AXIS Perimeter Defender with Genetec VMS

User Manual

Table of Contents

About VMS integration

About VMS integration

The Integration Pack allows seamless integration between AXIS Perimeter Defender and Genetec Security Center. Alarms triggered by AXIS Perimeter Defender are automatically converted to Security Center Custom Events, which in turn can trigger a wide set of actions and leverage the full power of the Security Center system. Simultaneously, the live metadata generated by AXIS Perimeter Defender is sent to Security Center for live display and recording. Therefore, the metadata is also available when playing the recorded video sequences in playback mode.

Installation host

To integrate AXIS Perimeter Defender and Security Center you need two software modules running on the Genetec Security Center server. You can also use another server connected by LAN to both the Axis cameras running AXIS Perimeter Defender and the Genetec Security Center server.

- AXIS Perimeter Defender runs as a Windows® service feeding the Security Center server with the metadata from the cameras. The Security Center server then saves the metadata, making it available for live stream and playback.
- The Metadata Bridge Configuration Tool is a graphical interface where you can configure the Metadata Bridge and enter the credentials and network addresses of the AXIS Perimeter Defender servers, if there are any.

Prerequisites

Global prerequisites

To successfully integrate AXIS Perimeter Defender with Genetec Security Center, the following requirements must be met:

- A working, correctly licensed, and configured Genetec Security Center server (at least 5.4 SR4 CU5 or 5.5 SR5 CU3).
- One or several Axis cameras running AXIS Perimeter Defender. The Axis cameras must be connected to and configured within Security Center.

Note

Even if AXIS Perimeter Defender is not calibrated you can still configure the AXIS Perimeter Defender Genetec Security Center Integration Pack. Note that AXIS Perimeter Defender must be configured before any alarms or metadata can be sent to the Security Center.

- At least one SDK connection license must be available within the Security Center. See *Licenses on page 5* .
- You must be able to install the Genetec SDK corresponding to your Security Center version on the host where you plan to install the AXIS Perimeter Defender Genetec Security Center Integration Pack. See *Installation host on page 3* .

Software prerequisites

The integration pack has the following prerequisites:

- Microsoft .net 4.5.1 must be available on the PC where the integration pack is installed. If it is not available, it will be automatically installed by the integration pack installer.
- Genetec Security Center 5.4 SR4 CU5 or 5.5 SR5 CU3 or a later version
- AXIS Perimeter Defender 1.2.1 or a later version
- The Genetec Security Center SDK Redistributable corresponding to the installed Security Center version must be installed on the server where the AXIS Perimeter Defender Genetec Security Center Integration Pack is installed. To obtain the Security Center Redistributable SDK, contact your Genetec representative.
- SDK connection license

About VMS integration

Limitations

Important

The current version of Security Center is able to process a limited number of metadata frames per second and per archiver (an indicative limit is 50 frames/second per archiver, independently from the number of connected cameras). AXIS Perimeter Defender sends metadata frames at 0.1 frames/second for cameras with no human activity (no actors moving in the field of view) and at 8 frames/second for cameras with human activity. This means that, depending on the number of AXIS Perimeter Defender cameras connected to the archiver and the relative activity in their field of view, the Security Center limit can be reached or not. If reached, the Alarm & Metadata Bridge automatically lowers the metadata frequency when sending metadata to Security Center, and this might result in jolting metadata rendering in the Security Desk.

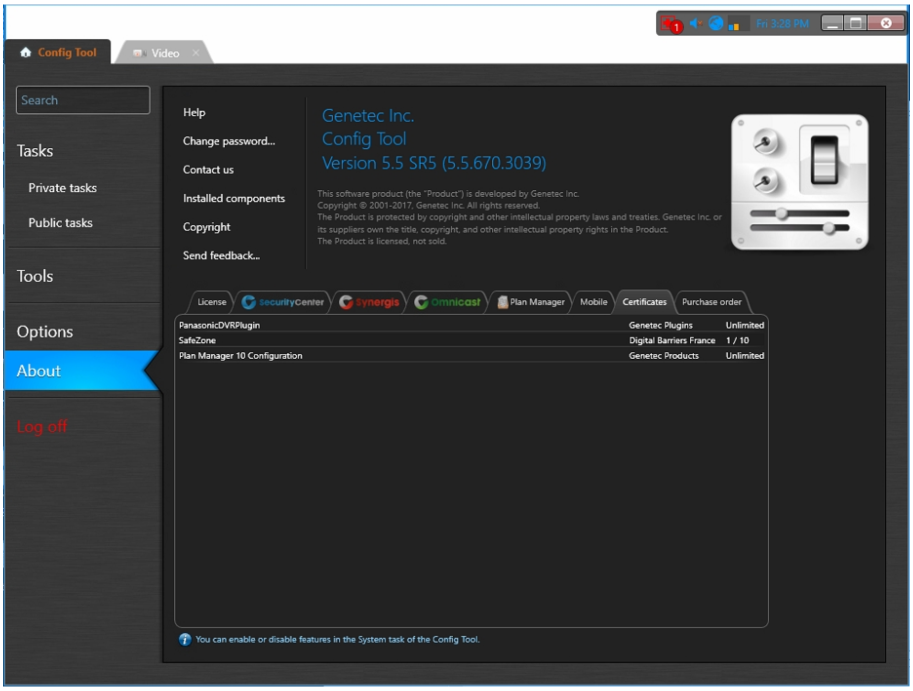
Licenses

Licenses

The AXIS Perimeter Defender Alarm & Metadata Bridge consists of two applications:

- A background windows service running around the clock, called **AXIS Perimeter Defender Alarm & Metadata Bridge**
- A graphical interface used to configure the service, called **Metadata Bridge Configuration Tool**

While running, both applications need a valid SDK connection license from Security Center to be able to connect to it. The SDK license is called "GSC-1SDK-Axis-PerimeterDefend". To find the license, go to **Config Tool** > **About** > **Certificates**.



Genetec Inc.
Config Tool
Version 5.5 SR5 (5.5.670.3039)

This software product (the "Product") is developed by Genetec Inc.
Copyright © 2001-2017, Genetec Inc. All rights reserved.
The Product is protected by copyright and other intellectual property laws and treaties. Genetec Inc. or its suppliers own the title, copyright, and other intellectual property rights in the Product.
The Product is licensed, not sold.

PanasonicDVRPlugin	Genetec Plugins	Unlimited
SafeZone	Digital Barriers France	1 / 10
Plan Manager 10 Configuration	Genetec Products	Unlimited

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

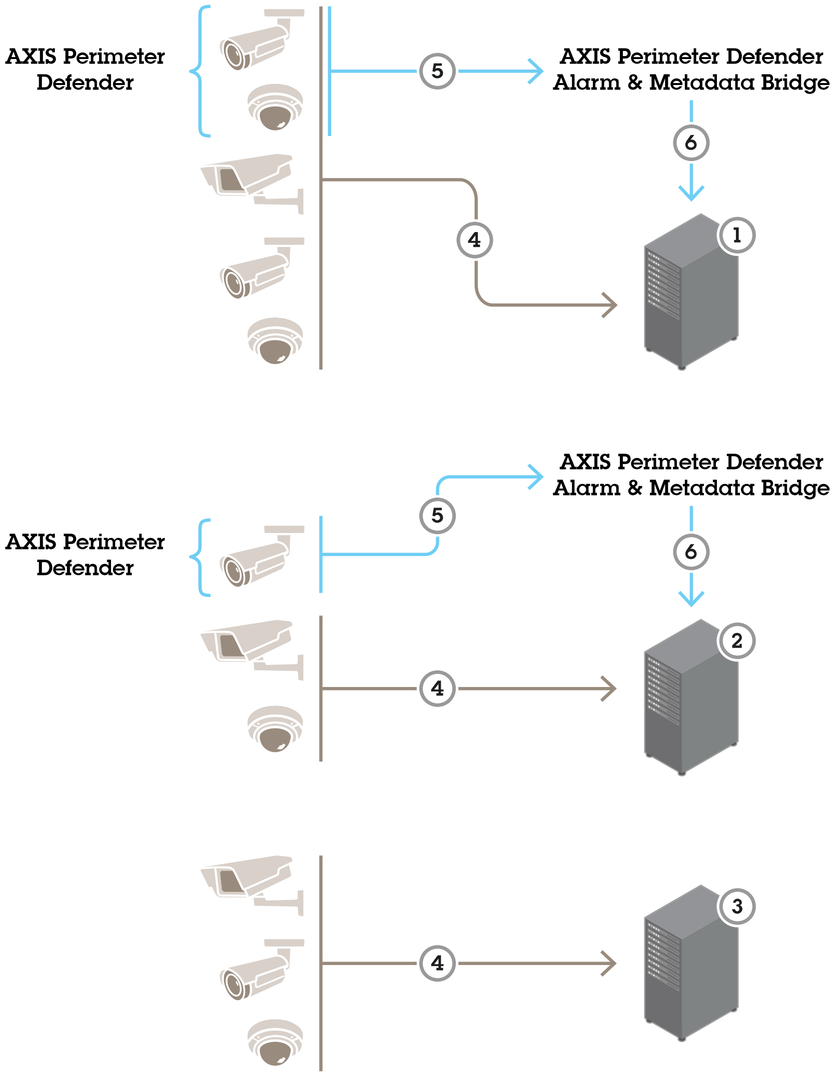
This screenshot shows a system that has ten installed licenses.

Installation scenario

A typical system consists of a Security Center server connected to a number of cameras. If one or more of these cameras are running AXIS Perimeter Defender, you must install AXIS Perimeter Defender Alarm & Metadata Bridge on that server.

In this installation scenario, two of the Security Center servers are connected to one or more cameras that run AXIS Perimeter Defender. Each server needs one instance of the AXIS Perimeter Defender Alarm & Metadata Bridge. The server connected to cameras that do not run AXIS Perimeter Defender does not need AXIS Perimeter Defender Alarm & Metadata Bridge.

Licenses


AXIS Perimeter Defender
AXIS Perimeter Defender Alarm & Metadata Bridge
5
6
1
4
AXIS Perimeter Defender Alarm & Metadata Bridge
AXIS Perimeter Defender
5
6
2
4
3
4

In this installation scenario, a total amount of eleven cameras are split across three security center servers.

1	*Security center server*
2	*Security center server*
3	*Security center server*
4	*Video stream*
5	*Metadata stream*
6	*Security center custom events and metadata overlay*

The AXIS Perimeter Defender Alarm & Metadata Bridge can be installed directly on the Genetec server or on a separate server.

How many licenses do I need?

The amount of licenses depends on the installation scenario. There are two options:

- We recommend to install at least two SDK connection licenses on every Genetec Security Center server to which the AXIS Perimeter Defender Alarm & Metadata Bridge connects. In the installation scenario, you would then need to install two licenses on the Security Center server 1 and two other licenses on the Security Center server 2, i.e. a total of four licenses. The third server does not need any license, as there is no AXIS Perimeter Defender Alarm & Metadata Bridge connecting to it.

Licenses

- A more cost-effective approach is to install only one license on every Security Center server to which the AXIS Perimeter Defender Alarm & Metadata Bridge connects. The constraint of this approach is that you must manually stop the AXIS Perimeter Defender Alarm & Metadata Bridge service before opening the Metadata Bridge Configuration Tool. The license that is used by the service is released when the service is stopped and can temporarily be used by the Metadata Bridge Configuration Tool. This means you must remember to restart the service again once you've finished with the configuration and you've closed the Metadata Bridge Configuration Tool.

How to buy licenses

The licenses can be purchased from Genetec. We recommend that you contact your Genetec sales representative, mentioning that you want to purchase SDK licenses named "GSC-1SDK-Axis-PerimeterDefend".

Installation

The installation setup file "AXIS Perimeter Defender Security Center Integration Pack X.Y.Z.W.exe" installs both AXIS Perimeter Defender Metadata Bridge and the Metadata Bridge Configuration Tool. The installer automatically takes care of all the necessary files and settings on the destination machine. To execute the installer, double-click the file and go through the installation screens. The default values of each field suit the majority of the standard installations.

AXIS Perimeter Defender configuration

The Alarm & Metadata Bridge can automatically retrieve and configure all Axis devices running AXIS Perimeter Defender by scanning the list of Axis devices connected to the Security Center. Moreover, the Alarm & Metadata Bridge automatically associates every AXIS Perimeter Defender alarm or metadata stream to the corresponding Genetec Video Source (i.e. the Axis device that runs AXIS Perimeter Defender). Therefore, no manual configuration steps are needed for AXIS Perimeter Defender.

About Metadata Bridge configuration

The Metadata Bridge can automatically retrieve and configure all the Axis cameras running AXIS Perimeter Defender by scanning the list of cameras connected to the Security Center. The Metadata Bridge automatically associates every AXIS Perimeter Defender alarm or metadata stream to the corresponding Genetec Video Source, i.e. the Axis camera where AXIS Perimeter Defender runs. Therefore, no manual configuration steps are required for AXIS Perimeter Defender.

AXIS Perimeter Defender generates metadata information that helps the security operator understand what is happening in the field of view of the camera. These metadata can be sent to Security Center for display and recording through the Metadata Bridge.

The bridge automatically subscribes to the metadata generated by the Axis camera running AXIS Perimeter Defender. If these cameras are connected to Security Center, the bridge then sends the metadata to Security Center that displays them on top of the corresponding video streams and archives them alongside the video footages to be able to overlay them again when playing back the video sequence.

Metadata does not require any special configuration, the Metadata Bridge automatically manages the necessary configuration automatically.

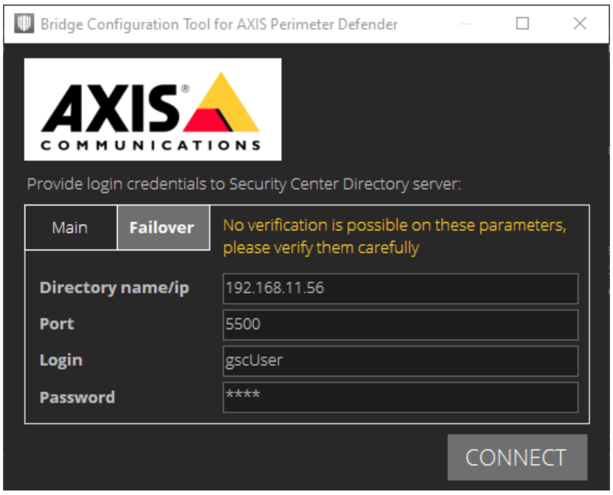
About failover options

When a Security Center system is configured with one or more failover servers for the Directory role, all the logged applications (including the Alarm & Metadata Bridge) automatically and transparently redirects to the failover server for the Directory role in case the main server fails. However, the redirection can take time, especially in large systems where the failover server must handle many simultaneous login requests. During redirection, the Alarm & Metadata Bridge is disconnected from Security Center and thus not operational.

To speed up the redirection, you can provide the Alarm & Metadata Bridge with the credentials of one of the failover servers for the Directory role. Whenever the Alarm & Metadata Bridge is disconnected from Security Center, or has problems logging into the main server, it will automatically switch to the failover server for the Directory role and log into it. This operation is usually quicker than the automatic redirection that Security Center provides.

When the main server comes back online, and depending on how the failover policy is configured, the failover server for the Directory role may automatically go offline. In this case, a second redirection from the failover to the main server occurs, with the same modality as the first switch.

You can enter the credentials of the failover server for the Directory role in the **Failover** tab of the login window in the Bridge Configuration Tool:



Provide login credentials to Security Center Directory server:

No verification is possible on these parameters, please verify them carefully

Directory name/ip 192.168.11.56

Port 5500

Login gscUser

Password ****

Note

- You must always provide credentials for the main server. The failover server credentials are optional.
- You can't test the failover credentials by clicking **CONNECT**, because when the main server is online, the failover server for the Directory role does not accept login requests. Therefore it's important to enter the correct credentials. If the credentials are wrong, the redirection from a failing server to a working one can take much longer than if a failover server has not been specified at all.

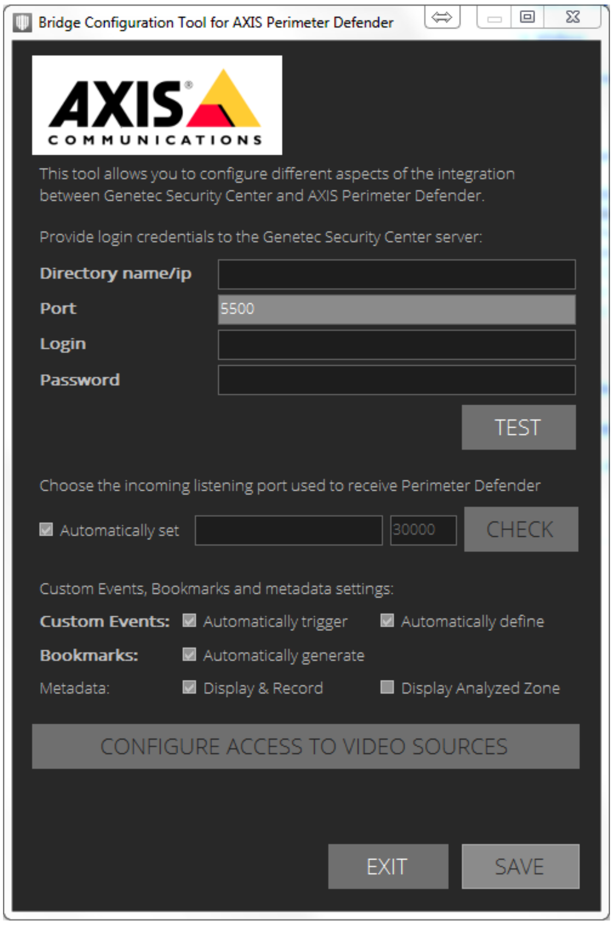
Special notes

When testing the credentials, the Metadata Bridge Configuration Tools needs for a short time an SDK connection license of type “GSC-1SDK-Axis-PerimeterDefend” to be able to connect to the Security Center Service. The AXIS Perimeter Defender Metadata Bridge also, if running, needs such a license. This means, if both of them are running and there is only one SDK connection license available, the Metadata Bridge Configuration Tool will not be able to connect to the Security Center server and will report an error, even if the provided credentials are correct. In this case, temporarily stop the AXIS Perimeter Defender Metadata Bridge service, run the tests and then restart the service.

How to log in

Enter the username and password for the Security Center server:

Installation



This tool allows you to configure different aspects of the integration between Genetec Security Center and AXIS Perimeter Defender.

Provide login credentials to the Genetec Security Center server:

Directory name/ip

Port 5500

Login

Password

Choose the incoming listening port used to receive Perimeter Defender

☑ Automatically set 30000

Custom Events, Bookmarks and metadata settings:

Custom Events: ☑ Automatically trigger ☑ Automatically define

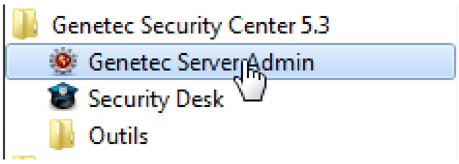
Bookmarks: ☑ Automatically generate

Metadata: ☑ Display & Record ☐ Display Analyzed Zone

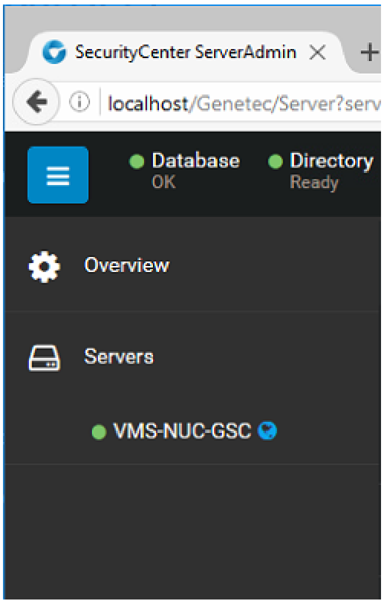
The screenshot is taken from a GSC 5.5 installation. If you are using GSC 5.4, the interface does not display the "Configure Access To Video Sources" button as this step is not necessary with 5.4.

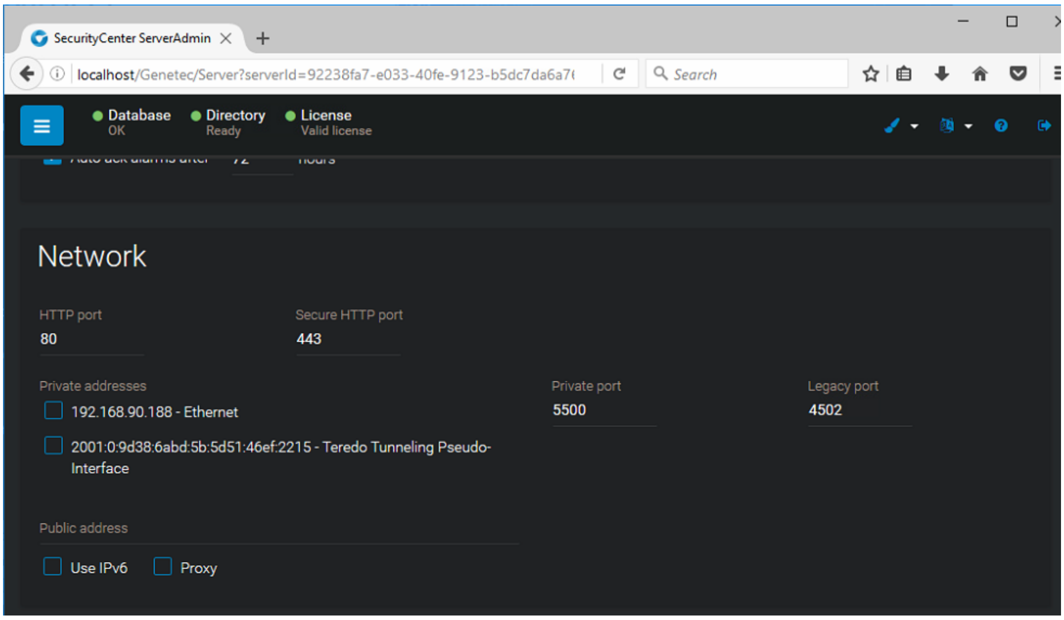
- **Directory name/ip** is the ip address, for example 192.168.1.100, or name (server.domain.com) of the Security Center server. If the Metadata Bridge is installed on the same machine as Security Center, the IP address "127.0.0.1" can be used.

- **Port** is the port where Security Center listens for the incoming SDK connection. To find the correct port number, go to **Security Center Server > Genetec Server Admin > Incoming Connection Port**. When in doubt, leave the default value of 5500.



Installation




SecurityCenter ServerAdmin
localhost/Genetec/Server?serverId=92238fa7-e033-40fe-9123-b5dc7da6a7(
Search
Database
OK
Directory
Ready
License
Valid license

Network

HTTP port: 80

Secure HTTP port: 443

Private addresses

□ 192.168.90.188 - Ethernet

□ 2001:0:9d38:6abd:5b:5d51:46ef:2215 - Teredo Tunneling Pseudo-Interface

Private port: 5500

Legacy port: 4502

Public address

□ Use IPv6 □ Proxy

- **Login** is the login of a user with administrative rights. If Security Center is configured to accept Windows domain logins, and you want to use those, add the domain name: “DOMAIN\User”.
- **Password** is the password corresponding to the user.

We recommend using the **Test** button to be sure that the provided credentials work as expected. Potential issues, besides the most evident ones like wrong login or wrong password, are:

- The Security Center does not have the SDK connection license which means the Metadata Bridge Configuration Tool can’t connect to the Security Center server.
- The Security Center server has stopped.
- If AXIS Perimeter Defender Bridge is installed on another machine, the network connection could be lost.

- All the available SDK connection licenses are in use (for example, the Metadata Bridge is using the unique available license). See *Special notes on page 9* .

Important

If the connection credentials are modified, the AXIS Perimeter Defender Metadata Bridge service needs to be restarted in order to use the new values.

Listening port for alarms

The Metadata Bridge automatically configures the different AXIS Perimeter Defender instances running on Axis cameras connected to the Security Center system so that they send alarms on a given port of the PC where the metadata bridge is installed. The default port is 10000. It does not need to be changed except if this port is already used by a different application.

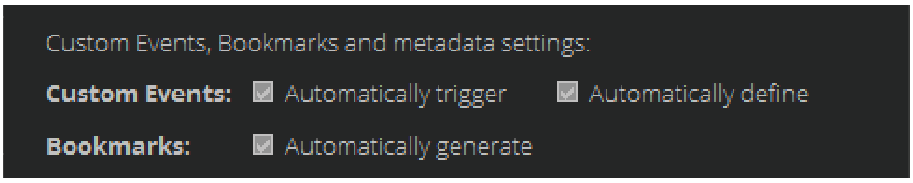
Important

If the listening port is modified, you must restart the AXIS Perimeter Defender Metadata Bridge service.

At the integration pack installation, a rule allowing incoming connections to any listening port of the Metadata Bridge is automatically added to the Windows® Firewall. The rule can be removed by a successive installation or blocked by some antivirus. Make sure that there is connection from the external world to the chosen listening IP port each time this is changed.

How to configure custom events

The following part of the Metadata Bridge Configuration Tool interface allows you to configure what default actions should be triggered by the Metadata Bridge when it receives an alarm from AXIS Perimeter Defender:



Custom Events, Bookmarks and metadata settings:

Custom Events: ☑ Automatically trigger ☑ Automatically define

Bookmarks: ☑ Automatically generate

For the Security Center to receive a custom event, these following conditions need to be fulfilled at the same time:

- To be defined
- To be triggered

The settings on the **Custom Event** line allows you to configure both actions:

- If you do not want to receive a custom event when AXIS Perimeter Defender triggers an alarm (for example, because Security Center already receives the AXIS Perimeter Defender alarms by another mean), clear **Automatically trigger**.

  If a Genetec Custom Event corresponding to the received AXIS Perimeter Defender alarm exists and you want to receive a custom event when AXIS Perimeter Defender triggers an alarm, select **Automatically trigger**.

- If you want all the necessary **Custom Events** to be automatically generated by the tool so they can be triggered when the corresponding AXIS Perimeter Defender alarm is received, select **Automatically define**.

  If you plan to manually define (a subset of) the necessary **Custom Events**, clear **Automatically define**.

The complete list of **Custom Events**:

- Axis Perimeter Defender Intrusion Start
- Axis Perimeter Defender Intrusion Stop
- Axis Perimeter Defender Loitering Start
- Axis Perimeter Defender Loitering Stop

- Axis Perimeter Defender Zone-Crossing Start
- Axis Perimeter Defender Zone-Crossing Stop
- Axis Perimeter Defender Conditional Start
- Axis Perimeter Defender Conditional Stop

Important

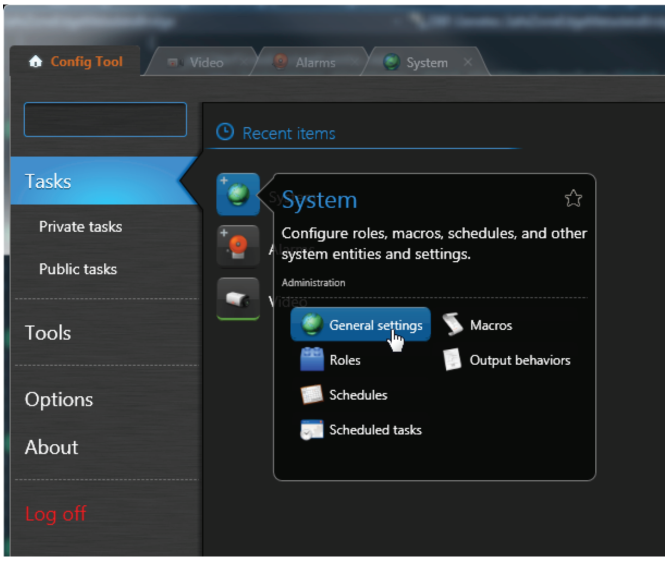
If you choose to define the **Custom Events** manually, it is important that the name of the custom event respects the following rules:

- The name must contain the “Axis” string.
- The name must contain one of the following strings: “Intrusion”, “Loitering”, “Zone-crossing”, “Conditional”.
- The name must contain one of the following strings: “Start”, “Stop”.

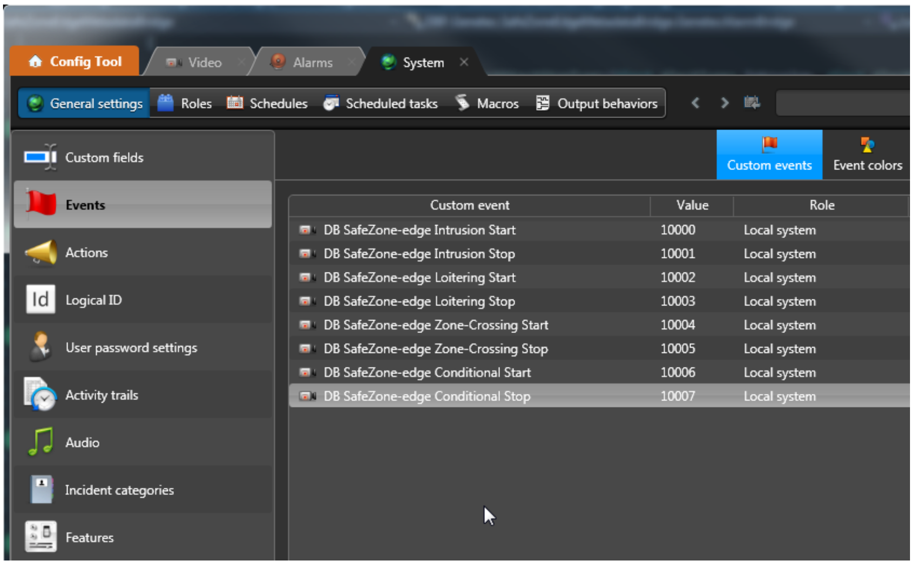
For these three rules, the comparison is done in a case-insensitive manner. The **Custom Event ID** number is irrelevant, choose the one you want.

If you only want a subset of the custom events, for example be notified only when an alarm starts but not when it stops, but you do not want to define the custom events manually, do the following:

1. Select **Automatically define** .
2. Open the Genetec Config Tool and go to **System** > **General Settings** > **Events**.



Configure roles, macros, schedules, and other system entities and settings.



Custom event	Value	Role
DB SafeZone-edge Intrusion Start	10000	Local system
DB SafeZone-edge Intrusion Stop	10001	Local system
DB SafeZone-edge Loitering Start	10002	Local system
DB SafeZone-edge Loitering Stop	10003	Local system
DB SafeZone-edge Zone-Crossing Start	10004	Local system
DB SafeZone-edge Zone-Crossing Stop	10005	Local system
DB SafeZone-edge Conditional Start	10006	Local system
DB SafeZone-edge Conditional Stop	10007	Local system

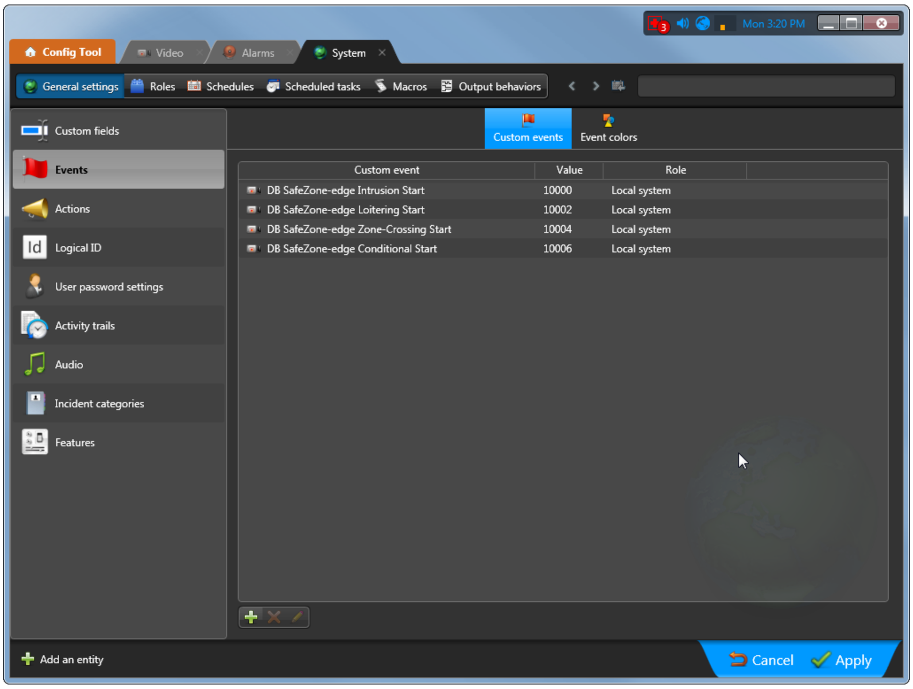
3. Make sure all of the custom events are defined in the list.

4. Clear **Custom Events Define missing ones** in the Metadata Bridge Configuration Tool.

5. Delete the Custom Events you don't want from the Genetec Config Tool, i.e. the four "Stop" custom events in this example.

6. To save the settings, click **Apply**.

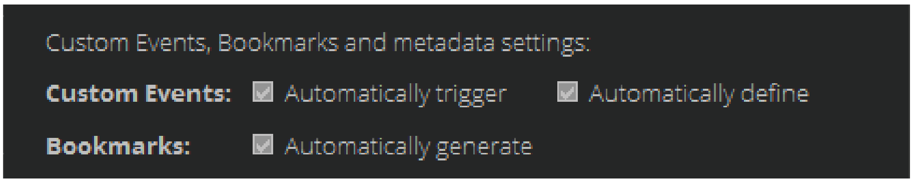
7. For the change to apply, restart the Security Center service.



Custom event	Value	Role
DB SafeZone-edge Intrusion Start	10000	Local system
DB SafeZone-edge Loitering Start	10002	Local system
DB SafeZone-edge Zone-Crossing Start	10004	Local system
DB SafeZone-edge Conditional Start	10006	Local system

How to generate bookmarks

If you want a bookmark to be automatically generated by the Metadata Bridge each time it receives an Alarm Start from AXIS Perimeter Defender, go to Metadata Bridge Configuration Tool > Bookmarks and select **Automatically generate**.



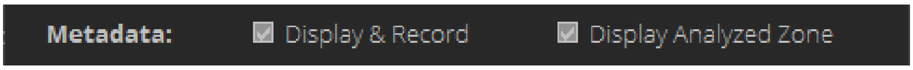
Custom Events, Bookmarks and metadata settings:

Custom Events: ☑ Automatically trigger ☑ Automatically define

Bookmarks: ☑ Automatically generate

A bookmark with label "AXIS Perimeter Defender {alarm_type}" ({alarm_type} being "Intrusion" or "Loitering" or "Zone-crossing" or "Conditional") will be created in the associated video stream (i.e. the one coming from the camera where AXIS Perimeter Defender has generated the alarm).

About metadata display



Metadata: ☑ Display & Record ☑ Display Analyzed Zone

The following options are available:

- If you clear **Display & record**, the Smart Client does not display the metadata and the recording server does not record them.
- If you select **Display analyzed zone**, the boundary of the image that is analyzed by AXIS Perimeter Defender is displayed as part of the overlay .

How to configure access to video sources

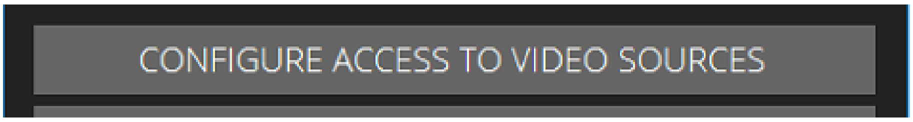
Note

This section only applies to GSC 5.5.

Configure access to video sources

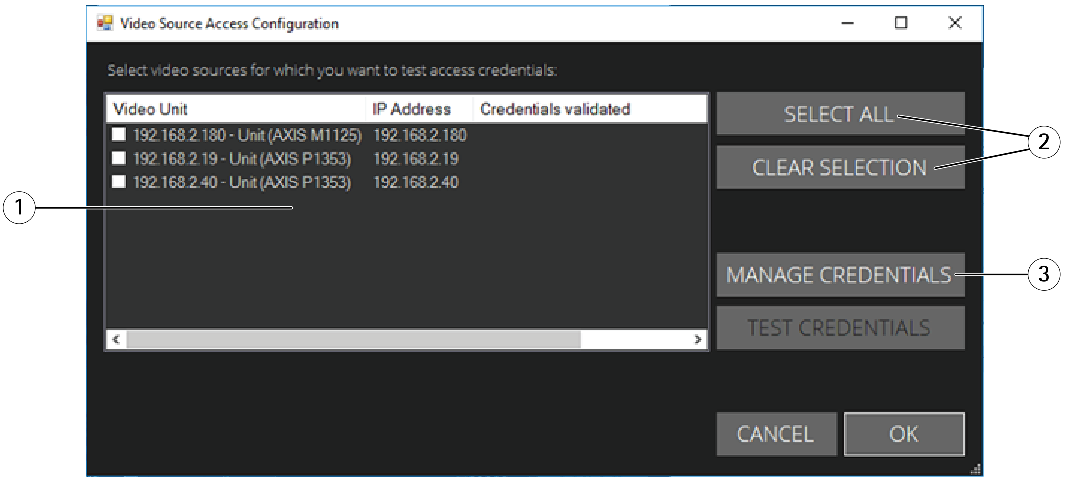
Provide the credentials that allows the bridge to access AXIS Perimeter Defender on the Axis cameras. Usually this means providing the credentials of a user who has administrator rights on the camera.

1. To access the settings, click **Configure access to video sources.**



2. Connect to GSC by clicking the **Test credentials** button.
3. In the list of devices, select individual cameras with AXIS Perimeter Defender or click **Select all**.
4. Click **Manage credentials** .

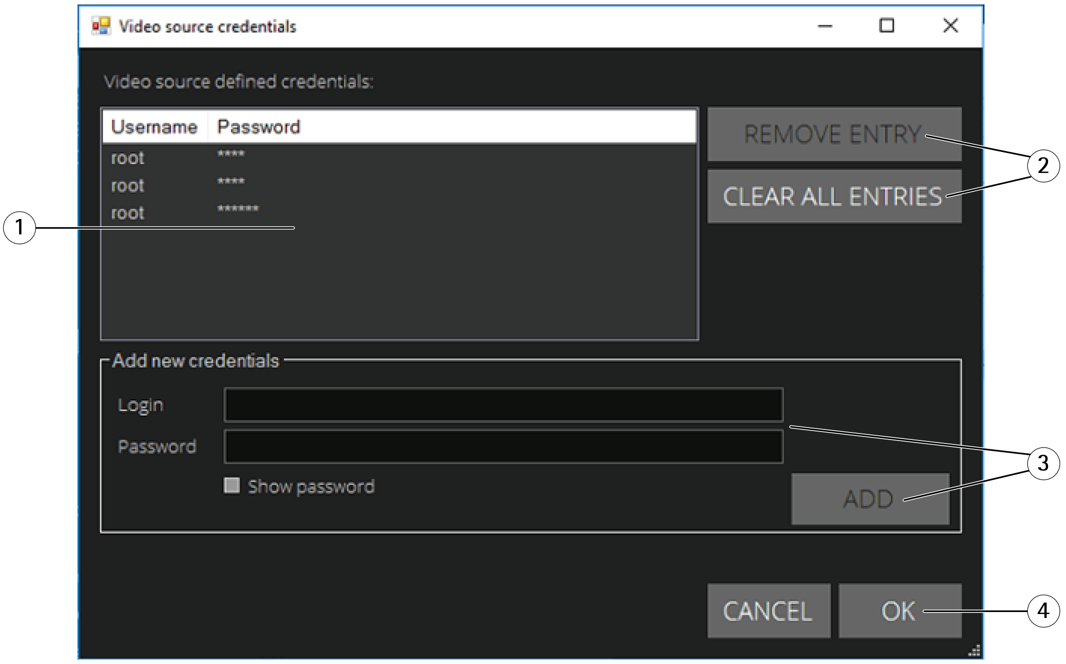
Installation



Select video sources for which you want to test access credentials:

Video Unit	IP Address	Credentials validated
□ 192.168.2.180 - Unit (AXIS M1125)	192.168.2.180	
□ 192.168.2.19 - Unit (AXIS P1353)	192.168.2.19	
□ 192.168.2.40 - Unit (AXIS P1353)	192.168.2.40	

This list shows all the Axis cameras defined in the Security Center system.



Video source defined credentials:

Username	Password
root	****
root	****
root	******

Login

Password

□ Show password

This lists the usernames and passwords that have already been defined. The provided usernames and passwords are saved in an encrypted container and can be loaded by the application at the next execution. For security reasons, passwords are never displayed in plain text and it is not possible to get the plain text version of a saved password.

How to remove credentials

5. To remove a username and password, select in the list and then click **Remove entry**.

6. To remove all usernames and passwords, click **Clear all entries**.

How to add credentials

7. Enter username and password. To display the password in plain text, select **Show password**.

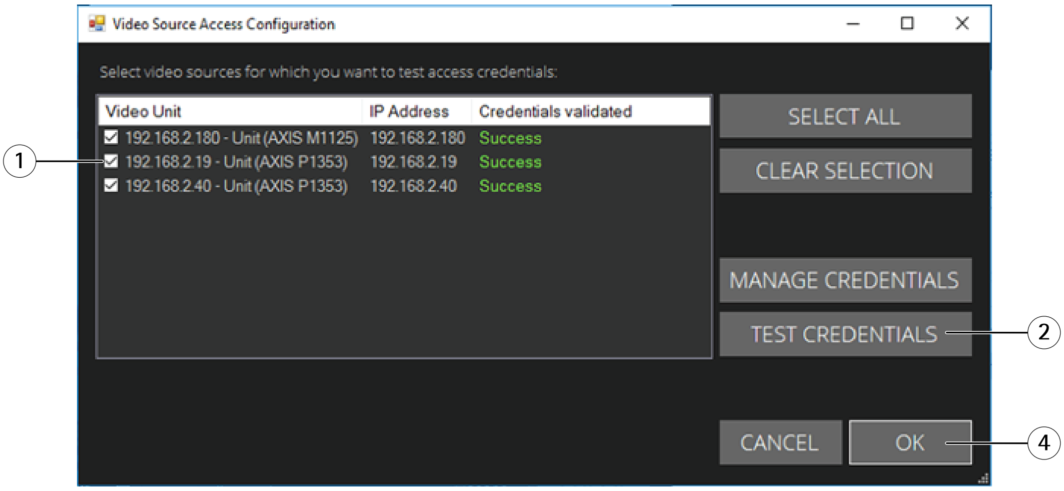
8. To add the entered credentials pair, click **Add**.

9. To close the window, click **OK**.

How to test the credentials

10. To test the credentials, select the devices you want to test and click **Test credentials**.

11. Wait for the test to finish, and make sure all devices has **Success** in the **Credentials validated** column.



Video Source Access Configuration

Select video sources for which you want to test access credentials:

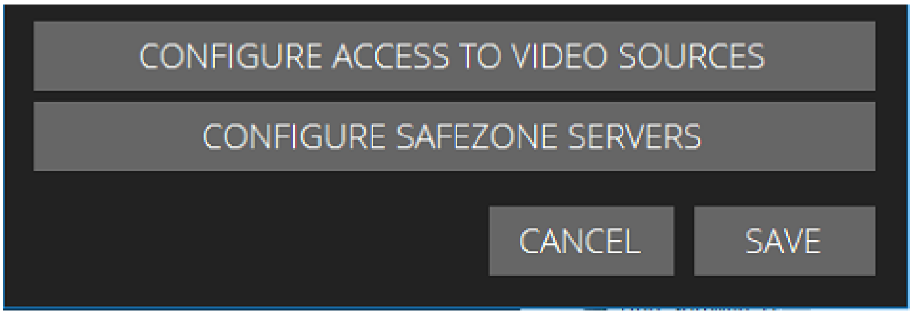
Video Unit	IP Address	Credentials validated
☑ 192.168.2.180 - Unit (AXIS M1125)	192.168.2.180	Success
☑ 192.168.2.19 - Unit (AXIS P1353)	192.168.2.19	Success
☑ 192.168.2.40 - Unit (AXIS P1353)	192.168.2.40	Success

Important

Only the cameras that passed the test are used by the Alarm & Metadata Bridge to send alarms & metadata to GSC. If a selected camera did not pass the test, make sure the credentials are correct and add the missing ones before closing the tool.

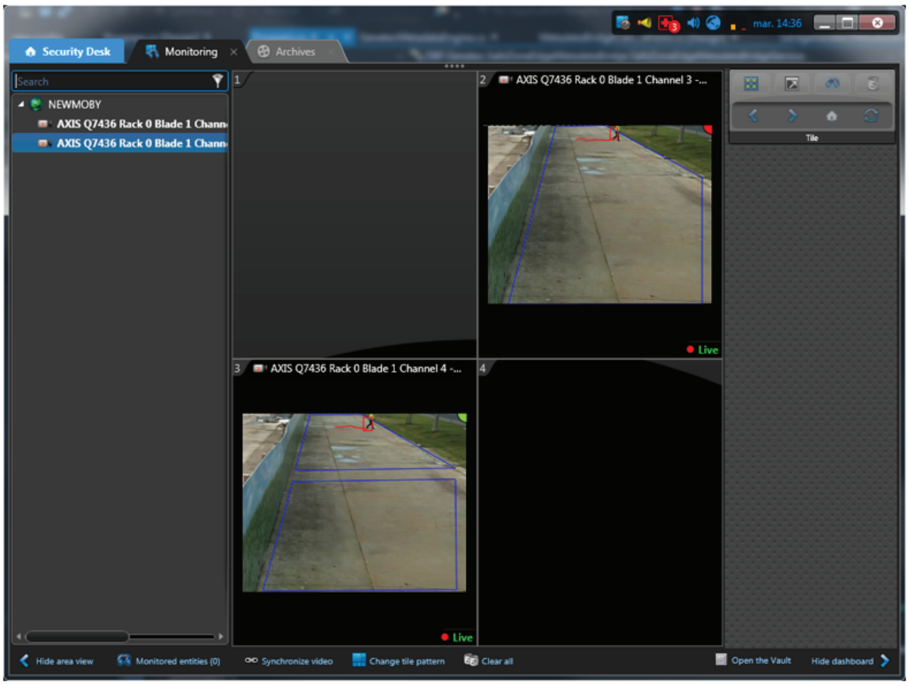
12. To close the window, by click **OK**.

13. To record the provided credentials into the encrypted container, click **Save**.

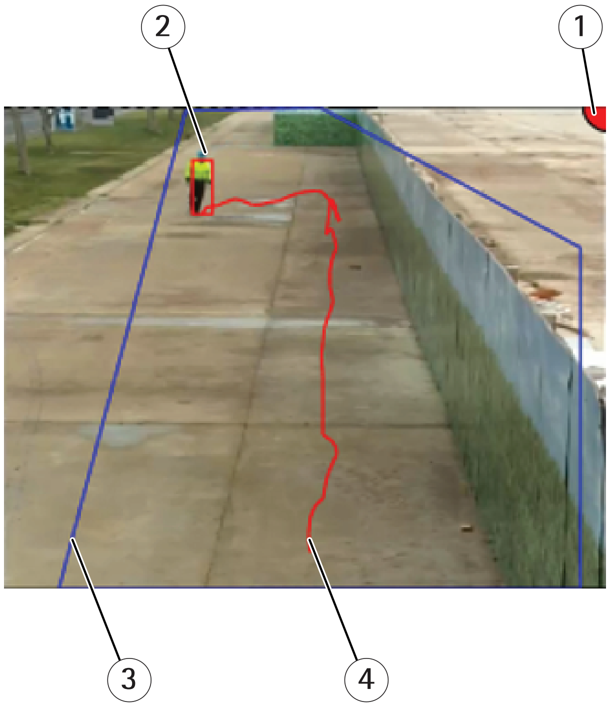


Security Desk

About metadata in Security Desk



This is how the metadata is displayed in Security Desk.



In this screenshot, the intrusion zone is displayed.

1 Alarm status
2 Detected object
3 Detection zone
4 Object trajectory

Different colors indicate the alarm status:

Red – If AXIS Perimeter Defender is running and an alarm is triggering for the camera, for example an intrusion alarm.

Green – If AXIS Perimeter Defender is running and no alarm is triggered.

Gray – During a short period (30–60 seconds) during startup of AXIS Perimeter Defender. During this phase AXIS Perimeter Defender is initializing and cannot generate alarms.

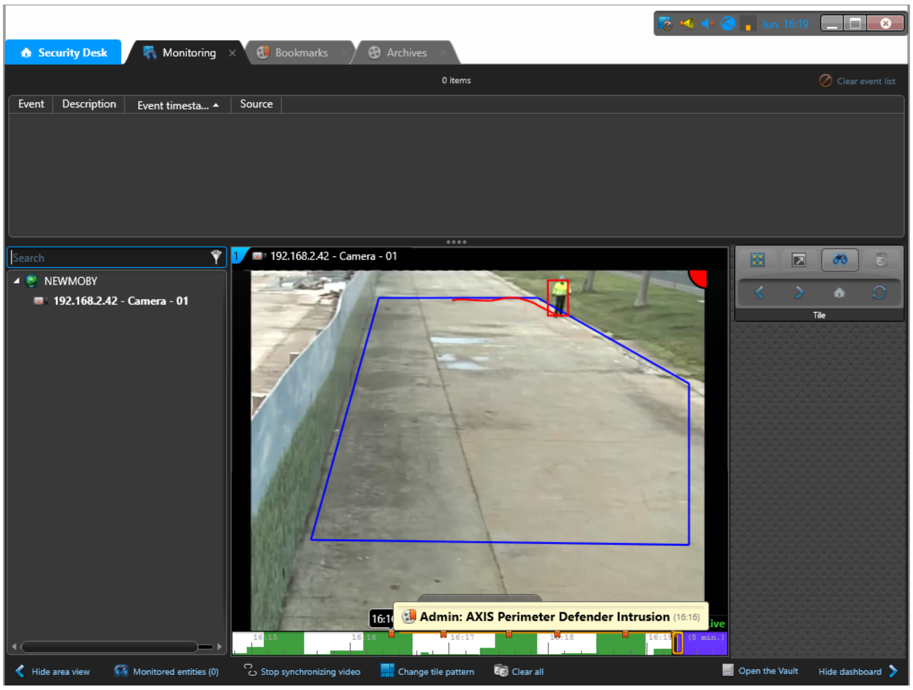
- A detected object (a person or a vehicle) is surrounded by a bounding box. The color of the bounding box is red for people and blue for vehicles.
- The detection zones defined on the camera are displayed in blue.
- The approximate trajectory is displayed in red, for people, or blue, for vehicles.

The same overlays are displayed when you playback the corresponding recorded video.

About bookmarks in Security Desk

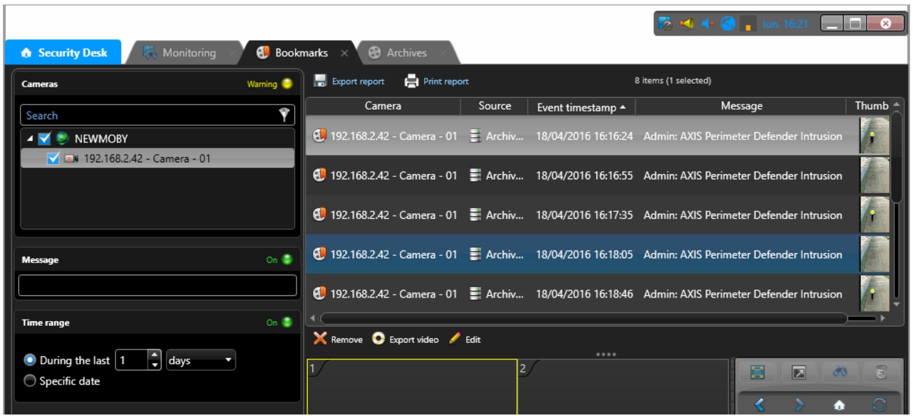
Security Desk displays bookmarks in the bottom time-line of each tile.

Security Desk



Each of the orange labels pointed by the arrow is a bookmark.

To find the corresponding video sequences, use the **Bookmarks** task.



8 items (1 selected)

Camera	Source	Event timestamp	Message	Thumb
192.168.2.42 - Camera - 01	Archiv...	18/04/2016 16:16:24	Admin: AXIS Perimeter Defender Intrusion	
192.168.2.42 - Camera - 01	Archiv...	18/04/2016 16:16:55	Admin: AXIS Perimeter Defender Intrusion	
192.168.2.42 - Camera - 01	Archiv...	18/04/2016 16:17:35	Admin: AXIS Perimeter Defender Intrusion	
192.168.2.42 - Camera - 01	Archiv...	18/04/2016 16:18:05	Admin: AXIS Perimeter Defender Intrusion	
192.168.2.42 - Camera - 01	Archiv...	18/04/2016 16:18:46	Admin: AXIS Perimeter Defender Intrusion	

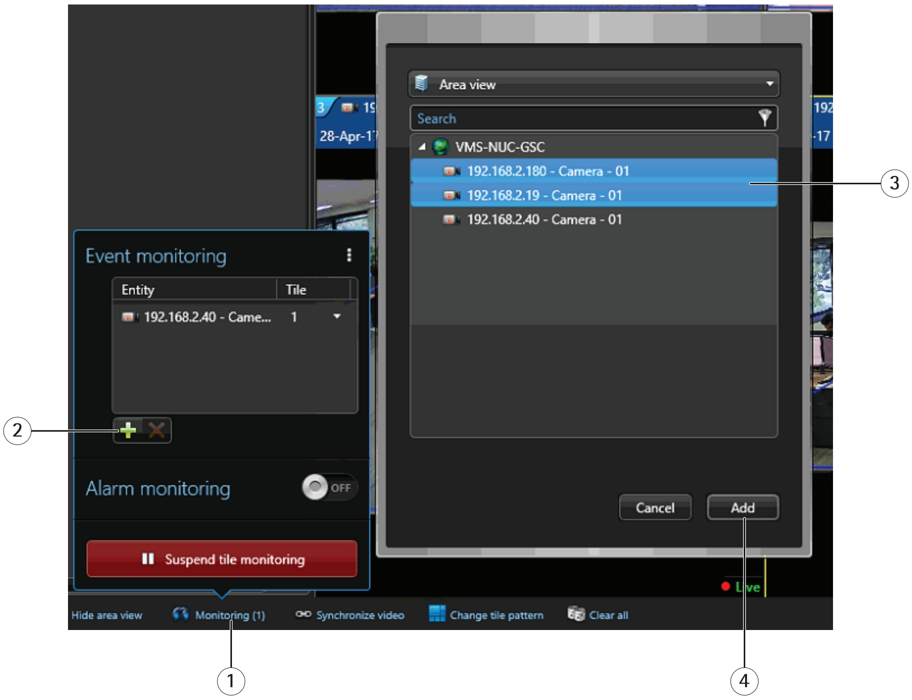
About custom events in Security Desk

Custom events in Security Center can be used to trigger a wide set of possible actions.

How to monitor custom events

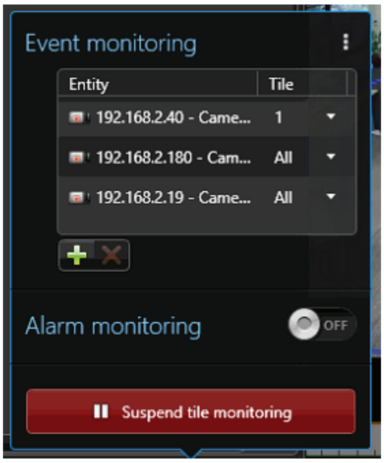
If you want to monitor custom events in Security Center, you need to configure the corresponding cameras as "monitored entities". Do the following

Security Desk



1 Monitoring tab
2 Plus icon
3 List of cameras
4 Add button

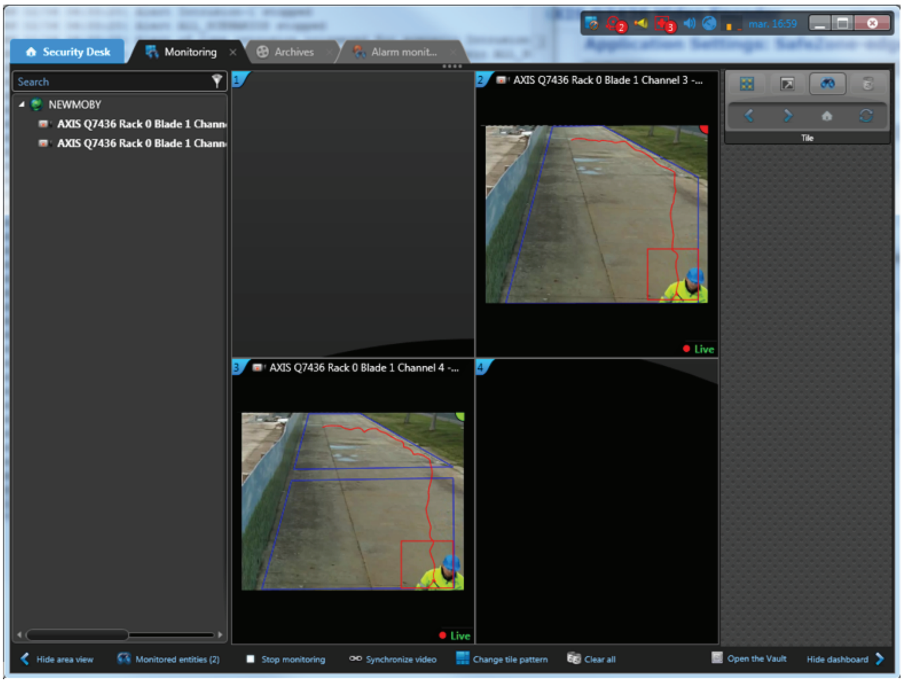
1. In the Security Desk, click the **Monitoring** tab.
2. Click **Monitored Entities** .
3. Click the plus icon.
4. In the list of cameras, select the camera you want to receive custom events from.
5. To add the cameras to the list of monitored entities, click **Add**.



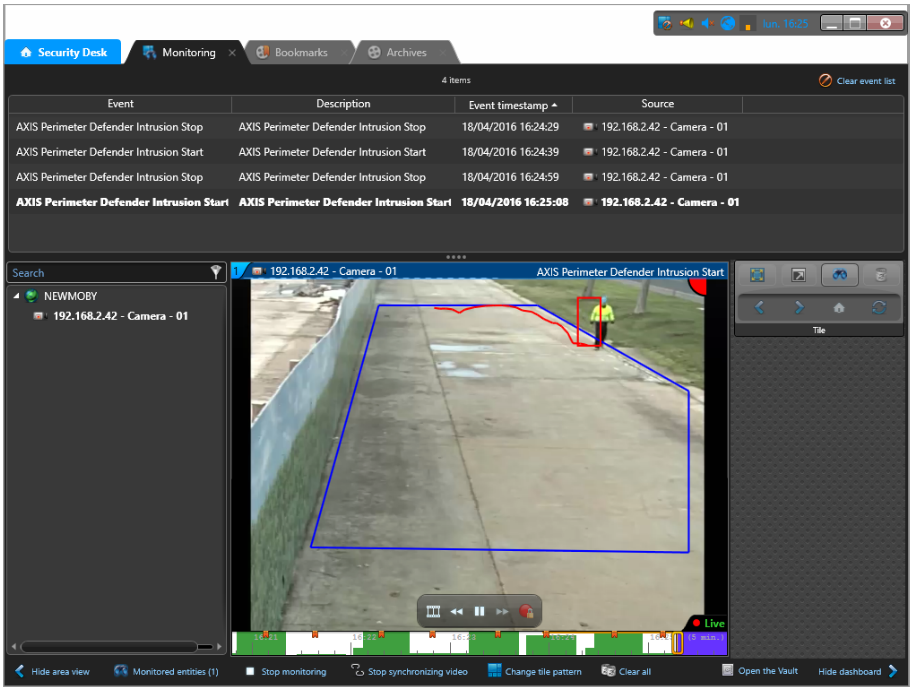
Entity	Tile
192.168.2.40 - Came...	1
192.168.2.180 - Cam...	All
192.168.2.19 - Came...	All

6. Now drag down the upper panel handle to display the custom events list in the **Monitoring** task of Security Desk.

Security Desk

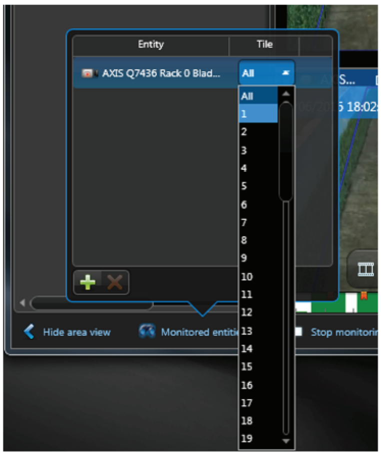


The custom events for the monitored cameras show up in the upper panel.



Event	Description	Event timestamp ▲	Source
AXIS Perimeter Defender Intrusion Stop	AXIS Perimeter Defender Intrusion Stop	18/04/2016 16:24:29	192.168.2.42 - Camera - 01
AXIS Perimeter Defender Intrusion Start	AXIS Perimeter Defender Intrusion Start	18/04/2016 16:24:39	192.168.2.42 - Camera - 01
AXIS Perimeter Defender Intrusion Stop	AXIS Perimeter Defender Intrusion Stop	18/04/2016 16:24:59	192.168.2.42 - Camera - 01
AXIS Perimeter Defender Intrusion Start	**AXIS Perimeter Defender Intrusion Start**	**18/04/2016 16:25:08**	**192.168.2.42 - Camera - 01**

If a camera is monitored, as soon as a Custom Event attached to that camera is received, Security Desk automatically shows the camera in the first free tile of the Monitoring Task. You can configure the monitored entity to always be displayed in the same tile.


Entity
Tile
AXIS Q7436 Rack 0 Blad...
All
All
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
Hide area view
Monitored entiti
Stop monitorin

User Manual
AXIS Perimeter Defender with Genetec VMS

Ver. M6.2
Date: March 2020
Part No. T10072021