master arm</b>	Master arm is arming an intrusion detection area in such a way that all sensors attributed to the area would set the alarm off if one of them is triggered.
<b>Media Router</b>	The Media Router role is the central role that handles all stream requests (audio and video) in Security Center. It establishes streaming sessions between the stream source, such as a camera or an 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).
<b>Mobile Admin</b>	(Obsolete as of SC 5.8 GA) Mobile Admin is a web-based administration tool used to configure the Mobile Server.
<b>Genetec™ Mobile</b>	Official name of the map-based Security Center mobile application for Android and iOS devices.
<b>mobile credential</b>	A mobile credential is a credential on a smartphone that uses Bluetooth or Near Field Communication (NFC) technology to access secured areas.

<b>Mobile License Plate Inventory</b>	Mobile License Plate Inventory (MLPI) is the Genetec 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.
<b>Mobile Server</b>	The Mobile Server role provides Security Center access on mobile devices.
<b>monitor group</b>	A monitor group is an 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 <i>Alarm monitoring</i> task in Security Desk.
<b>monitor ID</b>	Monitor ID is an ID used to uniquely identify a workstation screen controlled by Security Desk.
<b>Monitoring</b>	The <i>Monitoring</i> task is an operation task that you can use to monitor and respond to real-time events that relate to selected entities. Using the <i>Monitoring</i> task, you can also monitor and respond to alarms.
<b>motion detection</b>	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.
<b>Motion search</b>	The <i>Motion search</i> task is an investigation task that searches for motion detected in specific areas of a camera's field of view.
<b>motion zone</b>	A motion zone is a user defined areas within a video image where motion should be detected.
<b>Move unit</b>	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.
<b>network</b>	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.
<b>network address translation</b>	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.
<b>network view</b>	The network view is a browser view that illustrates your network environment by showing each server under the network they belong to.
<b>notification tray</b>	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.

<b>Omnicast™</b>	Security Center Omnicast™ is the IP video management system (VMS) that provides organizations of all sizes the ability to deploy a surveillance system adapted to their needs. Supporting a wide range of IP cameras, it addresses the growing demand for HD video and analytics, all the while protecting individual privacy.
<b>Omnicast™ compatibility pack</b>	Omnicast™ compatibility pack is the software component that you need to install to make Security Center compatible with an Omnicast™ 4.x system.
<b>Omnicast™ Federation™</b>	The Omnicast™ Federation™ role connects an Omnicast™ 4.x system to Security Center. That way, the Omnicast™ entities and events can be used in your Security Center system.
<b>output behavior</b>	An output behavior is an entity that defines a custom output signal format, such as a pulse with a delay and duration.
<b>parking facility</b>	A parking facility entity defines a large parking area as a number of sectors and rows for the purpose of inventory tracking.
<b>partition</b>	A partition is an entity in Security Center 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.
<b>People counting</b>	The <i>People counting</i> task is an operation task that keeps count in real-time of the number of cardholders in all secured areas of your system.
<b>perimeter arm</b>	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.
<b>Plan Manager</b>	(Obsolete) Plan Manager is a module of Security Center that provides interactive mapping functionality to better visualize your security environment. The Plan Manager module has been replaced by the Security Center role, Map Manager, since version 5.4 GA.
<b>plugin</b>	A plugin (in lowercase) is a software component that adds a specific feature to an existing program. Depending on the context, plugin can refer either to the software component itself or to the software package used to install the software component.
<b>plugin role</b>	A plugin role adds optional features to Security Center. A plugin role is created by using the <i>Plugin</i> role template. By default, it is

represented by an orange puzzle piece in the *Roles* view of the *System* task. Before you can create a plugin role, the software package specific to that role must be installed on your system.

<b>Point of sale</b>	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.
<b>primary server</b>	The 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.
<b>private IP address</b>	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.
<b>private task</b>	A private task is a saved task that is only visible to the user who created it.
<b>privilege</b>	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.
<b>public task</b>	A public task is a saved task that can be shared and reused among multiple Security Center users.
<b>reader</b>	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.
<b>recording mode</b>	Recording mode is the criteria by which the system schedules the recording of video streams. There are four possible recording modes: <ul style="list-style-type: none"><li>• <b>Continuous.</b> Records continuously.</li><li>• <b>On motion/Manual.</b> Records according to motion detection settings, and when a user or system action requests it.</li><li>• <b>Manual.</b> Records only when a user or system action requests it.</li><li>• <b>Off.</b> No recording is permitted.</li></ul>
<b>recording state</b>	Recording state is the current recording status of a given camera. There are four possible recording states: <i>Enabled</i> ,

*Disabled, Currently recording (unlocked), and Currently recording (locked).*

<b>redirector</b>	A redirector is a server assigned to host a redirector agent created by the Media Router role.
<b>redirector agent</b>	A redirector agent is an agent created by the Media Router role to redirect data streams from one IP endpoint to another.
<b>redundant archiving</b>	Redundant archiving is an option to enhance the availability of video and audio archives during failover and to protect against data loss. If you enable this option, all servers assigned to an Archiver role archive video, and audio, at the same time.
<b>Remote</b>	The <i>Remote</i> task is an operation task that you can use to remotely monitor and control other Security Desk applications in your system that are running the <i>Monitoring</i> task or the <i>Alarm monitoring</i> task.
<b>Report Manager</b>	The Report Manager role automates report emailing and printing based on schedules.
<b>report pane</b>	The report pane is one of the panes found in the Security Desk workspace. It displays query results or real-time events in a tabular form.
<b>request to exit</b>	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.
<b>role</b>	A role is a software component that performs a specific job within Security Center. To execute a role, you must assign one or more servers to host it.
<b>roles and units view</b>	The roles and units view is a browser view that lists the roles on your system with the units they control as child entities.
<b>route</b>	A route is a setting that configures the transmission capabilities between two end points in a network for the purpose of routing media streams.
<b>schedule</b>	A schedule is an 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).
<b>scheduled task</b>	A scheduled task is an entity that defines an action that executes automatically on a specific date and time, or according to a recurring schedule.

<b>Software Development Kit</b>	The Software Development Kit (SDK) is what end-users use to develop custom applications or custom application extensions for Security Center.
<b>secondary server</b>	A secondary server is any alternate server on standby intended to replace the primary server in the case the latter becomes unavailable.
<b>Security Center</b>	Security Center is a truly unified platform that blends IP video surveillance, access control, automatic license plate recognition, intrusion detection, and communications within one intuitive and modular solution. By taking advantage of a unified approach to security, your organization becomes more efficient, makes better decisions, and responds to situations and threats with greater confidence.
<b>Security Center Federation™</b>	The Security Center Federation™ role connects a remote independent Security Center system to your local Security Center system. That way, the remote system's entities and events can be used in your local system.
<b>Security Center Mobile</b>	(Obsolete) See Mobile Server and Genetec™ Mobile.
<b>security clearance</b>	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 enter an area if their security clearance is equal or higher than the minimum security clearance set on the area.
<b>Security Desk</b>	Security Desk is the unified user interface of Security Center. It provides consistent operator flow across all of the Security Center main systems, Omnicast™, Synergis™, and AutoVu™. The unique task-based design of Security Desk lets operators efficiently control and monitor multiple security and public safety applications.
<b>server</b>	In Security Center, a server entity represents a computer on which the Genetec™ Server service is installed.
<b>Server Admin</b>	Server Admin is the web application running on every server machine in Security Center that you use to configure the Genetec™ Server settings. You use this same application to configure the Directory role on the main server.
<b>sharing guest</b>	A sharing guest is a Security Center system that has been given the rights to view and modify entities owned by another Security Center system, called the sharing host. Sharing is done by placing the entities in a global partition.
<b>sharing host</b>	A sharing host is a Security Center system that gives the right to other Security Center systems to view and modify its entities by putting them up for sharing in a global partition.

<b>Synergis™ Appliance Portal</b>	Synergis™ Appliance Portal is the web-based administration tool used to configure and administer the Synergis™ appliance and upgrade its firmware.
<b>standard schedule</b>	A standard schedule is a schedule entity that can be used in all situations. Its only limitation is that it does not support daytime or nighttime coverage.
<b>strict antipassback</b>	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.
<b>supervised mode</b>	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.
<b>synchronous video</b>	A synchronous video is a simultaneous live video or playback video from more than one camera that are synchronized in time.
<b>Synergis™</b>	Security Center Synergis™ is the IP access control system (ACS) that heightens your organization's physical security and increases your readiness to respond to threats. Synergis™ supports an ever-growing portfolio of third-party door control hardware and electronic locks. Using Synergis™, you can leverage your existing investment in network and security equipment.
<b>Synergis™ Master Controller</b>	Synergis™ Master Controller (SMC) is an access control appliance of Genetec Inc. that supports various third-party interface modules over IP and RS-485. SMC is seamlessly integrated with Security Center and can make access control decisions independently of the Access Manager.
<b>System</b>	The <i>System</i> task is an administration task that you can use to configure roles, macros, schedules, and other system entities and settings.
<b>system event</b>	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.
<b>System status</b>	The <i>System status</i> task is a maintenance task that you can use to monitor the status of all entities of a given type in real time and to interact with them.

<b>tailgating</b>	Tailgating designates one of the following: <i>tailgating (access control)</i> or <i>tailgating (analytics)</i> .
<b>task</b>	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.
<b>taskbar</b>	A taskbar is a user interface element of the Security Center client application window, composed of the <i>Home</i> tab and the active task list. The taskbar can be configured to be displayed on any edge of the application window.
<b>task cycling</b>	A task cycling is a Security Desk feature that automatically cycles through all tasks in the active task list following a fixed dwell time.
<b>task workspace</b>	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, controls, and area view.
<b>temporary access rule</b>	A temporary access rule is an access rule that has an activation and an expiration time. Temporary access rules are suited for situations where permanent cardholders need to have temporary or seasonal access to restricted areas. These access rules are automatically deleted seven days after they expire to avoid cluttering the system.
<b>threat level</b>	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.
<b>tile</b>	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.
<b>tile ID</b>	The tile ID is the number displayed at the upper left corner of the tile. This number uniquely identifies each tile within the canvas.
<b>tile mode</b>	Tile mode is the main Security Desk canvas operating mode that presents information in separate tiles.
<b>tile pattern</b>	The tile pattern is the arrangement of tiles within the canvas.



<b>tile plugin</b>	A tile plugin is a software component that runs inside a Security Desk tile. By default, it is represented by a green puzzle piece in the area view.
<b>Time and attendance</b>	The <i>Time and attendance</i> task is an investigation task that reports on who has been inside a selected area and the total duration of their stay within a given time range.
<b>timed antipassback</b>	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.
<b>timeline</b>	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.
<b>twilight schedule</b>	A twilight schedule is a 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.
<b>unit</b>	<p>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:</p> <ul style="list-style-type: none"><li>• Access control units, managed by the Access Manager role</li><li>• Video units, managed by the Archiver role</li><li>• ALPR units, managed by the ALPR Manager role</li><li>• Intrusion detection units, managed by the Intrusion Manager role</li></ul>
<b>Unit discovery tool</b>	Starting with Security Center 5.4 GA the Unit discovery tool has been replaced by the Unit enrollment tool.
<b>Unit replacement</b>	Unit replacement is a tool that you can use 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.
<b>unlock schedule</b>	An unlock schedule defines the periods of time when free access is granted through an access point (door side or elevator floor).
<b>unreconciled read</b>	An unreconciled read is an MLPI license plate read that has not been committed to an inventory.

<b>user</b>	A user is an 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.
<b>user group</b>	A user group is an 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.
<b>user level</b>	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 staying logged on when a threat level is set. Level 1 is the highest user level, with the most privileges.
<b>validation key</b>	A validation key is a serial number uniquely identifying a computer that must be provided to obtain the license key.
<b>video analytics</b>	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 crossing a line, detection of unattended objects, or the direction of people walking or running.
<b>video archive</b>	A video archive is a collection of video, audio, and metadata streams managed by an Archiver or Auxilliary Archiver role. These collections are catalogued in the archive database that includes camera events linked to the recordings.
<b>video decoder</b>	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.
<b>video encoder</b>	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.
<b>video file</b>	A video file is a file created by an archiving role (Archiver or Auxilliary 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.
<b>Video file explorer</b>	The <i>Video file explorer</i> is an investigation task that you can use to browse through your file system for video files (G64 and G64x), and to play, convert to ASF, and verify the authenticity of these files.
<b>video sequence</b>	A video sequence is any recorded video stream of a certain duration.

<b>video stream</b>	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.
<b>video unit</b>	A video unit is a video encoding or decoding device that is capable of communicating over an IP network and that can incorporate one or more video encoders. The high-end encoding models also include their own recording and video analytics capabilities. Cameras (IP or analog), video encoders, and video decoders are all examples of video units. In Security Center, a video unit refers to an entity that represents a video encoding or decoding device.
<b>virtual zone</b>	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.
<b>Visit details</b>	The <i>Visit details</i> task is an investigation task that reports on the stay (check-in and check-out time) of current and past visitors.
<b>Visitor activities</b>	The <i>Visitor activities</i> task is an investigation task that reports on visitor activities (access denied, first person in, last person out, antipassback violation, and so on).
<b>Visitor management</b>	The <i>Visitor management</i> task is the operation task that you can use to check in, check out, and modify visitors, as well as manage their credentials, including temporary replacement cards.
<b>visual reporting</b>	Visual reporting is dynamic charts or graphs in Security Desk that deliver insights that you act on. You can perform searches and investigate situations using these visual and user-friendly reports. The visual report data can be analyzed to help identify activity patterns and enhance your understanding.
<b>visual tracking</b>	Visual tracking is a Security Center feature that lets you follow an individual in live or playback mode through areas of your facility that are monitored by cameras.
<b>VSIP port</b>	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.
<b>Watchdog</b>	Genetec™ Watchdog is a Security Center service installed alongside the Genetec™ Server service on every server computer. Genetec™ Watchdog monitors the Genetec™ Server service, and restarts it if abnormal conditions are detected.
<b>Web-based SDK</b>	The Web-based SDK role exposes the Security Center SDK methods and objects as web services to support cross-platform development.

<b>Web Client</b>	Security Center Web Client is the web application that gives users remote access to Security Center so that they can monitor videos, investigate events related to various system entities, search for and investigate alarms, and manage cardholders, visitors, and credentials. Users can log on to Web Client from any computer that has a supported web browser installed.
<b>Web Map Service</b>	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.
<b>wheel imaging</b>	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.
<b>widget</b>	A widget is a component of the graphical user interface (GUI) with which the user interacts.
<b>Windows Communication Foundation</b>	Windows Communication Foundation (WCF) is a communication architecture used to enable applications, in one machine or for multiple machines connected by a network, to communicate. Genetec Patroller™ uses WCF to communicate wirelessly with Security Center.
<b>zone</b>	A zone is an entity that monitors a set of inputs and triggers events based on their combined states. These events can be used to control output relays.
<b>Zone activities</b>	The <i>Zone activities</i> task is an investigation task that reports on zone related activities (zone armed, zone disarmed, lock released, lock secured, and so on).
<b>Zone Manager</b>	The Zone Manager role 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.
<b>Zone occupancy</b>	The <i>Zone occupancy</i> task is an investigation task that reports on the number of vehicles parked in a selected parking area, and the percentage of occupancy.

# Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ TechDoc Hub:** The latest documentation is available on the TechDoc Hub. To access the TechDoc Hub, log on to [Genetec™ Portal](#) and click [TechDoc Hub](#). Can't find what you're looking for? Contact [documentation@genetec.com](mailto: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 explains how the product works and provide instructions on how to use the product features. To access the help, click **Help**, press F1, or tap the ? (question mark) in the different client applications.

# Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to TechDoc Hub, where you can find information and search for answers to your product questions.

- **Genetec™ TechDoc Hub:** 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 TechDoc Hub for potential fixes, workarounds, or known issues.

To access the TechDoc Hub, log on to [Genetec™ Portal](#) and click [TechDoc Hub](#). Can't find what you're looking for? Contact [documentation@genetec.com](mailto:documentation@genetec.com).

- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: [Genetec™ Assurance Description](#) and [Genetec™ Advantage Description](#).

## Additional resources

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

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss many topics, ranging from technical questions to technology tips. You can log on 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://portal.genetec.com/support>.
- For issues with license content or part numbers, or concerns about an order, please contact Genetec™ Customer Service at [customerservice@genetec.com](mailto: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](mailto:sales@genetec.com), or call 1-866-684-8006 (option #2).

## Hardware product issues and defects

Please contact GTAC at <https://portal.genetec.com/support> to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.