



Security Center SaaS User Guide for Web

Click [here](#) for the most recent version of this document.

Document last updated: April 26, 2024



Legal notices

©2024 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™, Cloud Link Roadrunner™, 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™, Streamvault Edge™, 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 Center SaaS User Guide for Web

Original document number: EN.ppp.ddd

Document number: EN.600.002

Document update date: April 26, 2024

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

About this guide

This guide describes Genetec™ Operation for web, and provides instruction on how to perform tasks, such as event monitoring, access management, and unified reporting.

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: Introduction

About Genetec Operation web	2
---------------------------------------	---

Chapter 2: Maps

Maps task process overview	4
Monitoring cameras in a map	6
Monitoring doors in a map	9
Monitoring mobile users in a map	11
Navigating between related maps	14

Chapter 3: Tiles

Tiles task process overview	17
Monitoring entities in tilesMonitoring entities in tiles in Genetec Operation web	18

Chapter 4: Reports

Reports task process overview	22
Generating a forensic report	23

Chapter 5: Access control

Access control task process overview	28
Adding cardholders	29
Adding visitors	33
Editing cardholder and visitor profiles	36
Deleting cardholders and visitors	37
Adding credentials	38
Adding cardholder groups	41
Creating access rules	44

Chapter 6: Alarms, quick actions, and critical events

Triggering alarms	48
Acknowledging alarms	50
Forcing acknowledgment of all alarms	52
Triggering quick actions	53
Setting a threat level	54

Chapter 7: Event monitoring

Selecting event types to monitor	57
Monitoring events using the watchlist	58
Playing sounds with events	61

Glossary	63
--------------------	----

Where to find product information	67
---	----

Technical support 68

Introduction

Learn about Genetec™ Operation web.

This section includes the following topics:

- "[About Genetec Operation web](#)" on page 2

About Genetec Operation web

Genetec™ Operation web is an application that enables users to interact with Security Center SaaS through a supported web browser.

Genetec Operation web features the following:

- Intuitive user interface.
- *Maps* task to monitor entities, interact with their associated video and events, and command functions on a map.
- *Tiles* task to view live and playback video, and perform other video management and access control tasks.
- *Reports* task to search for and view events.
 - *Alarms* report to search for alarms generated on your system.
 - *Bookmarks* report to search for bookmarked video.
 - *Camera events* report to search for camera-related events generated on your system.
 - *Door activity* report to search for access control events, such as access denied events and door status.
 - *Forensic* report to search for video of people or vehicles within a specific time frame.
 - *Anything* report to simultaneously search all report categories, except Forensic search.
- *Access control* task to create and manage cardholders, visitors, credentials, cardholder groups, and access rules.
- *Watchlist* to monitor events from specific entities.
- *Threat levels* to enable a response to dangerous situations, such as a fire or a shooting, while you are monitoring your system. You can respond by changing the state of the entire Security Center SaaS system or specific areas.

Maps













Learn how to view and interact with cameras, doors, events, and incidents from the *Maps* task in Genetec™ Operation web.

This section includes the following topics:

- ["Maps task process overview"](#) on page 4
- ["Monitoring cameras in a map"](#) on page 6
- ["Monitoring doors in a map"](#) on page 9
- ["Monitoring mobile users in a map"](#) on page 11
- ["Navigating between related maps"](#) on page 14

Maps task process overview

View and interact with all your entities, events, and incidents from the *Maps* task in Genetec™ Operation web.

Task	More information
Choose your map.	From the Select map list at the top of the page, select a map to monitor.
Choose a preset view.	Click the Presets  button on the lower-right corner of the map to select a preset view.
Select the layers (<i>map objects</i>) you want to see on the map.	Click the Select layers  button to choose your map objects.
Search for a specific entity or address.	In the selected map, use the search bar within the task to find a specific entity or a street address on a geographic map.
Monitor doors, readers, and access control events.	<ul style="list-style-type: none"> Click a door or reader marker to open the side panel. In the side panel you can: <ul style="list-style-type: none"> Manually unlock a door . Override an unlock schedule . Shunt a reader . Share the entity . Add the entity to your watchlist . Forgive antipassback violations. View access control events. See related video. For more information, see Monitoring doors in a map on page 9.
Monitor cameras and motion events.	<ul style="list-style-type: none"> Click a camera marker to open the side panel. In the side panel you can: <ul style="list-style-type: none"> Download video . Share the entity . Add the entity to your watchlist . Save a snapshot . Add a bookmark . Create a playback loop by right-clicking the timeline and dragging to select the desired time frame. View camera events. For more information, see Monitoring cameras in a map on page 6.

Task	More information
Monitor zones.	<ul style="list-style-type: none">• Click a zone marker to open the side panel.• In the side panel you can:<ul style="list-style-type: none">• View zone state (normal, active, trouble).• View zone arming state (armed, disarmed).• Manually disarm a zone (🔒).• Manually arm a zone (🔒).• Share the entity (🔗).• Add the entity to your watchlist (👁️).• View zone events.
Monitor Genetec Operation mobile users.	<ul style="list-style-type: none">• Hover over a Genetec Operation mobile user marker to view their last time stamp.• Click a Genetec Operation mobile user marker to open the side panel.• In the side panel you can send messages to users, and view the following user information:<ul style="list-style-type: none">• First and last name.• User's picture, if one has been applied to their profile.• Email address.• Last recorded location.• Live video feed from the user's mobile phone.• For more information, see Monitoring mobile users in a map on page 11.

Monitoring cameras in a map

Using the *Maps* task of Genetec™ Operation web, you can monitor camera states, live and recorded video, and their associated events.

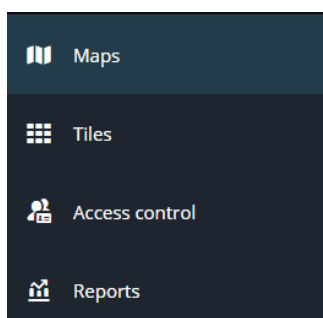
What you should know

In the *Maps* task, you can:

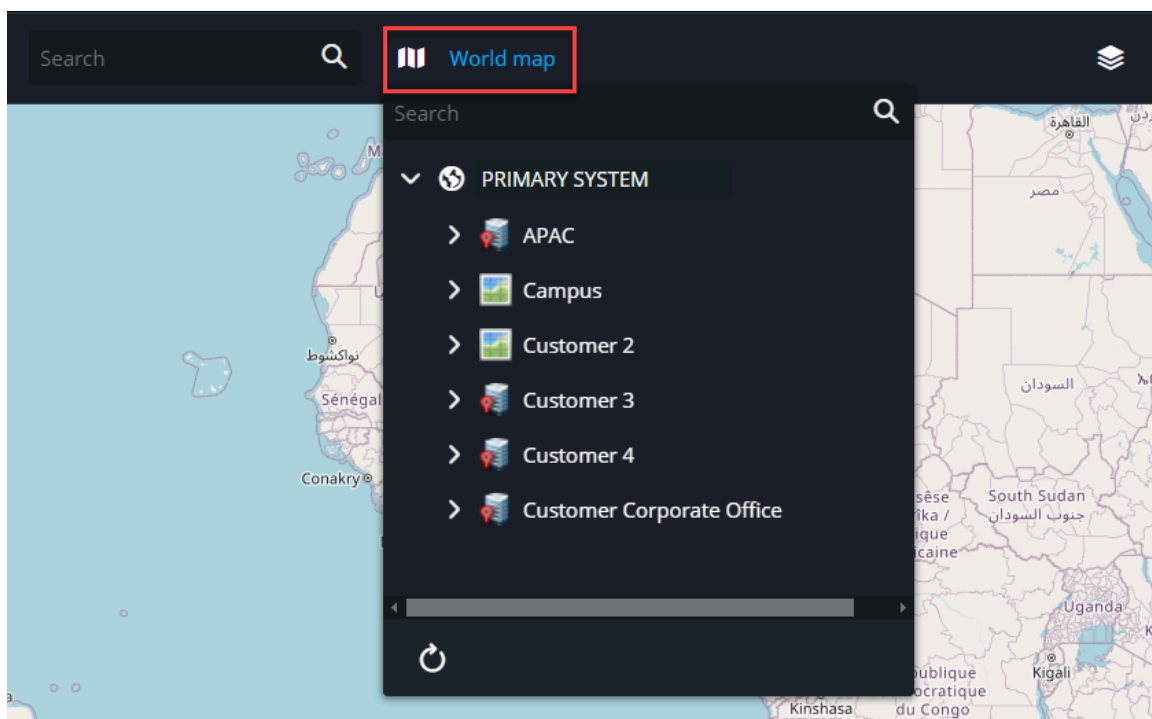
- View the state of a camera (offline, online, warning state, maintenance mode).
- View live or playback video.
- View camera events.
- Control cameras and associated entity commands.

Procedure

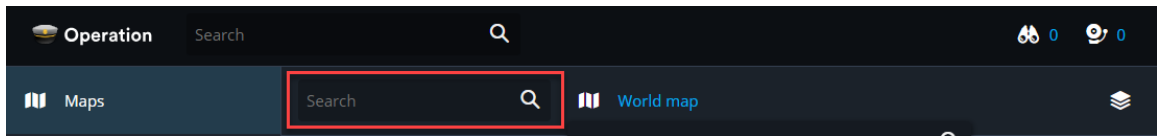
- 1 From the vertical navigation bar, click **Maps**.



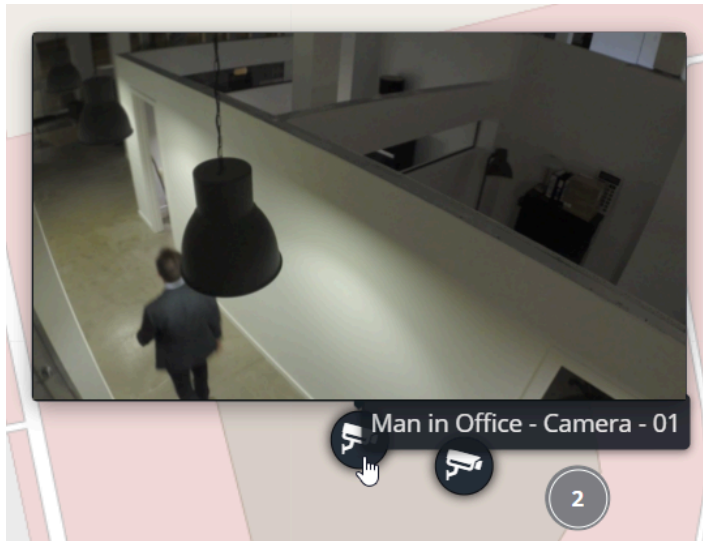
- 2 Click the **Select map** list and select your desired map.



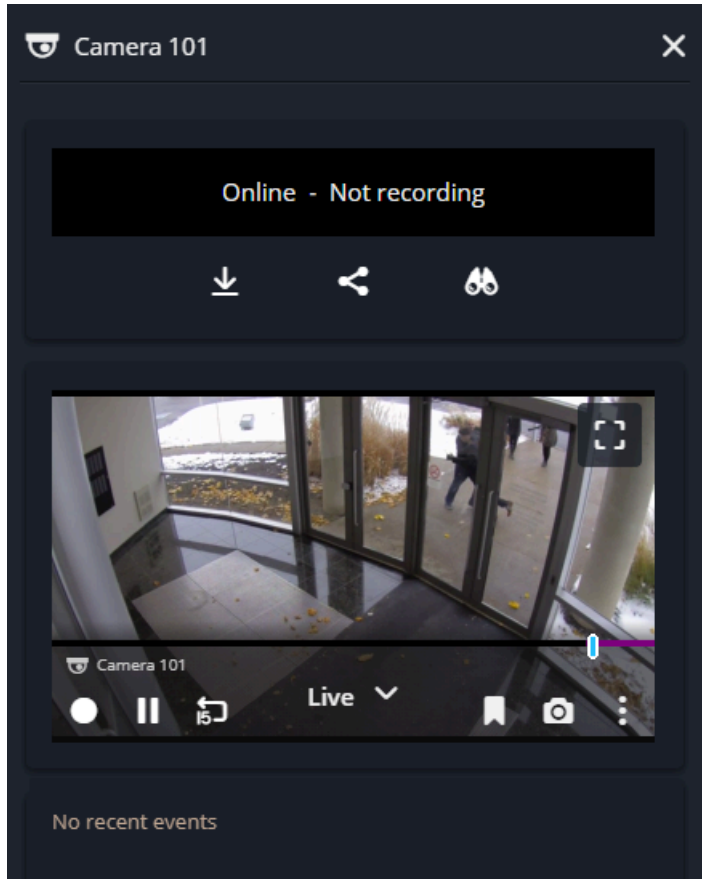
- 3 Search for a specific camera using the search bar in the task, or navigate to a camera marker (📹) in your map view.



- 4 To view associated video, hover over the camera marker.



- 5 Click the camera marker to display video, entity controls, and events in a side panel.





NOTE: To enlarge the video displayed in the side panel, click the **Maximize video** (☐☐) button.

Monitoring doors in a map

Using that *Maps* task in Genetec™ Operation web, you can monitor and interact with doors and readers.

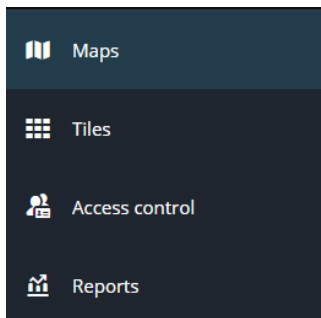
What you should know

In the *Maps* task, you can:

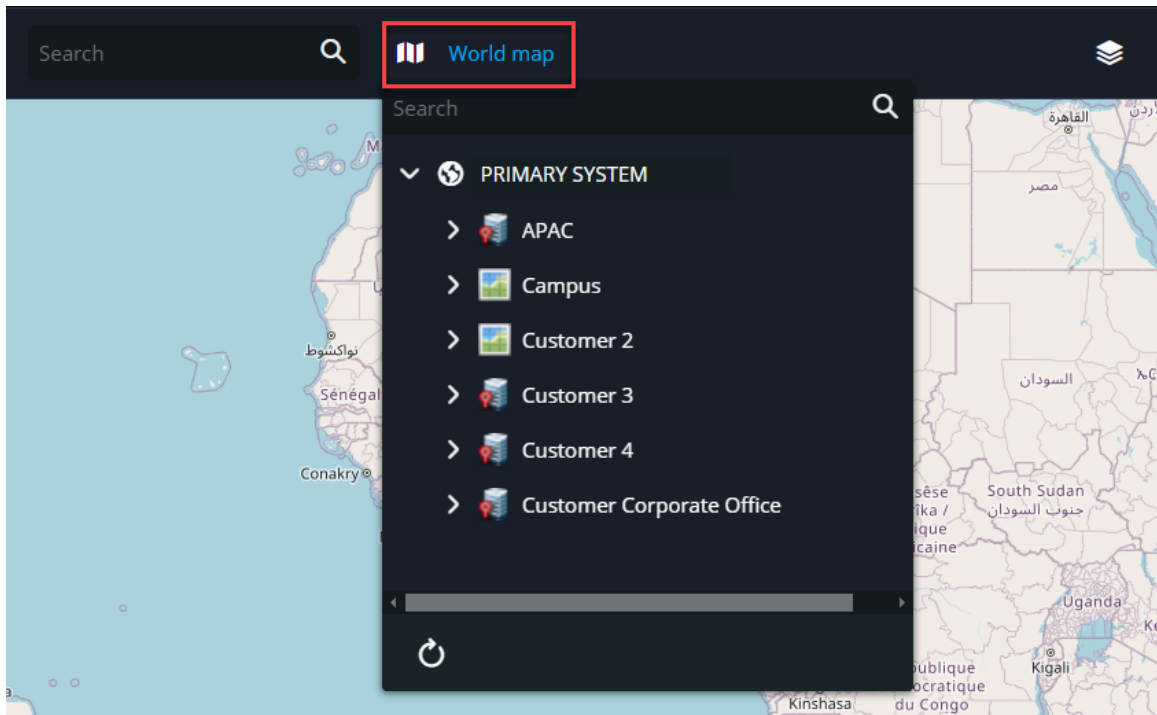
- View door health (offline, online, warning state, maintenance mode).
- View door status (closed or opened).
- View door lock status (locked  or unlocked .
- View associated video and access control events.
- Control door and reader entity commands.

Procedure

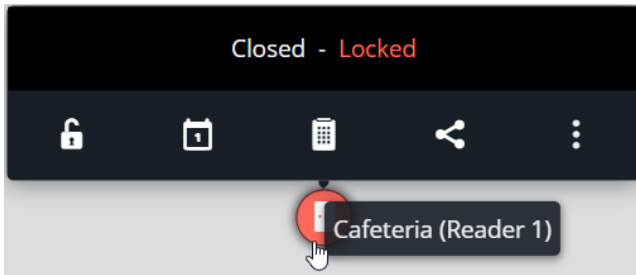
- 1 From the vertical navigation bar, click **Maps**.



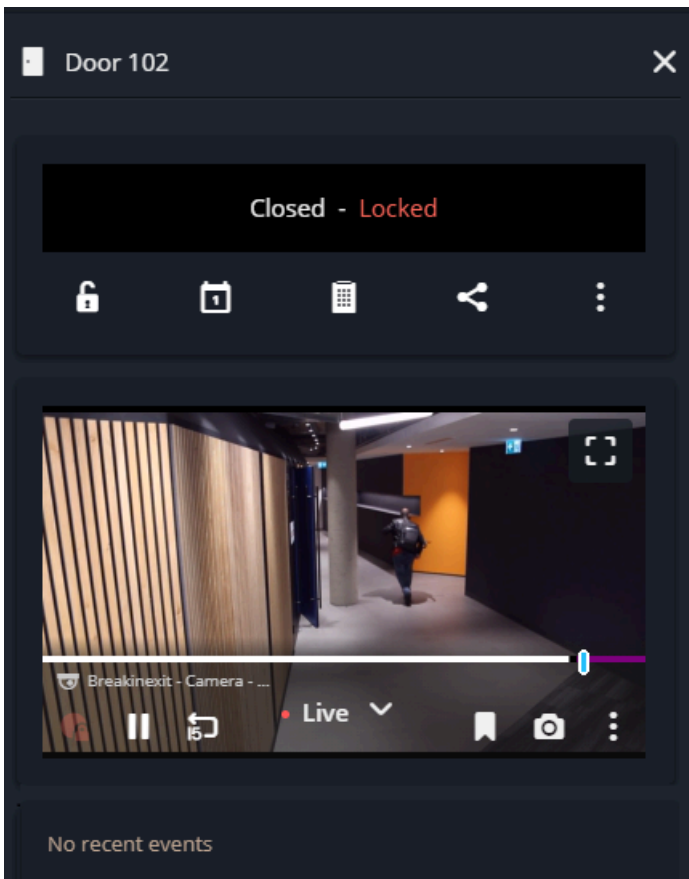
- 2 Click the **Select map** list and select your desired map.



- 3 Search for a specific door using the search bar, or navigate to a door marker displayed in your map view.
- 4 Hover over the door marker to view its lock status and commands.



- 5 Click a door marker to display video, entity controls, and events in a side panel.



NOTE: To enlarge the video displayed in the side panel, click the **Maximize video** (🗐) button.

Monitoring mobile users in a map

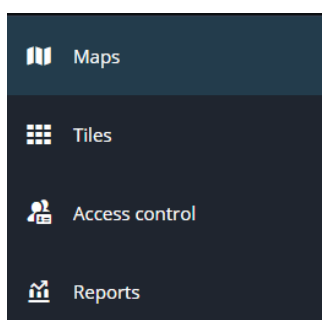
On georeferenced maps in the *Maps* task of Genetec™ Operation web, you can view the location of Genetec Operation mobile users, send them messages, and view video from their mobile phones.

Before you begin

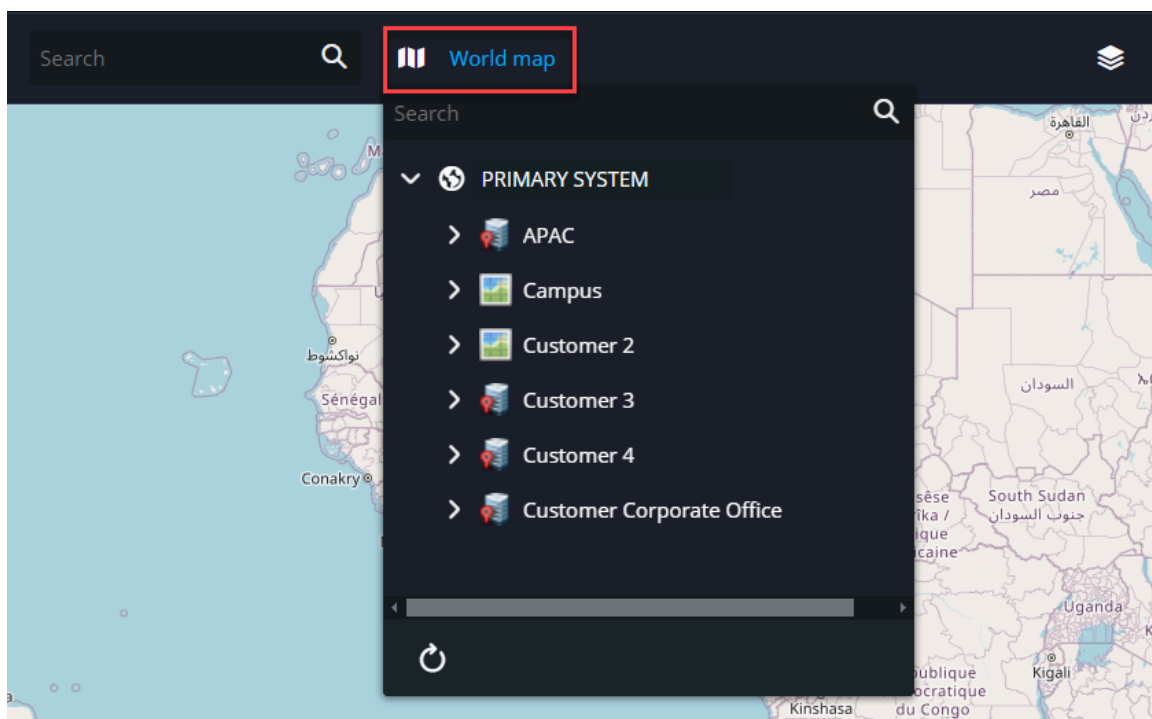
- You must have the *View mobile users* privilege to view mobile users on maps.
- For mobile users to be displayed on maps, the **Share location** option must be enabled in their Operation mobile application.

Procedure

- 1 From the vertical navigation bar, click **Maps**.

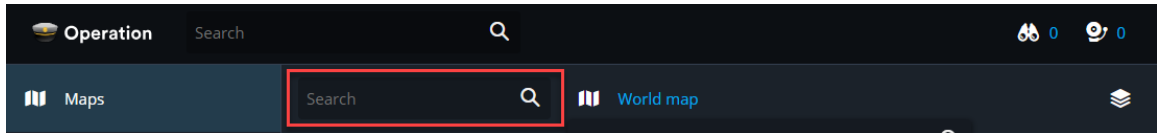


- 2 Click the **Select map** list and select a georeferenced map.

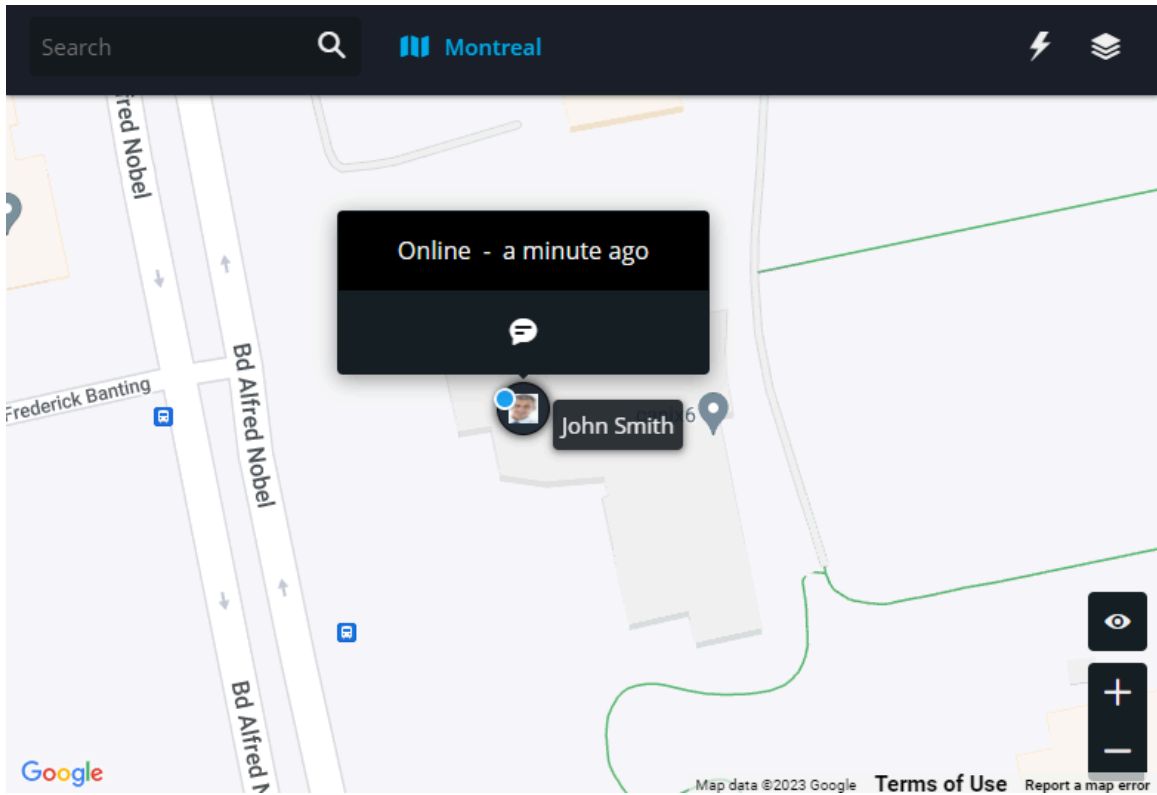


Markers representing active Operation mobile users are automatically displayed on the map. By default, these markers display cardholder pictures. If there is no cardholder picture available, the marker displays the user's initials.

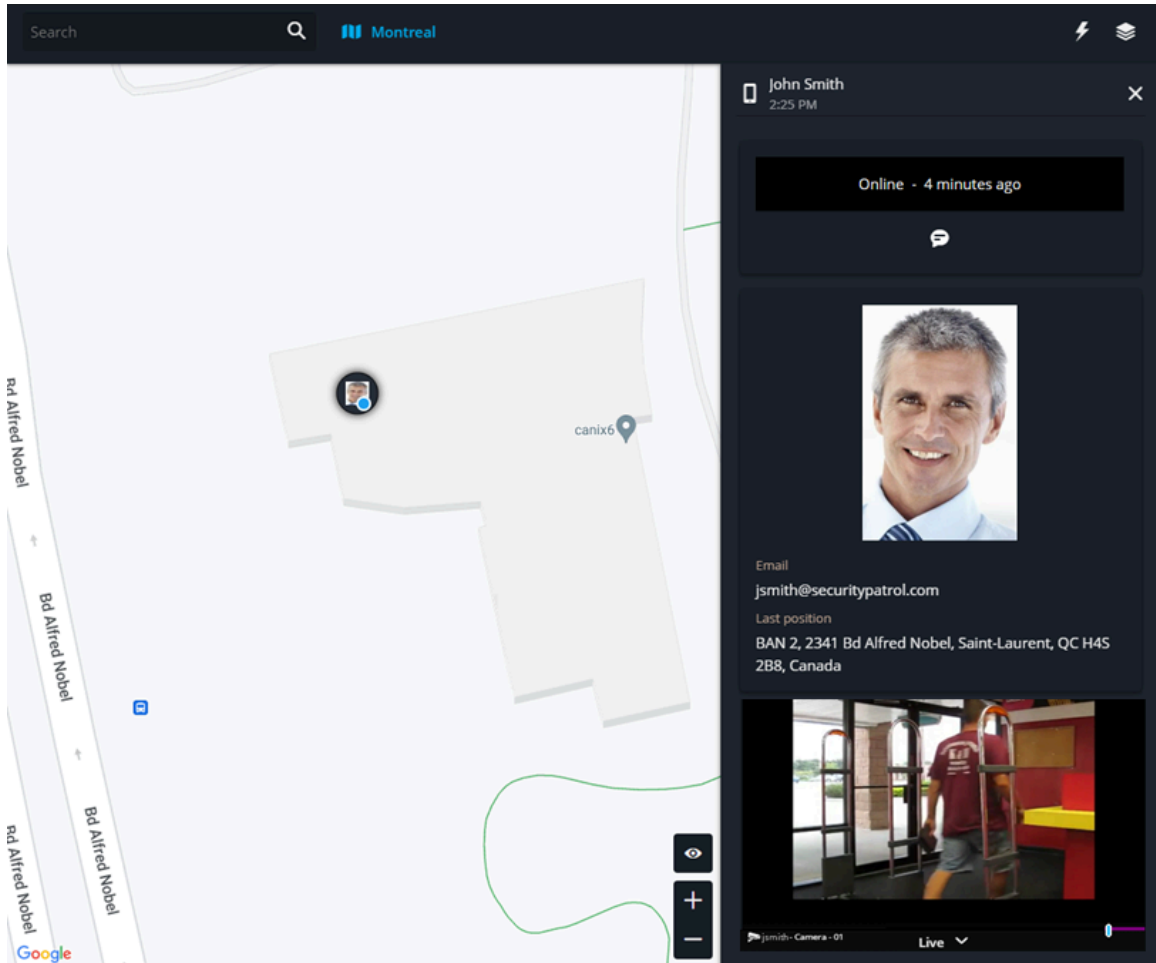
- To search for a mobile user, enter the user's first and family names or initials in the **Search** field.



- To view the last time stamp of the user, hover over their user marker.



- 5 Click a mobile user marker to display the following user information in a side panel:
- First and last name.
 - User's picture, if one has been applied to their profile.
 - Email address.
 - Last recorded location.
 - Live video feed from the user's mobile phone.



- 6 Send a message to the mobile user:
- Click the **Send a message** (message icon) button.
 - Enter a message in the dialog box.
 - Click **OK**.



The user receives the message in the Operation mobile app.

Navigating between related maps

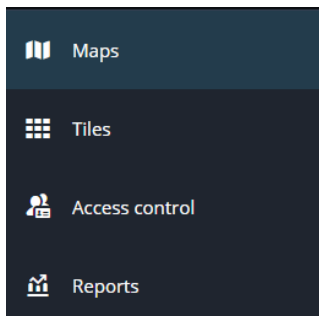
To navigate between related maps, you can click on map links or floor controls within a map.

What you should know

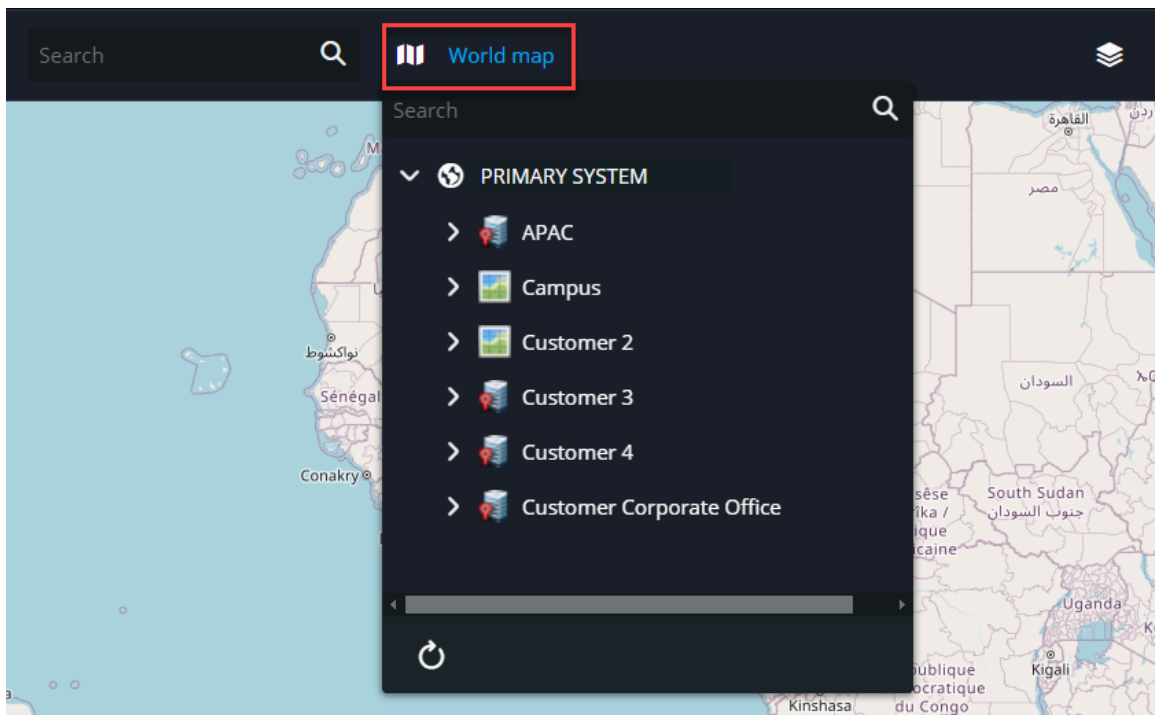
- [Map links](#) are configured on supported map objects.
- Floor controls are displayed on floor maps within buildings.
- A Security Center SaaS administrator must configure map links and floor controls.

Procedure

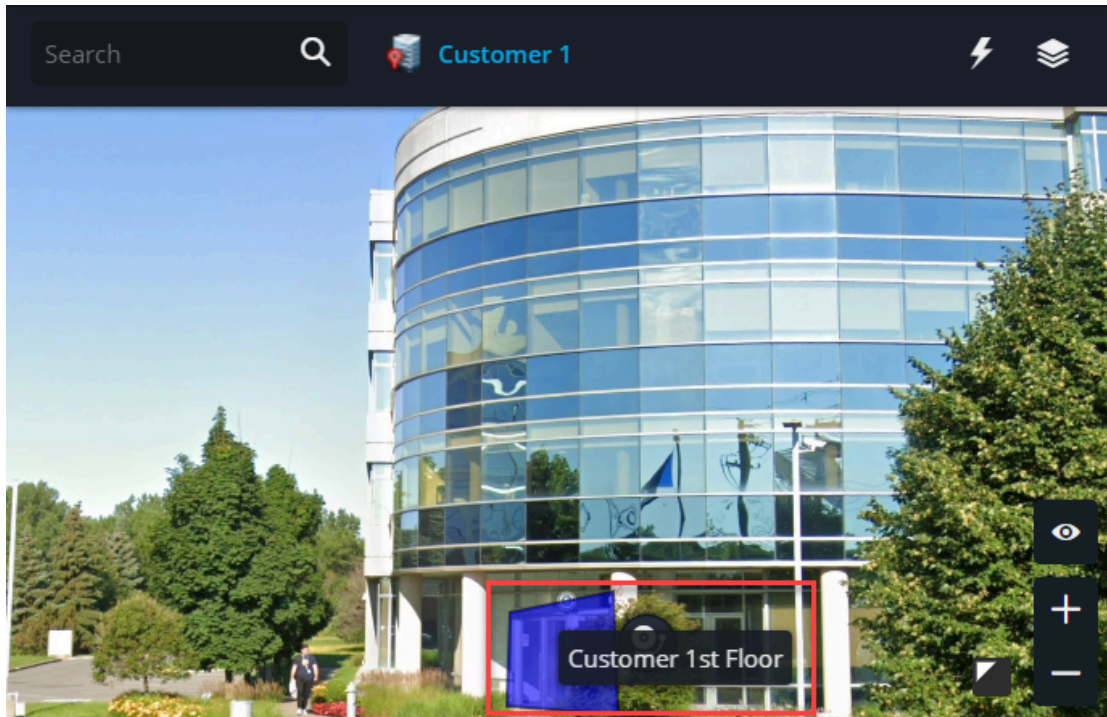
- 1 From the vertical navigation bar, click **Maps**.



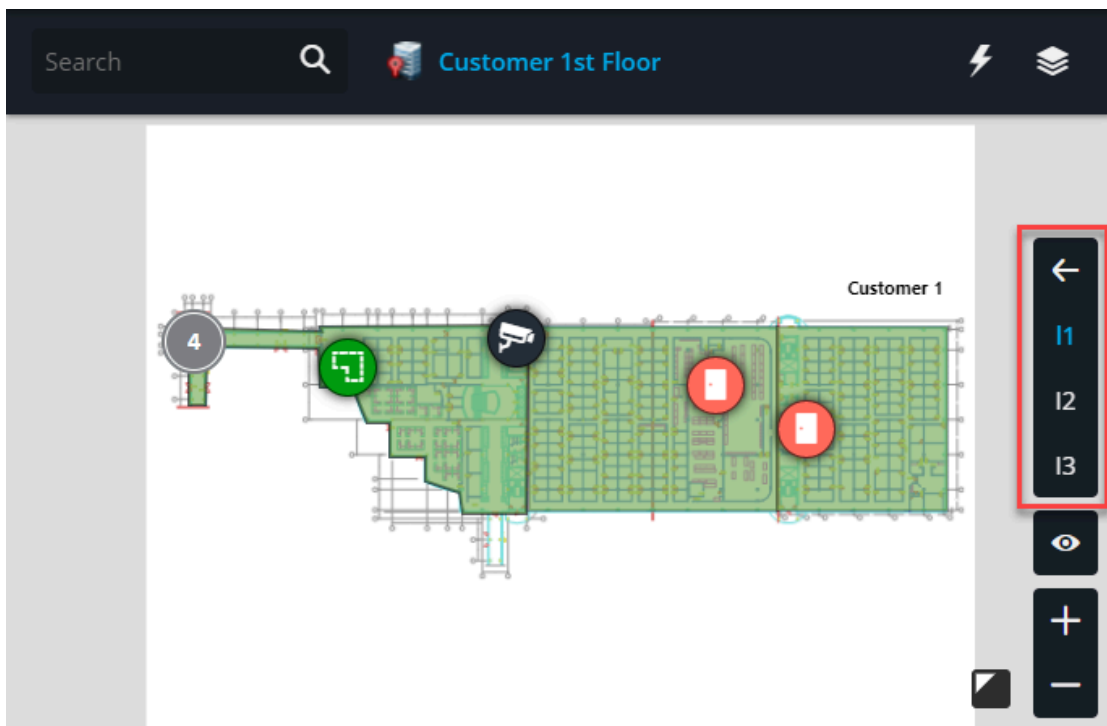
- 2 Click the **Select map** list and select a map.



- 3 Within a map, do one of the following:
 - Click on a map object that contains a map link.



- Click on a floor control.



The map associated with the map link or floor control opens.

Tiles

Learn how to monitor the state of your entities and manage their functions from the *Tiles* task in Genetec™ Operation web.





This section includes the following topics:

- ["Tiles task process overview"](#) on page 17
- ["Monitoring entities in tilesMonitoring entities in tiles in Genetec Operation web"](#) on page 18

Tiles task process overview

Monitor and interact with entities using the *Tiles* task in Genetec™ Operation web.

The following table lists the tasks required to monitor and interact with entities.

Task	More information
Select a tile pattern.	Click Change tile pattern  and select a tile pattern.
Monitor your entities.	<ul style="list-style-type: none"> • Select your entities, monitor their state, and manage their commands. • For more information, see Monitoring entities in tiles <i>Monitoring entities in tiles in Genetec Operation web</i> on page 18.
Add bookmarks when notable activities occur in a video feed. Bookmarks help with locating sequences later.	<ul style="list-style-type: none"> • While you are monitoring a video feed, click the bookmark button . • To view your bookmarks, you must generate a report. For more information, see Reports task process overview on page 22.
Create a playback loop in the video timeline.	<ul style="list-style-type: none"> • While you are monitoring a video feed, hover over the timeline, then right-click and drag your mouse to create a playback loop of the selected time frame. • To remove the loop, right-click the timeline again.
Create stand-alone video files that you can export and play outside of Security Center SaaS.	<ul style="list-style-type: none"> • While you are monitoring a video feed, click Show more  > Download . • When you export from a tile, the export range is taken from the configured playback loop, or the last five minutes of video if no loop is set. • You can export video in the following formats: <ul style="list-style-type: none"> • G64 • G64x • MP4 (default format) • ASF <p>NOTE: You need the <i>Single user video export</i> privilege, or authorization from a user with the <i>Export video</i> privilege.</p>

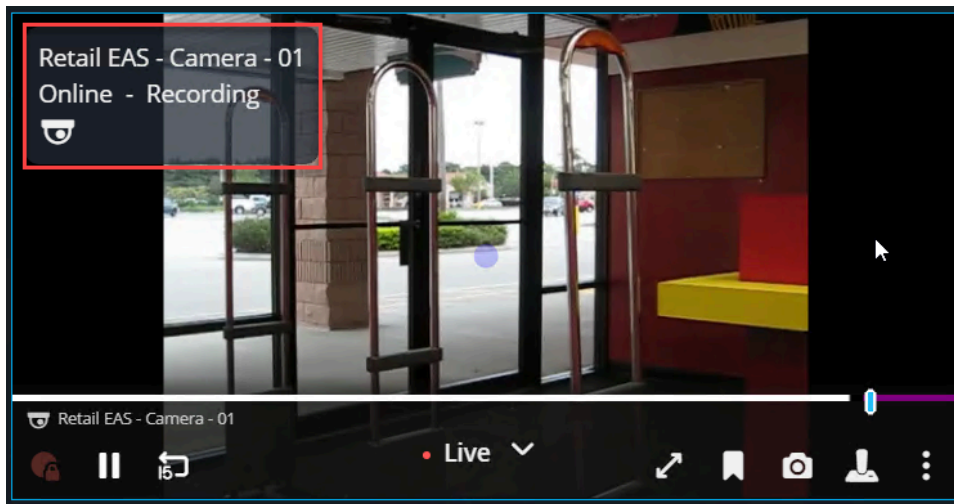
Monitoring entities in tiles

Monitoring entities in tiles in Genetec Operation web

Using the *Tiles* task in Genetec™ Operation web, you can monitor the state of your entities and manage their functions.

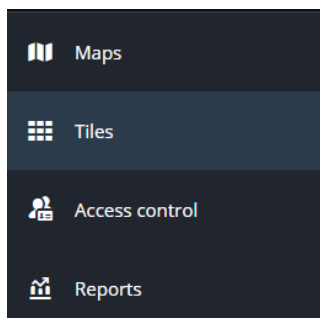
What you should know

- Your system administrator must apply privacy protection to video. Privacy protection can only be applied at the system level and not for individual cameras or videos.
- You can configure the entity state information that is displayed in the tile overlay in **Options > Tiles > Tile overlay**.

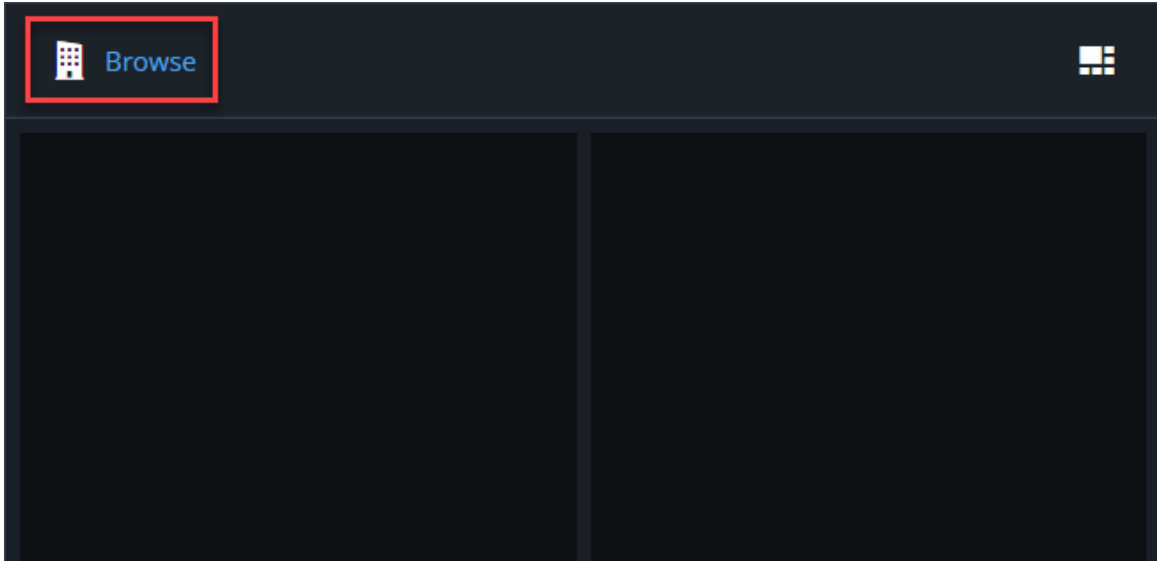


Procedure

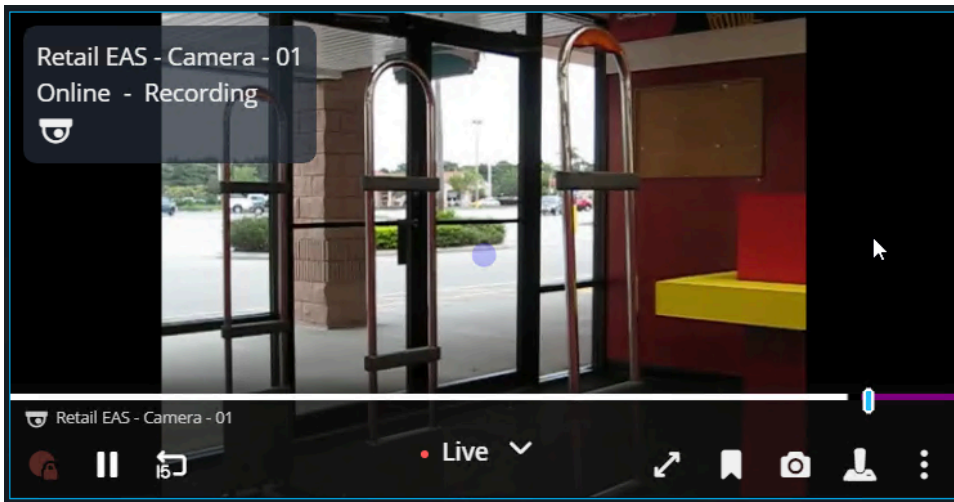
- 1 From the vertical navigation bar, click **Tiles**.



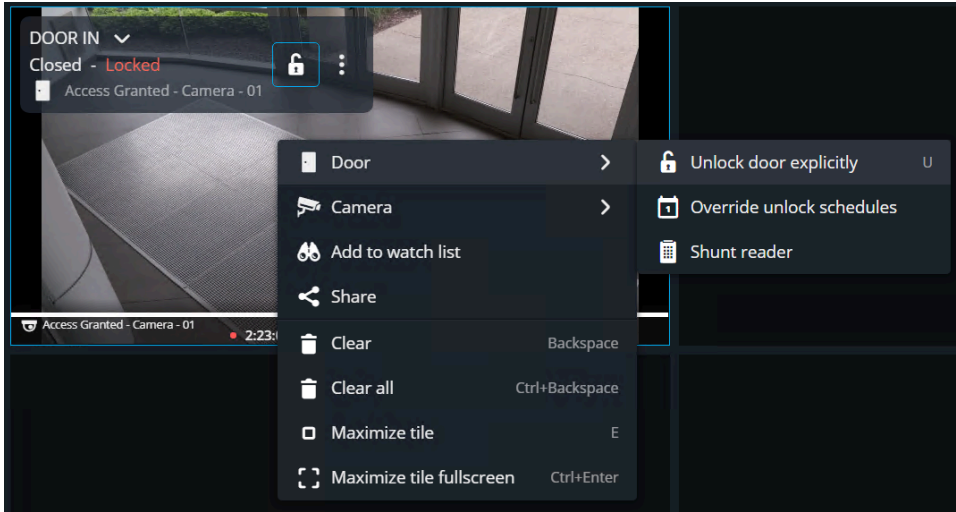
- 2 Click **Browse** (🏠) to find the entity or layout you want to monitor.



- 3 Double-click or drag the entity or layout to a tile.
NOTE: Only cameras and doors are supported. Selecting an unsupported entity does not populate the tile.
- 4 Hover over the tile to display the camera controls.



5 Right-click a tile to display the entity controls.



6 To clear entities from the canvas, do one of the following:

- Right-click a tile, and then click **Clear** (🗑️).
- Select a tile, and then press the Backspace key.
- To empty all tiles, press Ctrl+Backspace.

Reports

Generate customized queries about entities, activities, and events for investigation or maintenance purposes from the *Reports* task in Genetec™ Operation web.



This section includes the following topics:

- ["Reports task process overview"](#) on page 22
- ["Generating a forensic report"](#) on page 23

Reports task process overview

For investigation or maintenance purposes, you can generate customized queries about entities, activities, and events from the *Reports* task in Genetec™ Operation web.

The following table lists the tasks required to generate reports in the *Reports* task.

Task	More information
Choose a view.	<ul style="list-style-type: none"> • List view: Displays a list of events with their associated information displayed in columns. • Card view: Displays thumbnail images related to events. <p>NOTE: The <i>Forensic</i> report does not support the list and card view. Instead, you can sort by title or time, in ascending or descending order.</p>
Choose a report type.	<p>From the What list, select one of the following report types:</p> <ul style="list-style-type: none"> • Alarms: Report of alarms. • Bookmarks: Report of bookmarked videos. • Camera events: Report of camera-related events. • Door activity: Report of access control events, such as access denied events and door status. • Forensic: Displays video thumbnails related to the person or vehicle that meet specific criteria. • Anything: Generate a unified report of multiple event types. <p>NOTE: Forensic results are not included when you create an <i>Anything</i> report.</p>
Configure the When and Where filters.	<ul style="list-style-type: none"> • When: Filter by time frame or specific date. • Where: Filter by configured areas or specific entities.
Choose your report pane columns.	<p>After generating a report, you can sort the results of your query by clicking  > Edit columns to add or remove columns.</p> <p>NOTE: Column options depend on the type of report generated. There are no columns in the <i>Forensic</i> report.</p>
Investigate a specific result.	<p>Click a result to open a side pane containing the associated details and response actions, such as alarm acknowledgment options and incident user procedures.</p>
Export results.	<p>After generating a report, export the listed results as a CSV file by clicking  > Export CSV.</p> <p>NOTE: <i>Forensic</i> reports cannot be exported.</p>

Generating a forensic report

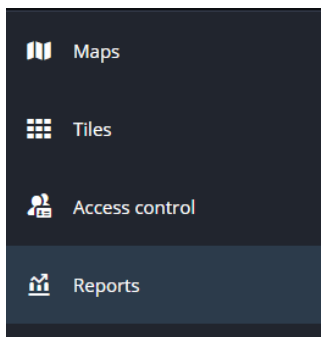
To search for video related to a specific person or vehicle, you can use the *Forensic* report in Genetec™ Operation web.

What you should know

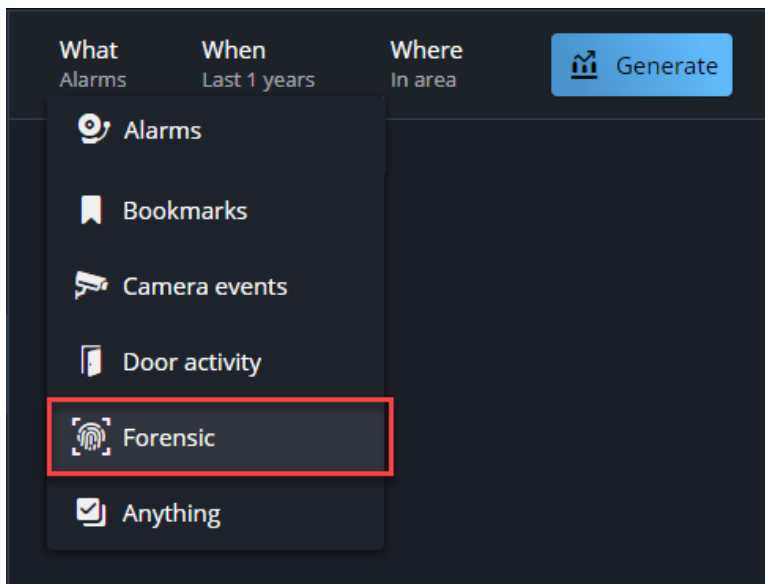
- To generate a *Forensic search* report, your Security Center SaaS system must include cameras that can record video analytics events. For a list of supported cameras and the video analytics functionality they support, see the [Supported Device List](#).
- Forensic results are not included when you create an *Anything* report.
- Applying privacy protection to the thumbnails in the *Forensic* report is not supported.
- Privacy protection for videos can only be applied at the system level and only by a system administrator.

Procedure

- 1 From the vertical navigation bar, click **Reports**.

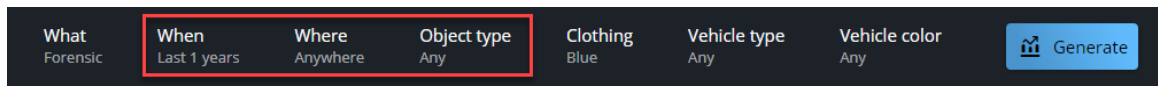


- 2 Click **What** and select **Forensic**.



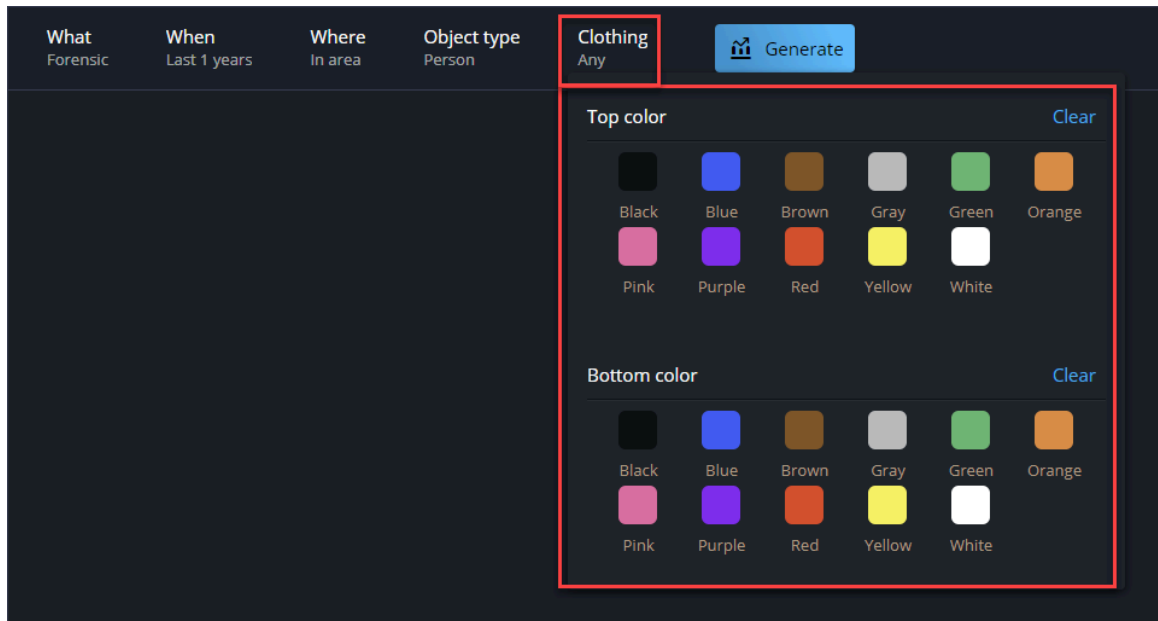
3 Select your report filters:

- **When:** Filter by time range or specific date.
- **Where:** Filter by configured areas or specific entities.
- **Object type:** Filter by person or vehicle. Select **Any** to filter by person and vehicle.



4 If you select **Any** or **Person** as your object type, use the **Clothing** filter to identify the person's clothing color.

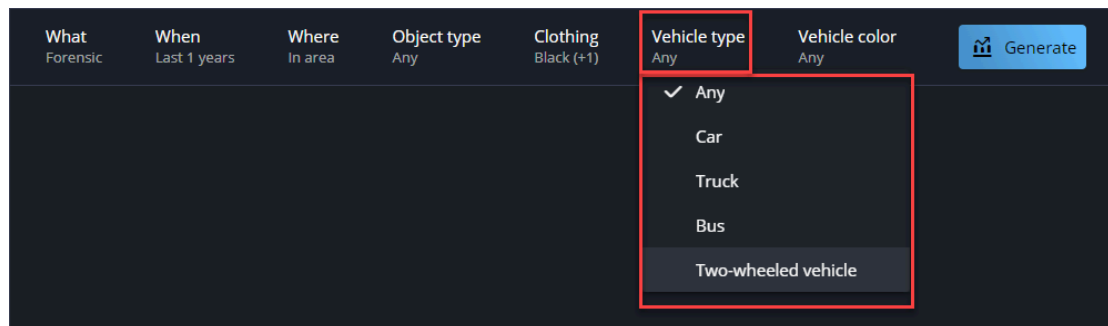
- **Top color:** The color of the person's shirt or jacket.
- **Bottom color:** The color of the person's pants.



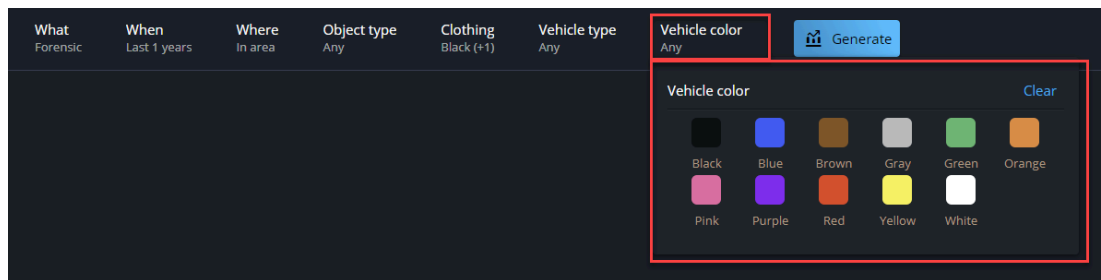
NOTE: You can select multiple clothing colors.

5 If you select **Any** or **Vehicle** as your object type, use the following filters to identify the vehicle:

- **Vehicle type:** Filter by vehicle type.



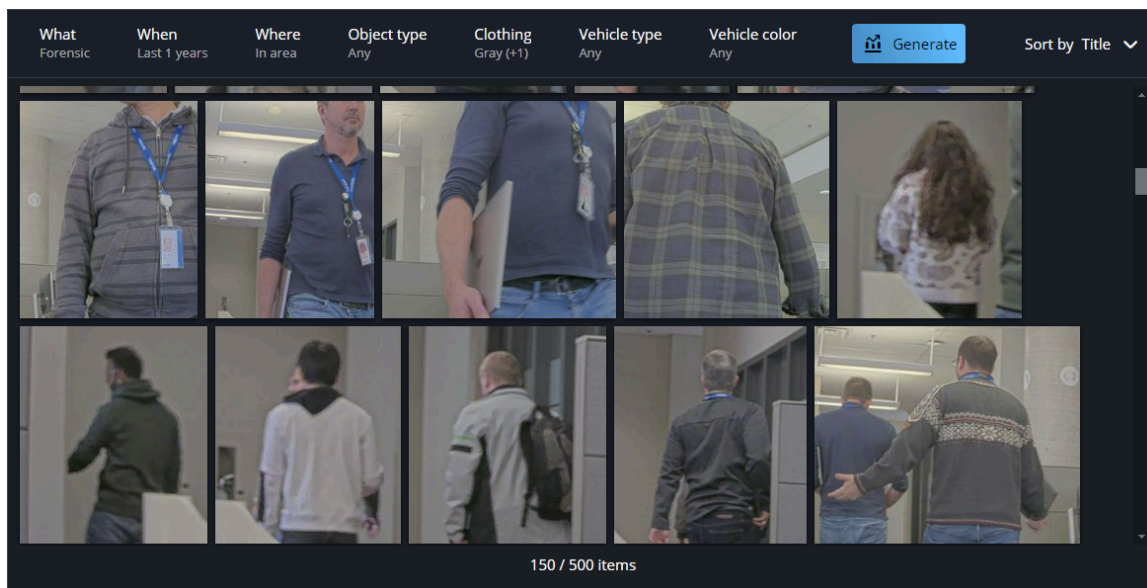
- **Vehicle color:** Filter by vehicle color.



NOTE: You can select multiple vehicle types and colors.

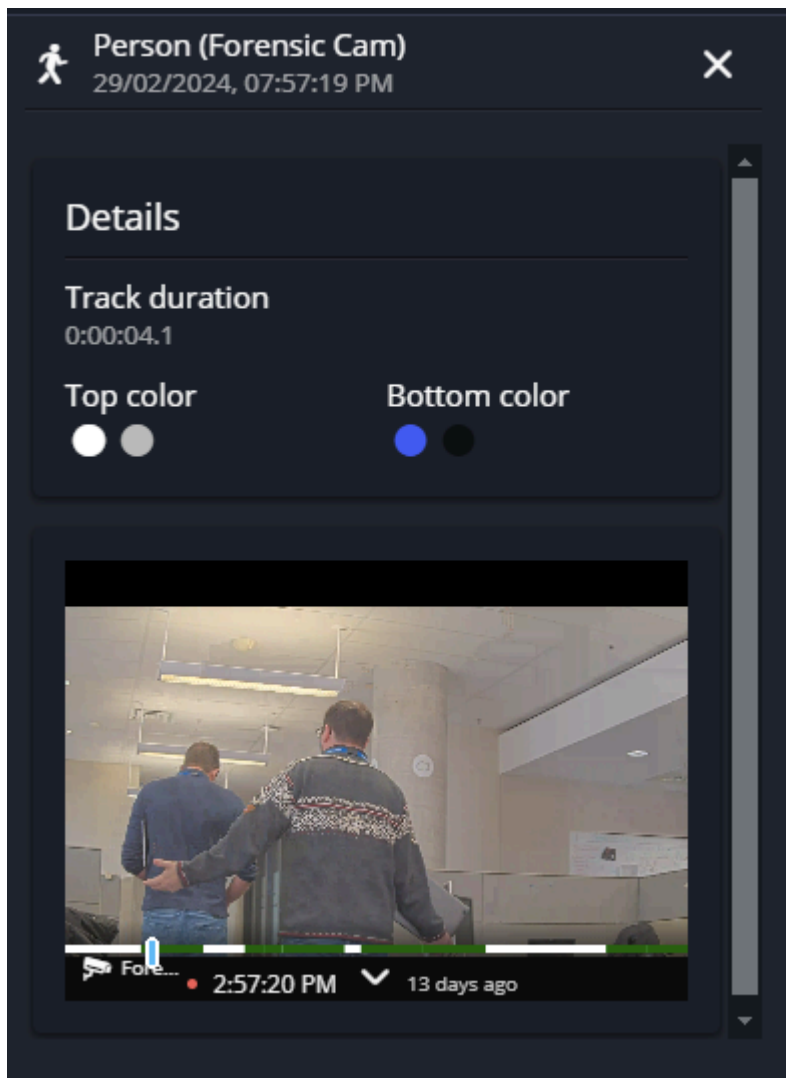
6 Click **Generate**.

Video thumbnails are displayed.



- 7 Click a thumbnail.

A details pane opens, displaying details about the video and a video tile. The green sections of the video timeline indicate the occurrence of motion events.



- 8 (Optional) To download the video, click **Show more** (⋮) in the video tile and select **Download** (↓).

Access control

Learn how to manage cardholders, cardholder groups, visitors, and access rules from the *Access control* task in Genetec™ Operation web.

This section includes the following topics:

- ["Access control task process overview"](#) on page 28
- ["Adding cardholders"](#) on page 29
- ["Adding visitors"](#) on page 33
- ["Editing cardholder and visitor profiles"](#) on page 36
- ["Deleting cardholders and visitors"](#) on page 37
- ["Adding credentials"](#) on page 38
- ["Adding cardholder groups"](#) on page 41
- ["Creating access rules"](#) on page 44

Access control task process overview

Using the *Access control* task in Genetec™ Operation web, you can manage cardholders, visitors, cardholder groups, credentials, and access rules.

The following table lists the tasks required to interact with entities in the *Access control* task.

Task	More information
Select an entity type to manage.	Choose from the following: <ul style="list-style-type: none"> • Cardholders and visitors • Credentials • Groups • Access rules
Choose a view.	On the <i>Cardholders and visitors</i> page, you can choose one of the following: <ul style="list-style-type: none"> • List view: The default view showing a list of cardholders and visitors with their associated information displayed in columns. • Card view: Displays cardholders and visitors by their card pictures.
Select columns.	<ul style="list-style-type: none"> • Some columns are hidden by default. • To select the columns you want to display, click Show more (⋮) then Select columns. • Column selections are not saved after leaving the page.
Select filters.	<ul style="list-style-type: none"> • Filter the cardholders by name, status, group, activation date, expiration date, or mobile phone number. • Filter selections are not saved after leaving the page. • To refresh the cardholder list, click Show more (⋮) then Refresh. <p>NOTE: Filters are applied automatically upon selection.</p>
Manage your entities.	<ul style="list-style-type: none"> • Adding cardholders on page 29. • Adding visitors on page 33. • Editing cardholder and visitor profiles on page 36. • Deleting cardholders and visitors on page 37. • Adding credentials on page 38. • Adding cardholder groups on page 41. • Creating access rules on page 44.

Adding cardholders

To provide individuals with access to secured areas, and to track their activities, you can create cardholders in the *Access control* task of Genetec™ Operation web.

Before you begin

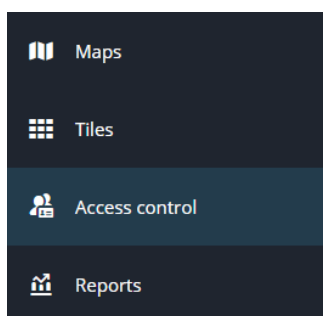
Your Security Center SaaS administrator must create partitions.

What you should know

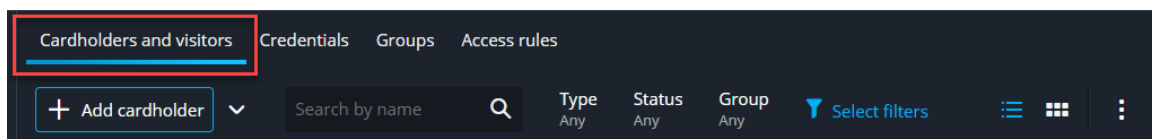
- You must have the *Add cardholders* privilege to add a cardholder.
- You must have the *Delete cardholders* privilege to remove a cardholder from a partition.

Procedure

- 1 From the vertical navigation bar, click **Access control**.



- 2 Click **Cardholders and visitors**.



The *Cardholders and visitors* page opens.

- 3 Click **Add cardholder**.

- 4 Enter the cardholder information.

The screenshot shows a dark-themed 'Add cardholder' form. At the top left is the title 'Add cardholder', and at the top right are 'Close' and 'Add' buttons. The form is divided into several sections:

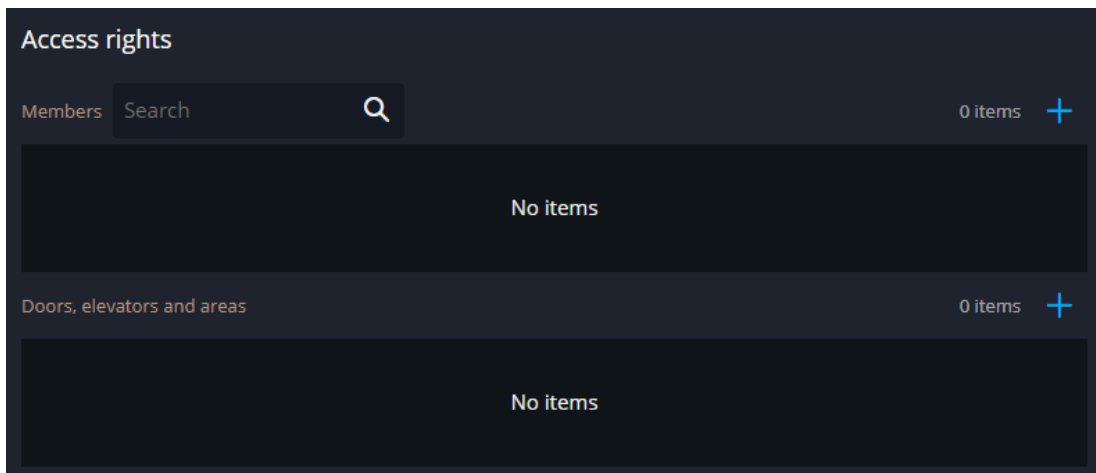
- Profile Picture:** A dark square placeholder with a person icon and a three-dot menu.
- Personal Information:** Four input fields arranged in a 2x2 grid: 'First name', 'Last name', 'Email', and 'Mobile phone number'.
- Status:** A section with a 'Status' label and a dropdown menu currently showing 'Active' with a green square icon. Below it, the text 'Activated: 03/20/2024 3:42 PM' is displayed.
- Expiration:** A section with an 'Expiration' label and a dropdown menu currently showing 'Never'.

- 5 Assign access rights to the cardholder.

- **Groups:** Click **+**, select the *cardholder groups* that the cardholder belongs to, then click **Add**.
Access rules can be inherited from the cardholder group that the cardholder belongs to.
- **Credentials:** To create a new credential:
 - a. Click **+** and select **New credential**.
 - b. Configure the credential.
 - c. Click **Create**.

To select an existing credential:

- a. Click **+** and select **Existing credential**.
 - b. Select a credential.
 - c. Click **Add**.
- **Access rules:** Click **+**, select *access rules* to apply to the cardholder, then click **Add**.



- 6 Configure the **Advanced** settings for the cardholder:
 - **Use extended grant time:** Select this option to provide more time for people with reduced mobility to pass through the door.
 - **Can escort visitors:** Select this option to allow the cardholder to act as a visitor host.
 - **Entity name:** Enter a name for the cardholder entity.
 - **Description:** Enter a description for the cardholder.
 - **Bypass antipassback rules:** Select **Inherited** to inherit the *antipassback* restrictions from the cardholder group that the cardholder belongs to. To exempt the cardholder from antipassback restrictions, select **Yes**.
 - **Security clearance:** Select **Inherited** to inherit the security clearance from the cardholder group that the cardholder belongs to. Select **Custom** to enter the security clearance level of the cardholder.

The security clearance level determines their access to areas when a threat level is set. Level 0 is the highest clearance level, with the most privileges.

- **Partitions:** Add or remove cardholders from partitions. Cardholders must belong to at least one partition.

The screenshot shows the 'Advanced' configuration panel for a cardholder profile. It includes the following sections:

- Use extended grant time:**
- Can escort visitors:**
- Entity name (required):** [Redacted text box]
- Description:** [Redacted text box]
- Logical ID:** [Dropdown menu]
- Bypass antipassback rules:** Inherited, Yes, No
- Security clearance:** Inherited, Custom
- Partitions:** 1 items +
 - Name
 - Local

7 Click **Add**.

The cardholder profile is created.

Adding visitors

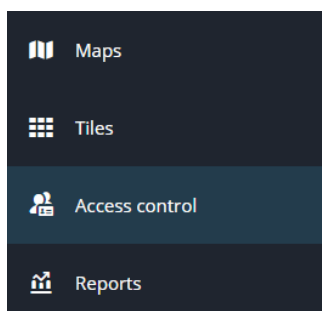
To ensure that visitors' activities can be monitored throughout their visits, you can add visitors in the *Access control* task of Genetec™ Operation web.

What you should know

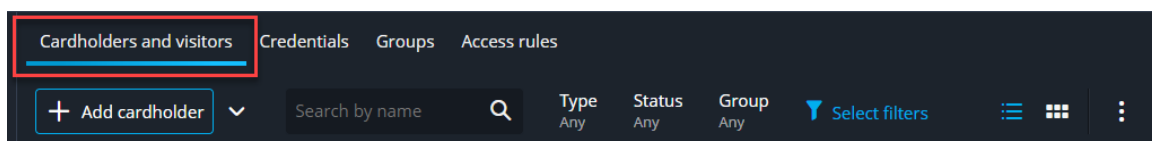
- You must have the *Check in visitors* privilege to add a visitor.

Procedure

- From the vertical navigation bar, click **Access control**.

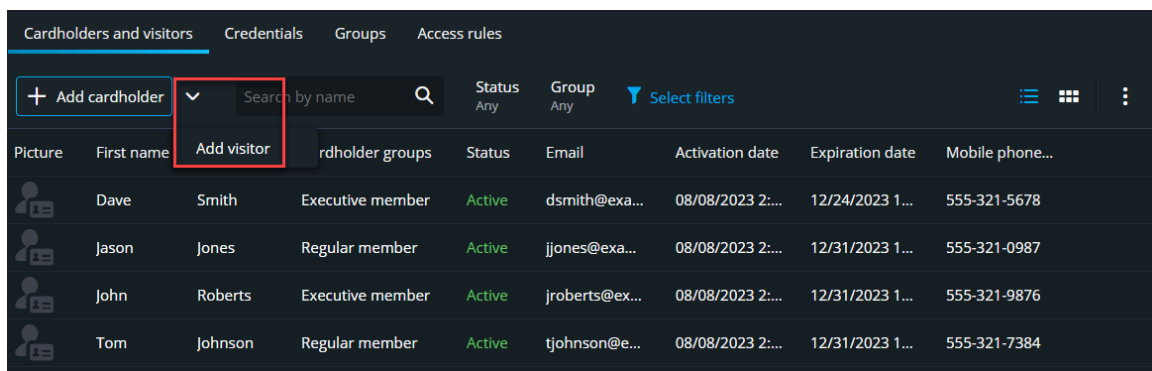


- Click **Cardholders and visitors**.



The *Cardholders and visitors* page opens.

- Click **Add visitor**.



4 Enter the visitor information.

Add visitor Close Add

First name

Last name

Email

Mobile phone number

Visitor hosts 0 items +

No items

Escort required

Expected arrival
01/17/2024 3:26 PM 📅

Status

Inactive

Activation
Never ▾

5 Assign access rights to the visitor.

- **Groups:** Click +, select the *cardholder groups* that the visitor belongs to, then click **Add**.
Access rules can be inherited from the cardholder group that the cardholder belongs to.
- **Credentials:** To create a new credential:
 - a. Click + and select **New credential**.
 - b. Configure the credential.
 - c. Click **Create**.
 To select an existing credential:
 - a. Click + and select **Existing credential**.
 - b. Select a credential.
 - c. Click **Add**.

6 Configure the **Advanced** settings for the visitor:

- **Use extended grant time:** Select this option to provide more time for people with reduced mobility to pass through the door.
- **Entity name:** Enter a name for the visitor entity.
- **Description:** Enter a description for the visitor.
- **Bypass antipassback rules:** Select **Inherited** to inherit the *antipassback* restrictions from the cardholder group that the visitor belongs to. To exempt the visitor from antipassback restrictions, select **Yes**.
- **Security clearance:** Select **Inherited** to inherit the security clearance from the cardholder group that the visitor belongs to. Select **Custom** to enter the security clearance level of the visitor. The security

clearance level determines their access to areas when a threat level is set. Level 0 is the highest clearance level, with the most privileges.

- **Partitions:** Add or remove visitors from partitions. Visitors must belong to at least one partition.

7 Click **Add**.

The visitor profile is created.

Editing cardholder and visitor profiles

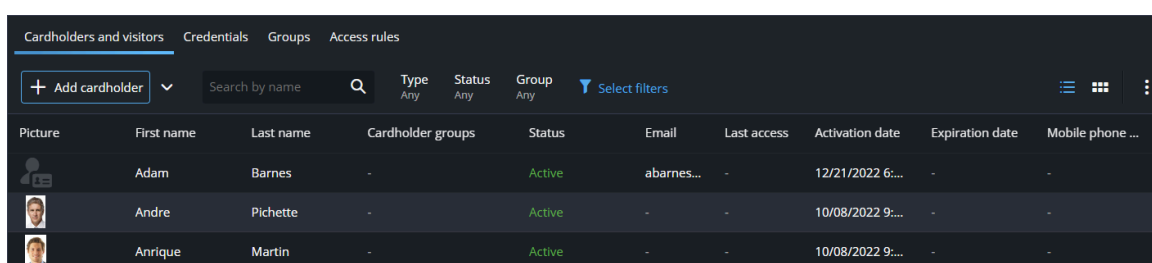
If a cardholder or visitor profile requires revisions, you can make and save the changes in Genetec™ Operation web.

What you should know

- You must have the *Modify cardholder properties* privilege to edit a cardholder profile.
- You must have the *Modify visitor properties* privilege to edit a visitor profile.

Procedure

- 1 From the vertical navigation bar, click **Access control**.
- 2 Select a cardholder or visitor from the list.



The screenshot shows the 'Cardholders and visitors' section of the Genetec interface. It includes a navigation bar with 'Cardholders and visitors', 'Credentials', 'Groups', and 'Access rules'. Below the navigation bar is a search and filter area with a '+ Add cardholder' button, a search box, and filters for 'Type', 'Status', and 'Group'. The main area displays a table with columns for 'Picture', 'First name', 'Last name', 'Cardholder groups', 'Status', 'Email', 'Last access', 'Activation date', 'Expiration date', and 'Mobile phone ...'. Three entries are visible in the table.

Picture	First name	Last name	Cardholder groups	Status	Email	Last access	Activation date	Expiration date	Mobile phone ...
	Adam	Barnes	-	Active	abarnes...	-	12/21/2022 6...	-	-
	Andre	Pichette	-	Active	-	-	10/08/2022 9...	-	-
	Anrique	Martin	-	Active	-	-	10/08/2022 9...	-	-

- 3 Make the required changes to the cardholder or visitor profile in the details pane.
- 4 Click **Save**.

Deleting cardholders and visitors

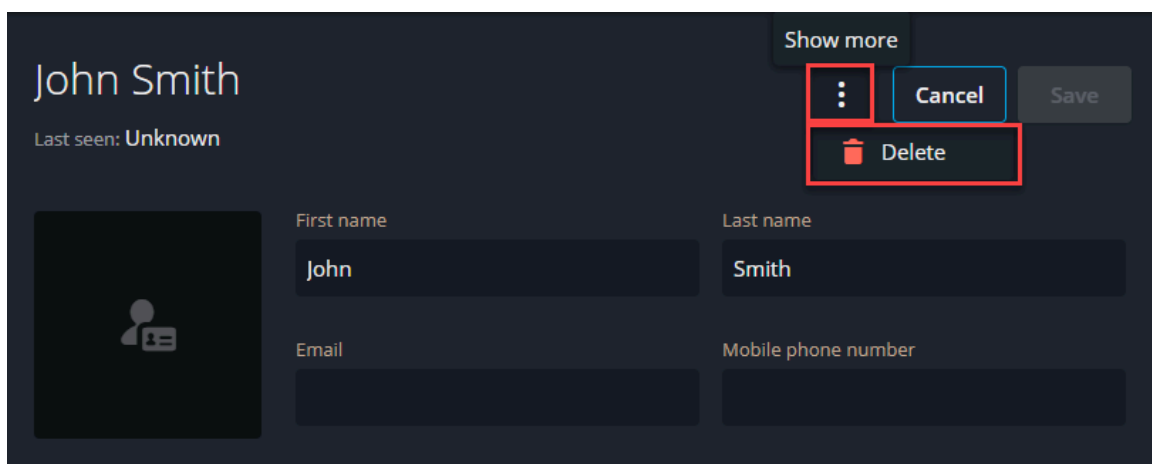
If an individual no longer requires access to secured areas, you can delete their profile in the *Access control* task of Genetec™ Operation web.

What you should know

- You must have the *Delete cardholders* privilege to delete a cardholder profile.
- You must have the *Check out visitors* privilege to delete a visitor profile.

Procedure

- 1 From the vertical navigation bar, click **Access control**.
- 2 Select a cardholder or visitor from the list.
- 3 Do one of the following:
 - For cardholders, click **Show more** > **Delete**.
 - For visitors, click **Show more** > **Check out**.



Adding credentials

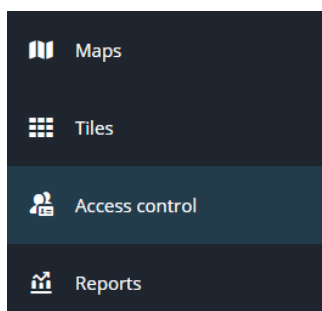
Using the *Access control* task in Genetec™ Operation web, you can create a credential, configure its properties, and assign it to a cardholder or visitor.

What you should know

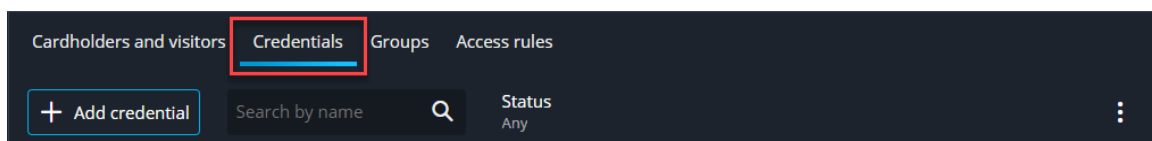
You need the *Add credentials* privilege.

Procedure

- 1 From the vertical navigation bar, click **Access control**.

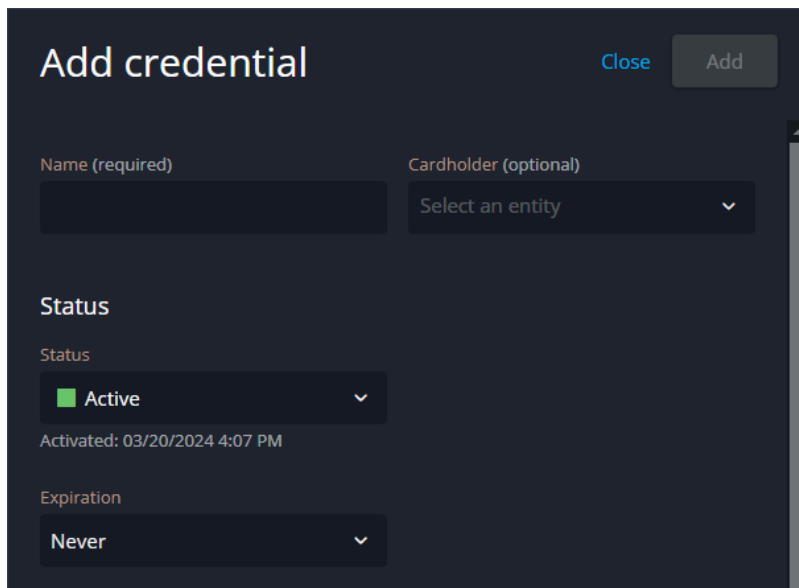


- 2 Click the **Credentials** tab.



- 3 Click **Add credential**.
The *Add credential* details pane opens.
- 4 Enter a name for the credential.
- 5 From the **Cardholder** list, select the cardholder who the credential applies to.

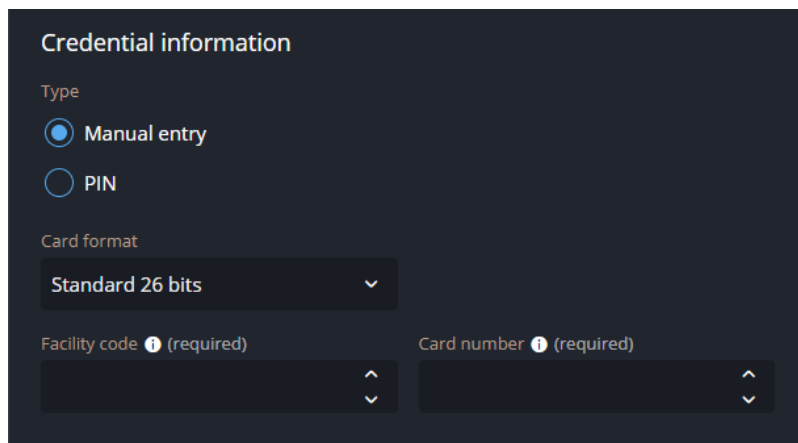
- 6 In the *Status* section, set the status and expiration:
 - a) From the **Status** list, select **Active** or **Inactive**.
 - b) From the **Expiration** list, set an expiration type.



The screenshot shows a dark-themed 'Add credential' form. At the top, there is a title 'Add credential' on the left, a 'Close' link in the middle, and an 'Add' button on the right. Below the title, there are two input fields: 'Name (required)' and 'Cardholder (optional)'. The 'Cardholder' field is a dropdown menu with the text 'Select an entity' and a downward arrow. Below these fields is a section titled 'Status'. Under 'Status', there is a dropdown menu with 'Active' selected, indicated by a green square and a downward arrow. Below the status dropdown, the text 'Activated: 03/20/2024 4:07 PM' is displayed. At the bottom of the 'Status' section, there is an 'Expiration' dropdown menu with 'Never' selected and a downward arrow.

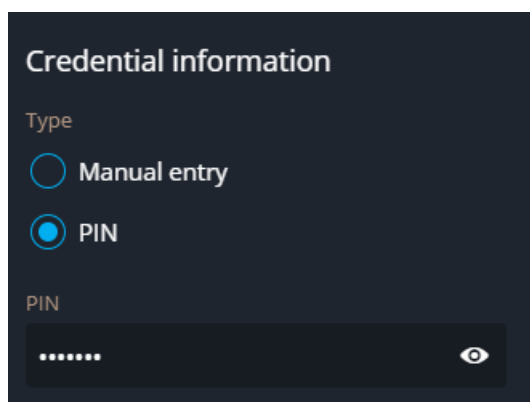
7 In the *Credential information* section, choose one of the following:

- Manual entry
 - a. Select a card format.
 - b. Enter the card information.
 - c. Click **Create**.



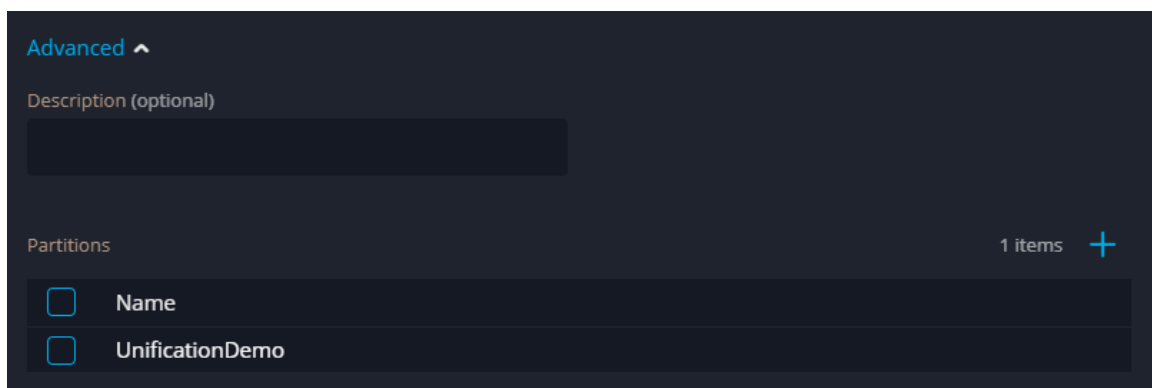
The screenshot shows the 'Credential information' section of a user interface. Under the 'Type' heading, the 'Manual entry' radio button is selected. Below this, the 'Card format' is set to 'Standard 26 bits'. There are two input fields: 'Facility code (required)' and 'Card number (required)', both of which are currently empty.

- PIN
 - a. Enter the PIN as a numerical value.
NOTE: The maximum PIN length is nine digits.



The screenshot shows the 'Credential information' section with the 'PIN' radio button selected. Below the type selection, there is a 'PIN' input field containing six dots, indicating a masked numerical value. A toggle icon (an eye) is visible to the right of the input field.

8 In the *Advanced* section, add an optional description and apply one or more partitions to the credential.



The screenshot shows the 'Advanced' section of the configuration. It includes a 'Description (optional)' text area. Below that is a 'Partitions' section with a list of two items: 'Name' and 'UnificationDemo'. Each item has a checkbox to its left. The 'UnificationDemo' partition is currently selected. A '+ 1 items' indicator is visible in the top right corner of the partitions list.

9 Click **Add**.

Adding cardholder groups

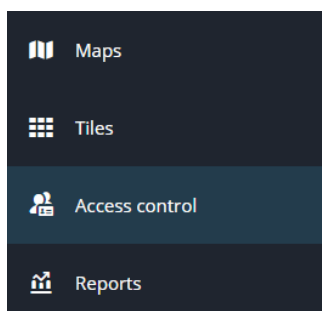
To configure the access rights and properties that are shared among multiple cardholders, you can create cardholder groups in the *Access control* task of Genetec™ Operation web.

What you should know

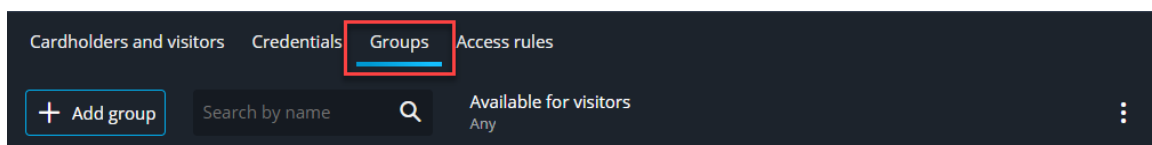
You need the *Add cardholder groups* privilege.

Procedure

- 1 From the vertical navigation bar, click **Access control**.

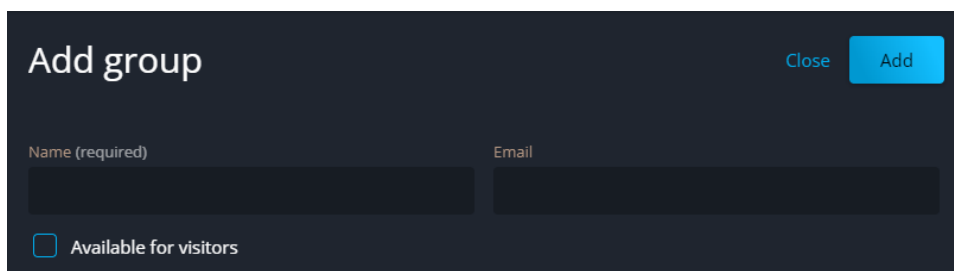


- 2 Click the **Groups** tab.

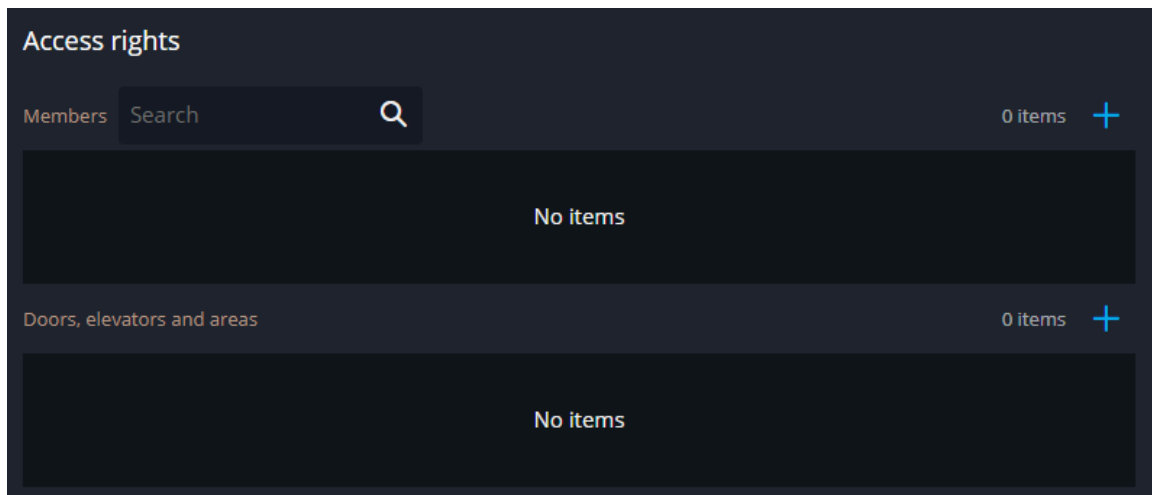


The *Groups* page opens.

- 3 Click **Add group**.
The details pane opens.
- 4 Enter a name and email address for the group.
- 5 To enable visitors to be added to the group, select the **Available for visitors** option.

A dark-themed 'Add group' form. At the top left is the title 'Add group' and at the top right are 'Close' and 'Add' buttons. Below the title are two input fields: 'Name (required)' and 'Email'. At the bottom left is a checkbox labeled 'Available for visitors'.

- 6 In the *Access rights* section, add members and access rules to the group.
 - a) Add members to the group.
 - b) Add access rules to the group.



- 7 Click **Advanced** and configure the **Advanced** settings for the group.
 - **Description:** Enter a description for the cardholder.
 - **Bypass antipassback rules:** Select **Inherited** to inherit the *antipassback* restrictions from the cardholder group that the cardholder belongs to. To exempt the cardholder from antipassback restrictions, select **Yes**.
 - **Security clearance:** Select **Inherited** to inherit the security clearance from the cardholder group of the cardholder belongs to, or **Custom** to enter the cardholder's security clearance level. The security clearance level determines their access to areas when a threat level is set. Level 0 is the highest clearance level, with the most privileges.
 - **Partitions:** Add or remove cardholders from partitions.

NOTE: Cardholders must belong to at least one partition.

Advanced parameters ^

Description

Bypass antipassback rules

Inherited from group settings
 Yes
 No

Security clearance

Inherited from group settings
 Custom

7

Partitions 1 items +

<input type="checkbox"/>	Name
<input type="checkbox"/>	UnificationDemo

Creating access rules

To control access anywhere on your site, you can apply access rules to areas, doors, and elevators in the *Access control* task of Genetec™ Operation web.

Before you begin

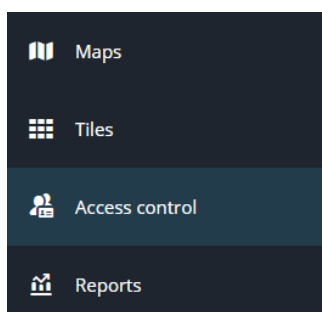
Create schedules to apply to access rules. For more information, see [Creating schedules](#) on the TechDoc Hub.

What you should know

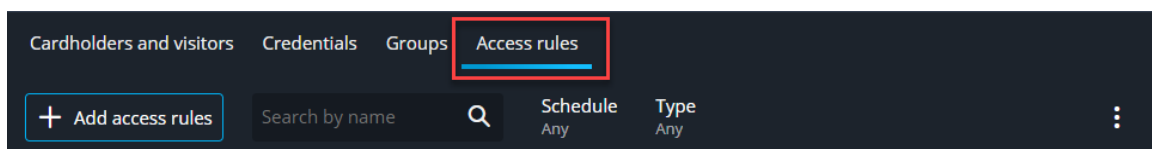
You need the *Add access rules* privilege.

Procedure

- 1 From the vertical navigation bar, click **Access control**.



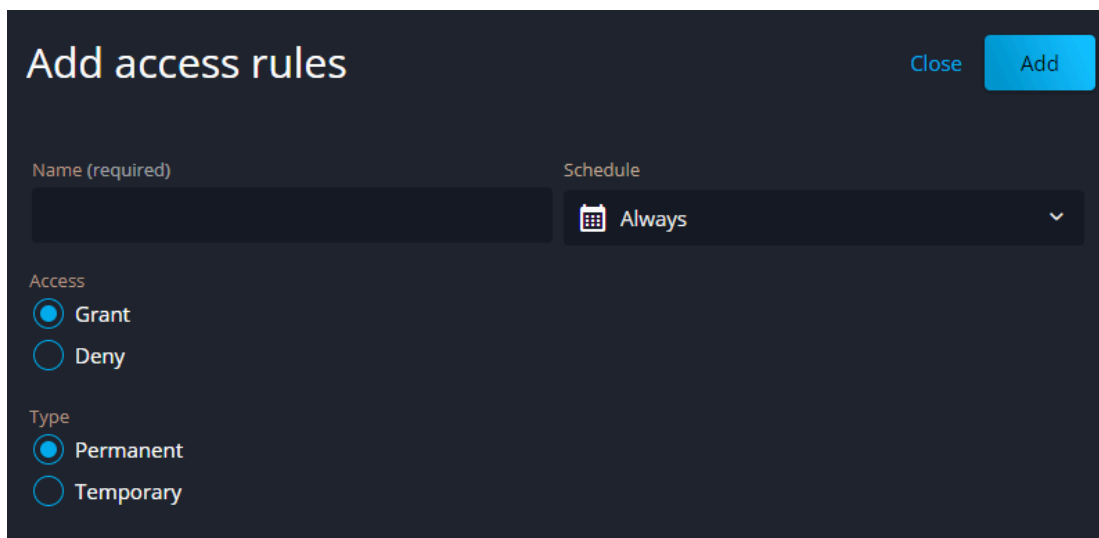
- 2 Click the **Access rules** tab.



The *Access rules* page opens.

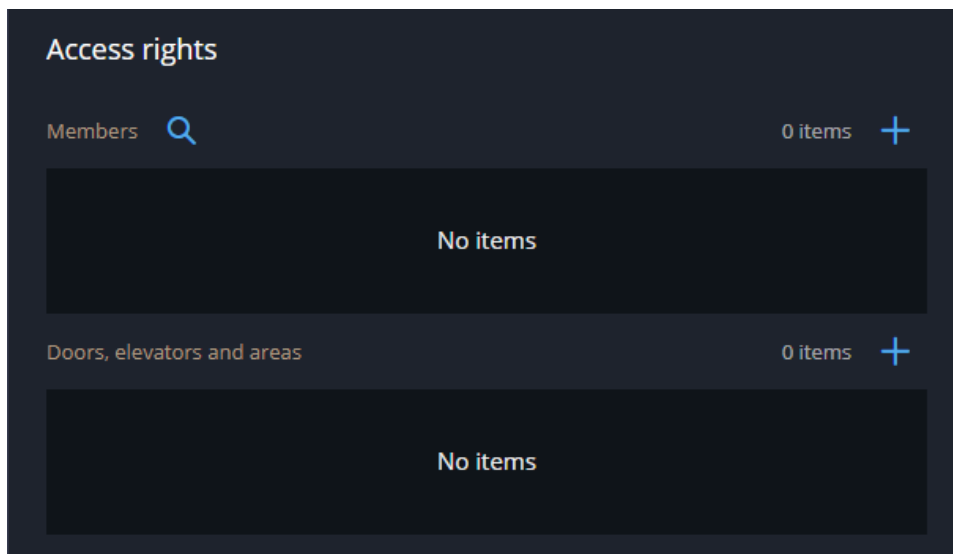
- 3 Click **Add access rules**.
The *Add access rules* pane opens.
- 4 Enter a name for the access rule.
BEST PRACTICE: Use a descriptive name to easily determine what each rule does. For example, *Lab technicians only* or *Regular employee hours*.
- 5 From the **Schedule** list, select a schedule.
- 6 Select whether to grant access or deny access when the rule is active.
BEST PRACTICE: Schedules typically grant access. Access is denied when schedules are inactive. Use explicit deny schedules only for exceptions.

- 7 Select whether the rule is permanent or temporary.
If the rule is temporary, enter an activation and expiration date.



The screenshot shows a dark-themed dialog box titled "Add access rules". In the top right corner, there are "Close" and "Add" buttons. The dialog is divided into several sections: "Name (required)" with an empty text input field; "Schedule" with a calendar icon and a dropdown menu currently set to "Always"; "Access" with two radio buttons, "Grant" (which is selected) and "Deny"; and "Type" with two radio buttons, "Permanent" (which is selected) and "Temporary".

- 8 In the *Access rights* section, select the cardholders and entities:
- In the *Members* section, select the cardholders or cardholder groups that the rule applies to.
 - In the *Doors, elevators and areas* section, select the entities that the rule applies to.



The screenshot shows the "Access rights" section of the interface. It has a dark background and is divided into two main sections. The top section is titled "Members" and includes a search icon and a plus sign. Below this, there is a large dark rectangle with the text "No items" centered inside. The bottom section is titled "Doors, elevators and areas" and also includes a plus sign. Below this, there is another large dark rectangle with the text "No items" centered inside.

- 9 Click **Advanced** and configure the advanced settings of the access rule:

Advanced ^

Description (optional)

Partitions 1 items +

Name

UnificationDemo

The access rule is created.

Alarms, quick actions, and critical events

Learn how to respond to alarms, trigger quick actions, and set a system threat level to help notify your security personnel of a threatening situation.

This section includes the following topics:

- ["Triggering alarms"](#) on page 48
- ["Acknowledging alarms"](#) on page 50
- ["Forcing acknowledgment of all alarms"](#) on page 52
- ["Triggering quick actions"](#) on page 53
- ["Setting a threat level"](#) on page 54



Triggering alarms

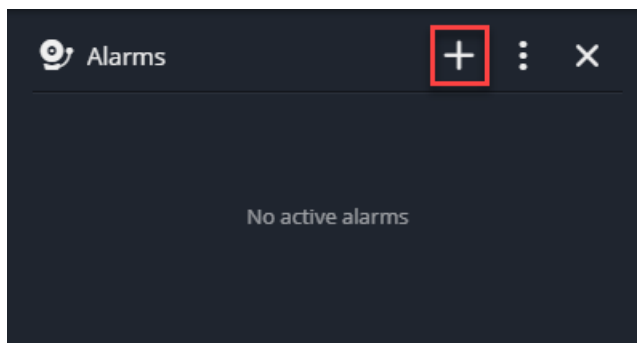
To activate an alarm, you can trigger it manually from the notification tray in Genetec™ Operation web.

What you should know

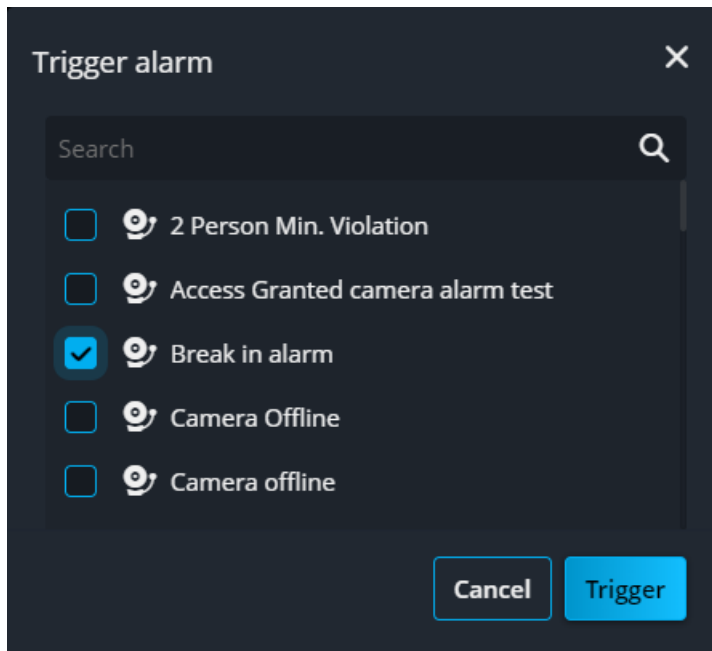
You must have the *Trigger alarms* privilege to trigger an alarm.

Procedure

- 1 Click the **Active alarms**  icon in the notification tray.
The *Alarms* side panel opens, containing a list of active alarms.
- 2 Click the **Trigger alarm**  button.

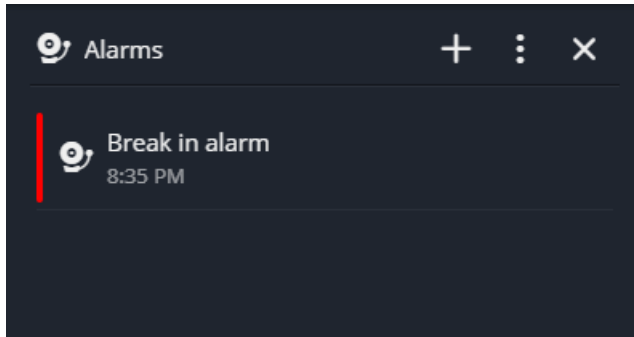


- 3 In the *Trigger alarm* dialog box, select the alarms that you want to trigger.



- 4 Click **Trigger**.

The triggered alarms are listed in the *Alarms* side panel.



NOTE: To see the triggered alarm in the **Alarms** side panel, you must be a recipient of the alarm.


Acknowledging alarms

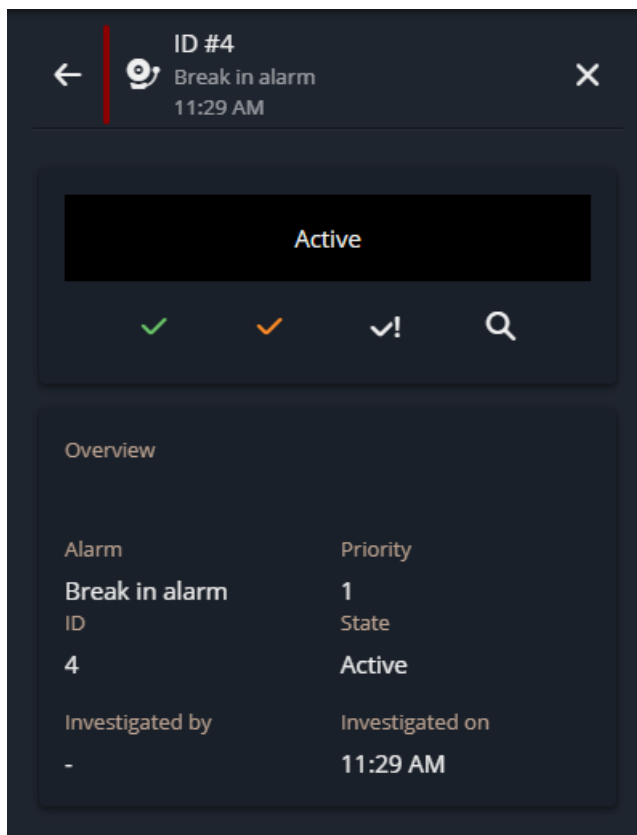
You can view and acknowledge active alarms in the *Alarms* side panel in Genetec™ Operation web.

What you should know


- You must have the *Acknowledge alarms* privilege to acknowledge an alarm.
- You must have the *Forcibly acknowledge alarms* privilege to forcibly acknowledge an alarm.
- The **Active alarms** icon changes from white to red when there is an active alarm.




Procedure

- 1 Click the **Active alarms**  icon in the notification tray.
The *Alarms* side panel opens, containing a list of active alarms.
- 2 Click an alarm.
Details about the alarm are displayed in the side panel.



- 3 Select an alarm command:

Button	Command	Description
	Acknowledge (Default)	Acknowledge the alarm. The alarm is no longer active, and is removed from the alarm list in the side panel.

Button	Command	Description
	Acknowledge (Alternate)	Set the alarm to the <i>alternate</i> acknowledged state. Your company defines the reasons to use this acknowledgment type. For example, you can use the state to acknowledge a false alarm. This state can be used as a filter in alarm queries.
	Forcibly acknowledge	Force the alarm to be acknowledged. The Forcibly acknowledge setting is helpful for clearing alarms that are currently under investigation and their acknowledgment condition is not yet cleared.
	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.

Forcing acknowledgment of all alarms

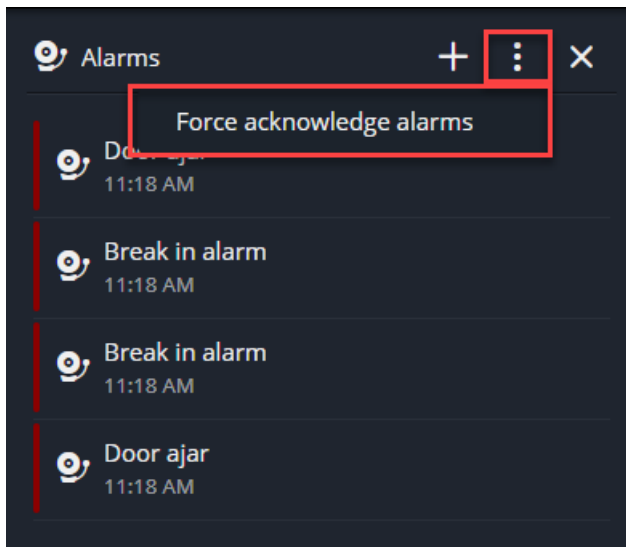
To clear all alarms across your Security Center SaaS system, you can force acknowledge all alarms in Genetec™ Operation web.

What you should know

- The **Force acknowledge alarms** button is only available to admin users.
- The **Force acknowledge alarms** button clears all alarms across your Security Center SaaS system, including:
 - Alarms that are currently under investigation.
 - Alarms that have not had their acknowledgment condition cleared.
 - Alarms that are not visible to admin users.
- You must have the *Forcibly acknowledge alarms* privilege to forcibly acknowledge alarms.

Procedure

- 1 Click the **Active alarms** (🔔) icon in the notification tray.
A side panel containing a list of active alarms opens.
- 2 Click **⋮**, and then click **Force acknowledge alarms**.



A warning message is displayed to verify if you want to forcibly acknowledge all alarms.

- 3 Click **Continue**.

All active alarms in your Security Center SaaS system are cleared.

Triggering quick actions

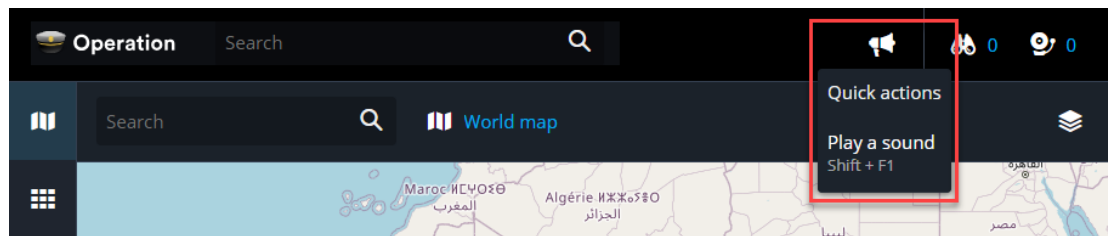
To trigger quick actions in Genetec™ Operation web, you can use the function keys on your keyboard or from the menu in the notification tray.

What you should know

- Quick actions are mapped to a function keys on a keyboard.
- Administrators must configure hot actions before the menu appears in Genetec Operation.
- Depending on your browser, some function keys might already have associated browser-based commands. To verify how to trigger your quick actions, consult the **Quick actions** (🔊) menu.

Procedure

- Do one of the following:
 - In the notification tray, click **Quick actions** (🔊) and select one from the list.



- Hold the Shift key and press a function key.
NOTE: The function key is related to the location of the quick action in the menu. For example, pressing Shift+F1 triggers the first quick action in the menu.

Setting a threat level

If a critical event occurs, such as a fire or shooting, you can set a threat level in Genetec™ Operation web.

Before you begin

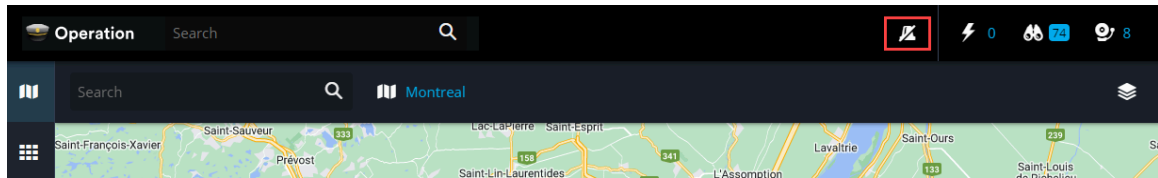
- Administrators define the threat levels that are available to Genetec Operation web.
- The *Modify threat levels* privilege is needed to set a threat level.

What you should know

- Setting a threat level can alter the state of map objects depending on the event-to-actions associated to it.

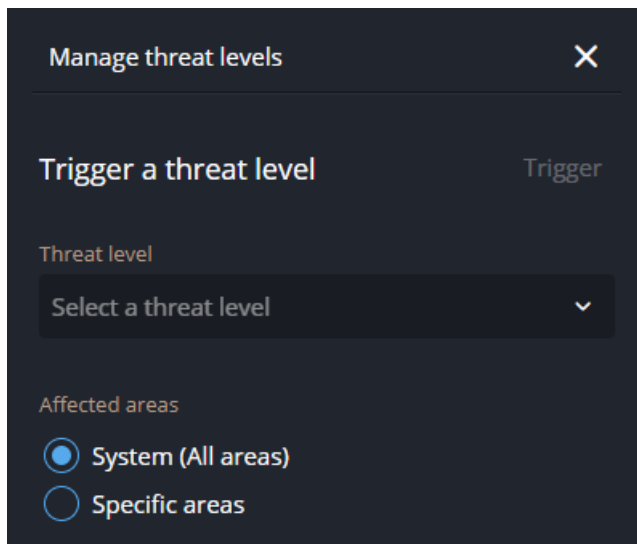
Procedure

- 1 Click **Threat levels** (🔔) in the notification tray.




The *Manage threat levels* panel opens.

- 2 From the **Threat level** list, select a threat level.
- 3 In the *Affected areas* section, choose either **System (All areas)** or **Specific areas**.



- 4 If you selected **Specific areas**, select the areas that the threat level applies to.
- 5 Click **Trigger**.
The *Trigger threat level* dialog box opens.
- 6 Click **Trigger**.
Active threat levels are displayed in the *Manage threat levels* panel.

- 7 (Optional) Deactivate a threat level:
 - a. Click **Threat levels** .
 - b. In **Manage threat levels** > **Active threat levels**, select the areas where you want to deactivate the threat level.
 - c. Click **Deactivate**.
 - d. In the *Clear threat level* dialog box, click **Deactivate**.

Event monitoring

Learn how to monitor events in Genetec™ Operation web.

This section includes the following topics:

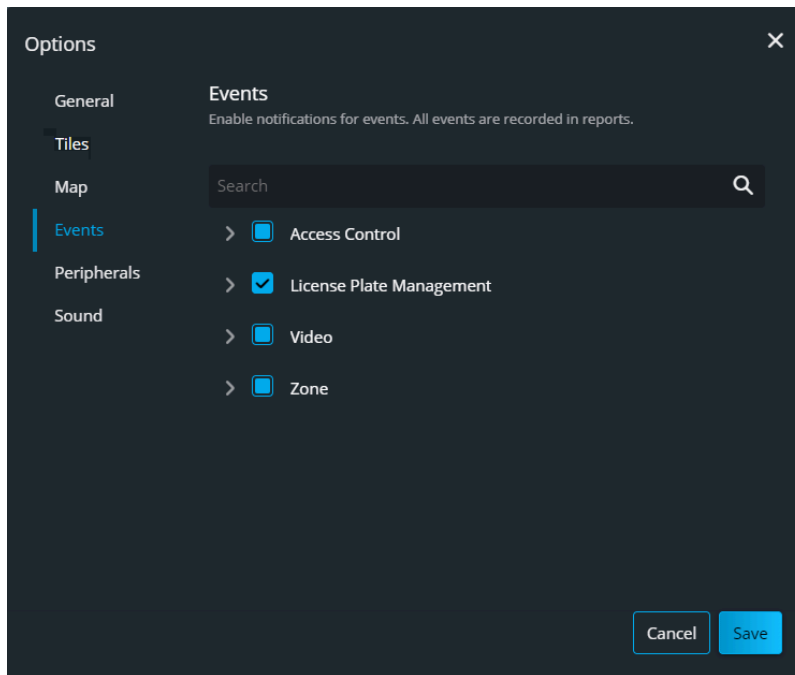
- ["Selecting event types to monitor"](#) on page 57
- ["Monitoring events using the watchlist"](#) on page 58
- ["Playing sounds with events"](#) on page 61


Selecting event types to monitor

Before you add entities to the watchlist, you must select the event types you want to monitor.

Procedure

- 1 From the homepage, click **Options** (⚙️).
The *Options* dialog box opens.
- 2 Click **Events**.
- 3 Select the general event type to see all events, or expand the list and select specific events in each category.



TIP: You can also open these options directly from the watchlist by clicking  > **Event options**.

- 4 Click **Save**.


Monitoring events using the watchlist

Using the watchlist in Genetec™ Operation web, you can monitor access control camera-related events in real-time.

Before you begin

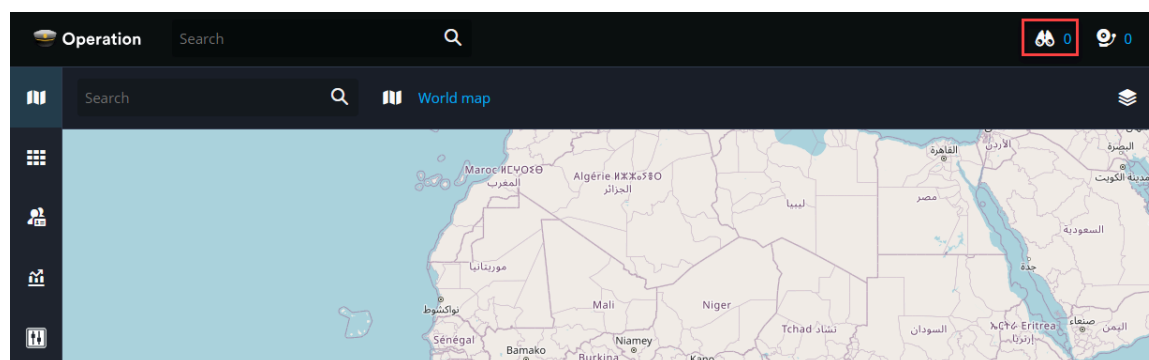
[Selecting event types to monitor](#) on page 57.

What you should know

- To monitor specific events, add the entities that trigger these events to the watchlist.
- To access your watchlist from any task, click the **Watchlist**  button in the notification tray.
- The **Watchlist** icon displays the number of missed events since the side pane was last closed. Up to 250 events can be displayed. Opening the *Watchlist* pane resets the tray number to zero.
- Events are visible in the watchlist for a maximum of 15 minutes. To view older events, generate a unified report in the *Reports* task.

Procedure

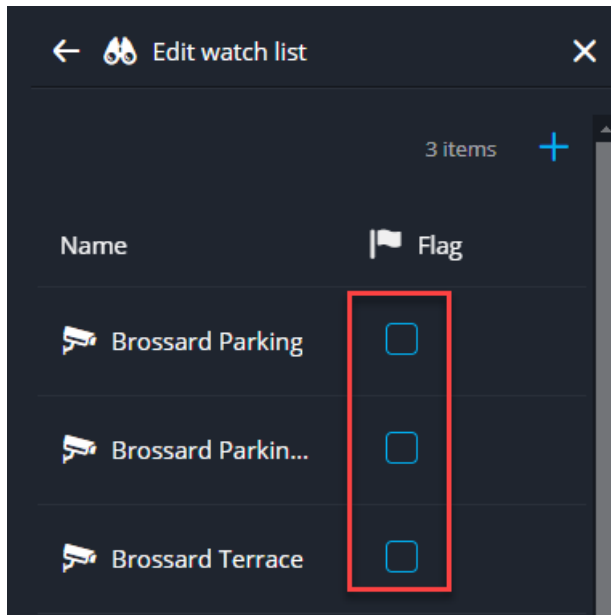
- 1 Add entities to your watchlist.
 - a. Click **Watchlist** in the notification tray.



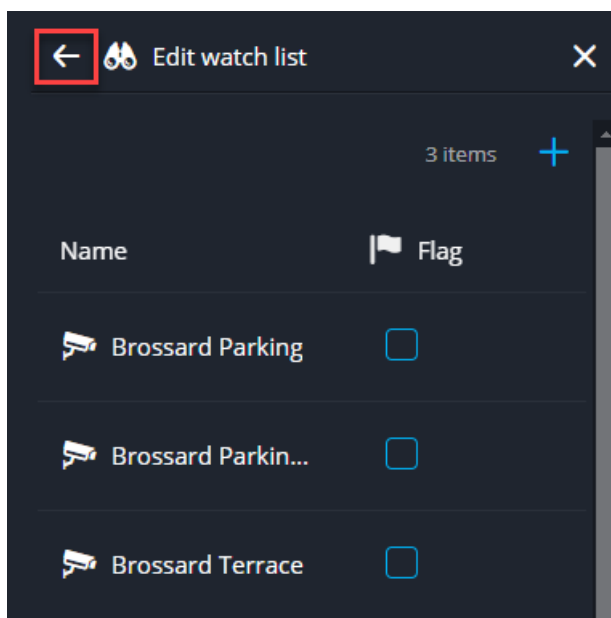
- b. Click **Add items**.
- c. From the *Select entities to watch* dialog box, select the entities related to the events you want to monitor.
- d. Click **Add**.

The entities display in the watchlist.

- 2 (Optional) To display the events related to a specific entity at the top of the list, select the **Flag** checkbox next to the entity.

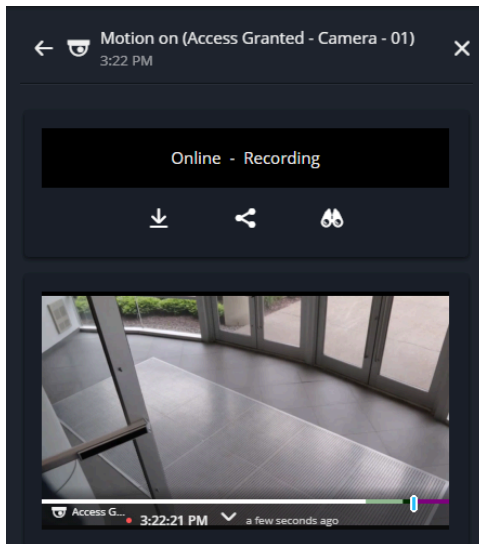


- 3 Click the back arrow.



The watchlist starts populating with events as they occur.

- 4 To view details of an event, click the event in the watchlist.
A pane opens, displaying details of the event and entity commands.



- 5 Clear the watchlist:
- Hover over an event and click **Dismiss** (✕) to remove it from the watchlist.
 - Click **⋮** > **Dismiss all** to clear the whole list.

Playing sounds with events

In Genetec™ Operation web, you can configure a sound to play when an event occurs.

Before you begin

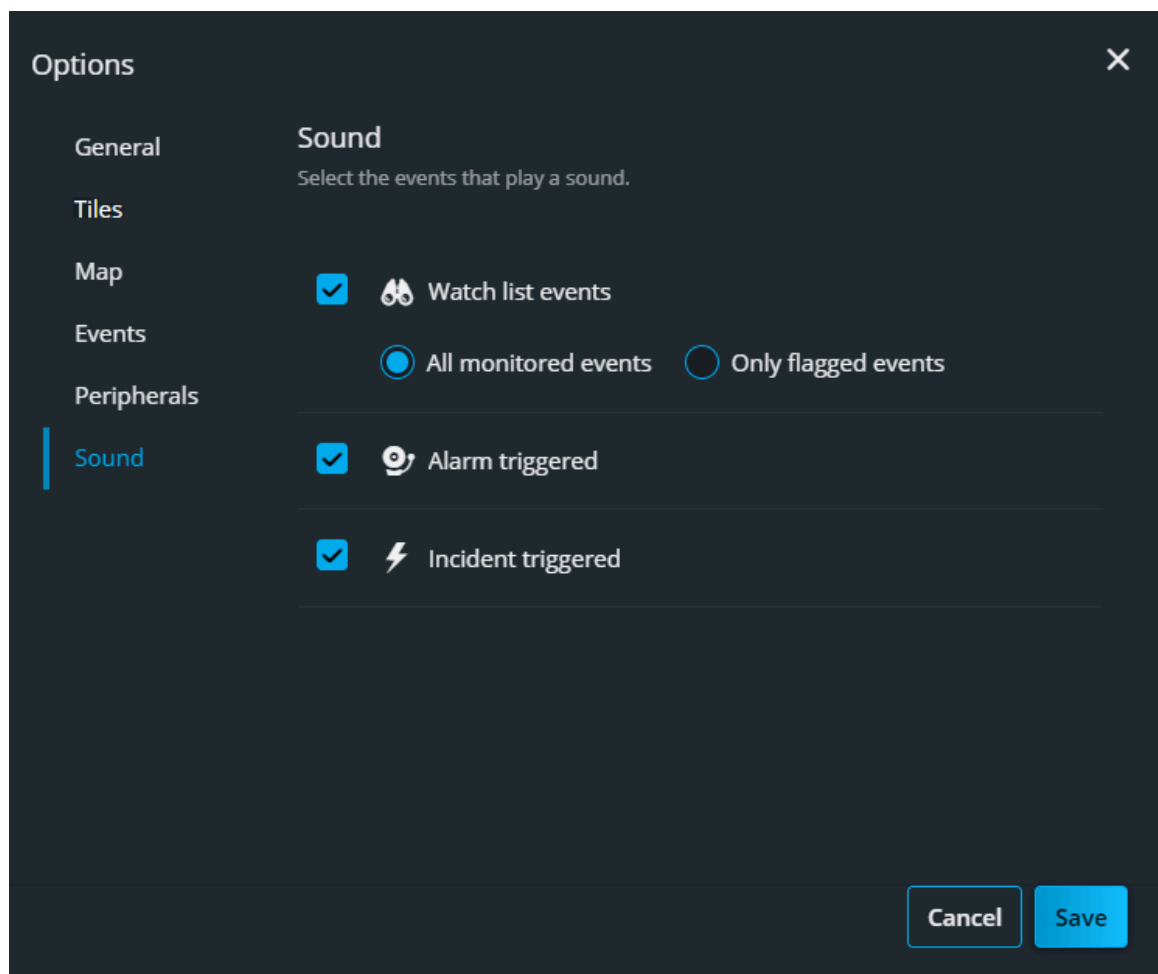
Make sure that the browser tab of Genetec Operation web is unmuted.

What you should know

- The sound that plays when an alarm or incident is triggered matches the sound selected for the related entity in Genetec™ Configuration.
- The sound used for new events plays when a watchlist event occurs.
- Sounds can be played for all watchlist events or for only flagged watchlist events.

Procedure

- 1 From the homepage, click **Options** (⚙️).
The *Options* dialog box opens.
- 2 Click **Sound**.



- 3 Select the events for which you want a sound to play.
- 4 Click **Save**.

Glossary

Access control

The *Access control* task is the administration task for configuring your access control entities, which include roles, units, cardholders, credentials, and access rules.

access rule

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.

active alarm

An active alarm is an alarm that has not yet been acknowledged.

alarm

An alarm entity informs users of a situation that requires immediate attention and provides details on 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.

alarm acknowledgment

An alarm acknowledgment is the final user response to an alarm that ends its lifecycle and removes it from the active alarm list.

antipassback

Antipassback is an access restriction placed on a secured area that prevents a cardholder from entering an area that they have not yet exited from, and vice versa.

bookmark

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.

camera

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.

cardholder

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.

cardholder group

A cardholder group is an entity that defines the common access rights of a group of cardholders.

Config Tool

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.

credential

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.

custom event

A custom event is an event added after the initial system installation. Events defined at system installation are called system events. Custom events can be user-defined or automatically added through plugin installations. Unlike system events, custom events can be renamed and deleted.

door

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 *In* and *Out* by default. Each side is an access point (entrance or exit) to a secured area.

door contact

A door contact monitors the state of a door, whether it is open or closed. It can also be used to detect an improper state, such as door open too long.

door side

Every door has two sides, named *In* and *Out* by default. Each side is an access point to an area. For example, passing through one side leads into an area, and passing through the other side leads out of that area. For the purposes of access management, the credentials that are required to pass through a door in one direction are not necessarily the same that are required to pass through in the opposite direction.

entity

An entity represents anything in your system that requires configuration. This can be 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.

event

An event is a notification that informs the user about an activity or incident that occurred within their system.

event-to-action

An event-to-action links an action to an event. For example, you can configure an alarm to trigger when a door is forced open.

failover

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.

Federation™

Federation™ joins multiple, independent Genetec™ security systems into a single virtual system. With this feature, users on a central system, called the Federation host, can view and control entities that belong to remote systems.

Federation™ host

The Federation™ host is the Security Center or Security Center SaaS system that runs Federation™ roles. Users on the Federation™ host can view entities that belong to federated systems and control the entities directly from their system.

Genetec Configuration

Genetec™ Configuration is the Security Center SaaS administrative application used to manage all Security Center SaaS users and to configure all Security Center SaaS entities such as areas, cameras, doors, schedules, cardholders, and hardware devices.

Genetec Operation

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

incident category

An incident category is an entity that represents a grouping of incident types that have similar characteristics.

map

A map is a two-dimensional diagram that visualizes physical locations. Maps typically show your security equipment in a geographical area or in building floorplans.

map link

A map link is a map object that brings you to another map with a single click.

map object

Map objects graphically represent entities, cities, highways, and other geographical features on maps. Using map objects, you can interact with your system without leaving the map.

map preset

A map preset is a saved map view. Every map has at least one preset, called the *default view*, that is displayed when a user opens the map.

Maps

The *Maps* task is an operation task that heightens your situational awareness by providing the context of a map to your security monitoring and control activities.

Media Router

The Media Router is the central role that handles all audio and video stream requests in Security Center or Security Center SaaS. It establishes streaming sessions between the stream source, such as a camera or an Archiver role, and the client applications that request the sessions. The location and transmission capabilities of each party determine the routing decisions.

privacy protection

In Security Center, privacy protection is software that anonymizes or masks parts of a video stream where movement is detected. The identity of individuals or moving objects is protected, without obscuring movements and actions or preventing monitoring.

redirector

A redirector is a server assigned to host a redirector agent created by the Media Router role.

redirector agent

A redirector agent is an agent created by the Media Router role to redirect data streams from one IP endpoint to another.

Reports

The Reports task enables users to generate customized queries about entities, activities, and events for investigation or maintenance purposes.

reverse tunnel

A reverse tunnel is a private communication channel open between a server inside a secured LAN and a client outside. In the Security Center implementation, certificate authentication is used to protect against manipulator-in-the-middle attacks.

Reverse Tunnel

The Reverse Tunnel role is used on the federated system to connect to the Federation™ host residing in the cloud. The connection is established using a keyfile generated from the cloud system. The keyfile can only be used once to ensure maximum security.

reverse tunneling

Reverse tunneling is a method of securing communication between clients and servers that are behind a firewall. This technique enhances security and simplifies firewall management. When using a reverse tunnel, the server initiates a connection to the client. This tunnel connection is secured by a previously shared keyfile that contains an identity certificate. When established, the reverse tunnel allows bidirectional communication without opening inbound firewall ports.

Reverse Tunnel Server

The Reverse Tunnel Server role is used on the Federation™ host to manage reverse tunnels. Reverse tunnels are created using this role, but must be opened from the federated sites using the Reverse Tunnel roles.

role

A role is a software component that performs a specific job within Security Center or Security Center SaaS.

Security Center

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.

Security Center Federation™

The Security Center Federation™ role connects the local system to an independent remote Security Center system. After connecting to the remote system, your local system acts as the Federation™ host and you can view federated entities and events locally.

Security Center SaaS

Security Center SaaS is a unified hybrid-cloud solution offering physical security as a service. It integrates advanced security capabilities, emphasizes cybersecurity and privacy, and manages complex security tasks on premises, in the cloud, or both. With the flexibility of Security Center SaaS, organizations can efficiently monitor and respond to security threats from one place.

task

A task is a customizable user interface designed to handle a specific aspect of your work. For example, you can employ a monitoring task to observe real-time system events, an investigation task to identify suspicious activity, or an administration task to configure system settings.

threat level

A threat level warns system users of changing security conditions, such as a fire or a shooting, in a specific area or the entire system. Specific handling procedures can be automatically applied when a threat level is raised or canceled.

tile

A tile is an individual window within the canvas, used to display a single entity. The entity displayed is typically the video from a camera, a map, or anything of a graphical nature. The look and feel of the tile depends on the displayed entity.

tile ID

The tile ID is the number displayed at the upper left corner of the tile. This number uniquely identifies each tile within the canvas.

tile pattern

The tile pattern is the arrangement of tiles within the canvas.

user

A user is an entity that represents a person with access to your system. System administrators create user entities and configure their rights and privileges on the system.

user group

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.

zone

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.

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.
- **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](#). Unable to find what you are looking for? Contact documentation@genetec.com.

- **Genetec Technical Assistance Center (GTAC):** Contacting GTAC is described in the [Genetec Advantage Description](#).

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>.

Hardware product issues and defects

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