

## **AXIS Perimeter Defender with Genetec VMS**

### **User Manual**

# AXIS Perimeter Defender with Genetec VMS

## Table of Contents

---

Introduction .....	3
VMS Integration .....	4
Installation Host .....	4
Prerequisites .....	4
Licensing .....	5
Installation .....	5
Configuration .....	5
Operating the Security Desk .....	10

# AXIS Perimeter Defender with Genetec VMS

## Introduction

---

### Introduction

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

# AXIS Perimeter Defender with Genetec VMS

## VMS Integration

---

### VMS Integration

#### Installation Host

The integration between AXIS Perimeter Defender and Security Center is based on two software modules running on the Security Center server (or another server connected by LAN to both the Axis cameras running AXIS Perimeter Defender and the Genetec Security Center server):

- The "AXIS Perimeter Defender" runs as a Windows Service. It feeds the Security Center Server with the metadata coming from AXIS Perimeter Defender. The Security Center Server records them on disk and makes them available to the Security Desk for live and playback display.
- The "Metadata Bridge Configuration Tool" is a graphical tool that allows the user to configure the Metadata Bridge and to provide the credentials and network addresses of the AXIS Perimeter Defender server, if there are any.

#### Prerequisites

##### Global prerequisites

In order to operate a successful integration between AXIS Perimeter Defender and Genetec Security Center, the following solution modules must be available:

- A working, correctly licensed and configured Security Center Server (at least 5.3 SR4 CU1 or 5.4 SR3)
- Some Axis cameras running AXIS Perimeter Defender. The Axis cameras must be connected to and configured within Security Center.

##### Note

AXIS Perimeter Defender does not need to be fully configured (i.e. calibrated and event defined) to configure the AXIS Perimeter Defender Genetec Security Center Integration Pack. Nevertheless, as long as a not-yet-configured it does not send alarms nor metadata, you will not be able to receive them in the Security Center.

- At least one "GSC-1SDK-Axis-PerimeterDefend" SDK connection license must be available within the Security Center (see dedicated section "Licensing" for more details)
- 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 dedicated section "Installation host" for further details)

##### Software Prerequisites

The integration pack has the following prerequisites:

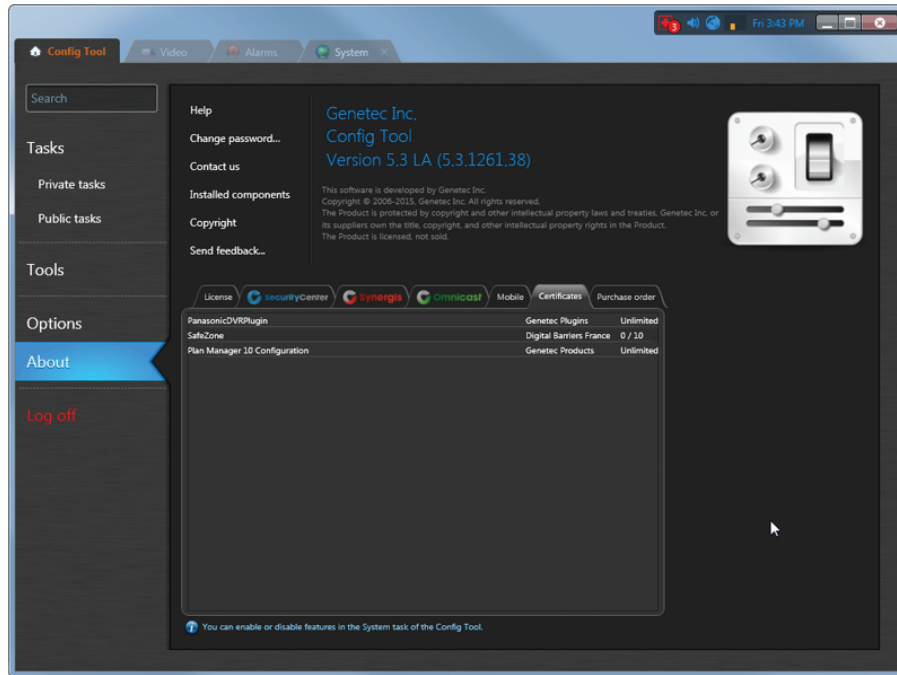
- Microsoft .net 4.0 must be available on the PC where the integration pack is installed. If it is not available, it will be automatically installed by the Integration pack installer.
- At least Genetec Security Center 5.3 SR4 CU1 or 5.4 SR3
- AXIS Perimeter Defender 1.0.0 or a later version
- The Genetec 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 (see following section for details).

# AXIS Perimeter Defender with Genetec VMS

## VMS Integration

### Licensing

Every running instance of the AXIS Perimeter Defender Metadata Bridge needs an "SDK connection license" from Security Center in order to be able to connect to it. The SDK license is named "GSC-1SDK-Axis-PerimeterDefend" and is displayed in the Certificates tab of the About menu of the Config Tool. The following picture displays a system with 10 of these licenses installed:



These licenses can be purchased from Genetec, contact your Genetec sales representative in case of doubt, mentioning that you want to purchase SDK licenses named "GSC-1SDK-Axis-PerimeterDefend".

The number of needed licenses depends on the number of installed Metadata Bridges and not on the number of servers or AXIS camera running AXIS Perimeter Defender. The Metadata Bridge Configuration Tool also needs an additional license during the configuration phase, see *Login Credentials on page 6* for further details.

### Installation

The installer executable ("AXIS Perimeter Defender Security Center Integration Pack X.Y.Z.W.exe") installs both the 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, the user must double-click on it and go through the few installation screens. The default values of each field suit the majority of the standard installations.

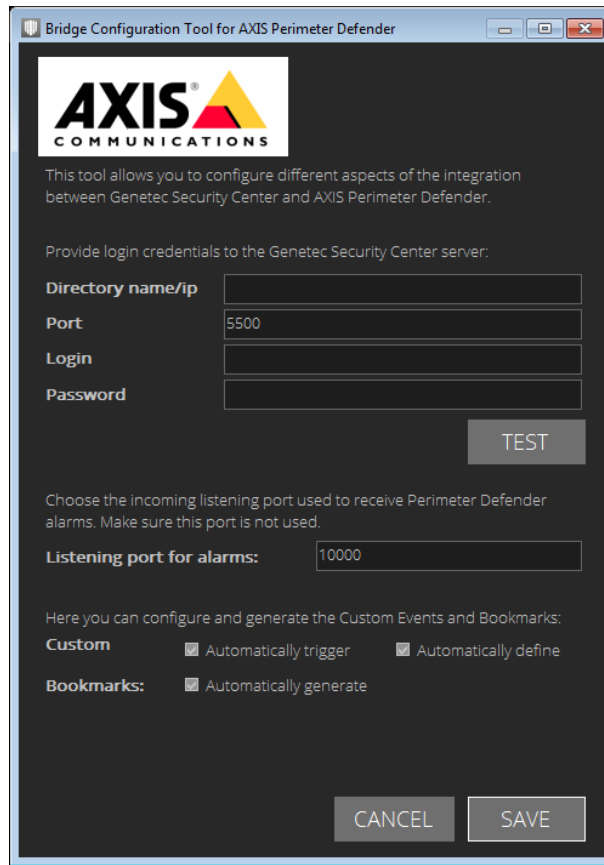
### Configuration

When the installation finishes, the Metadata Bridge Configuration Tool starts and presents the interface for the necessary configuration step. The following screenshot shows the tool interface:

# AXIS Perimeter Defender with Genetec VMS

## VMS Integration

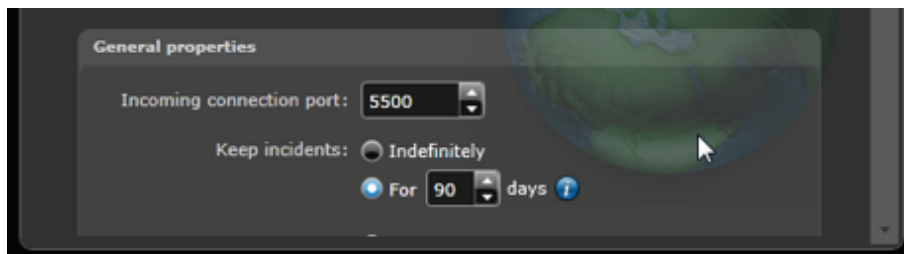
---



### Login Credentials

The user must provide login credentials to the Security Center Server:

- **Directory name/ip** is the ip address (like 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, "127.0.0.1" can be used.
- **Port** is the number of the port where Security Center listens for incoming SDK connection. Where in doubt, leave the default value of 5500. The correct value can be found in the "Genetec Server Admin" application (installed on the Security Center Server) and then looking at the "Incoming Connection Port" line.



- **Login** is the login of a user having administrative rights on the system. If Security Center is configured to accept Windows Domain logins, and you want to use those, prepend the login name with the domain name, like "DOMAIN\User".
- **Password** is the password corresponding to the user you specified.

# AXIS Perimeter Defender with Genetec VMS

## VMS Integration

---

We strongly 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" GSC-1SDK-Axis-PerimeterDefend , and thus the Metadata Bridge Configuration Tool can't connect to the Security Center Server.
- The Security Center server is not running (stopped) or the network connection (if the AXIS Perimeter Defender Bridge is installed on another machine) is broken.
- All the available SDK connection licenses of type GSC-1SDK-Axis-PerimeterDefend are in use (for example, the Metadata Bridge is using the unique available license). See the next section "Special Notes".

### 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 configures the different AXIS Perimeter Defender instances running on Axis cameras connected to the Security Center system so they will 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, the AXIS Perimeter Defender Metadata Bridge service needs to be restarted in order to use the new value.

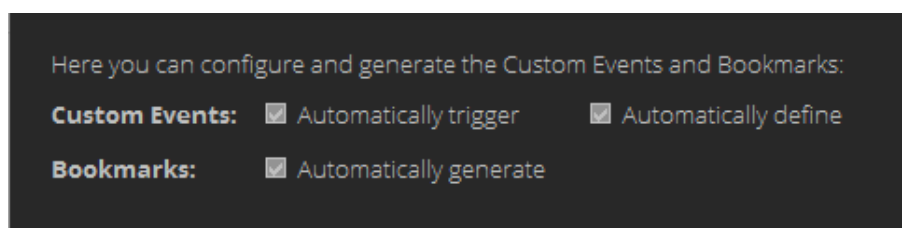
At the Integration Pack installation, a rule allowing incoming connections to any listening port of the Metadata Bridge is automatically added to the Windows Firewall. Nevertheless, the rule can be removed by a successive installation or blocked by some antivirus. It is recommended to double-check the connectivity from the external world to the chosen listening IP port each time this last is changed.

### Note

This parameter does not need to be configured or modified in the **Outputs** section of AXIS Perimeter Defender Setup Interface, as the Metadata Bridge does it automatically.

### 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:



In order for the Security Center to be able to receive a Custom Event, these two conditions needs to be fulfilled at the same time:

- To be defined
- To be triggered

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

- If the **Custom Events – Automatically Trigger** checkbox is ticked, and if a Genetec Custom Event corresponding to the received AXIS Perimeter Defender alarm exists, this one is triggered and sent to Security Center. Untick this box if you are not interested in receiving a Custom Event when AXIS Perimeter Defender triggers an alarm (for example, because Security

# AXIS Perimeter Defender with Genetec VMS

## VMS Integration

Center already receives the AXIS Perimeter Defender alarms by another mean). If you want to receive Custom Events on AXIS Perimeter Defender alarms, leave this box ticked.

- If the **Automatically define** checkbox of the **Custom Events** section is ticked, all the necessary Custom Events are automatically generated by the tool so they can be triggered when the corresponding AXIS Perimeter Defender alarm is received. So untick this box if you plan to manually define (a subset of) the necessary Custom Events, and leave this box ticked if you want them to be automatically defined.

The complete list of the Custom Events that will be created is:

- 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

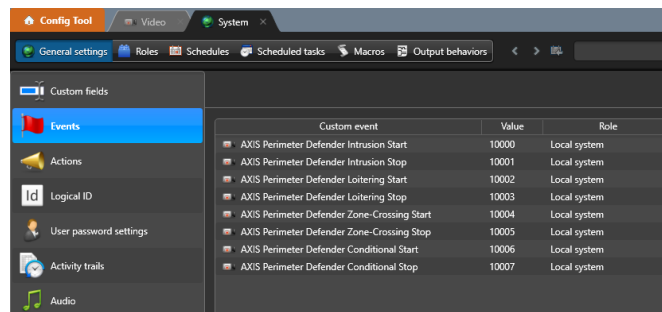
If you choose to define the Custom Events manually, it is important that the name of the Custom Event respects the following rules:

- It must contain the "Axis" string.
- It must contain one of the following strings: "Intrusion", "Loitering", "Zone-crossing", "Conditional".
- It must contain one of the following strings: "Start", "Stop".

(For these three rules, the comparison is done in a case-insensitive manner. Moreover, 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:

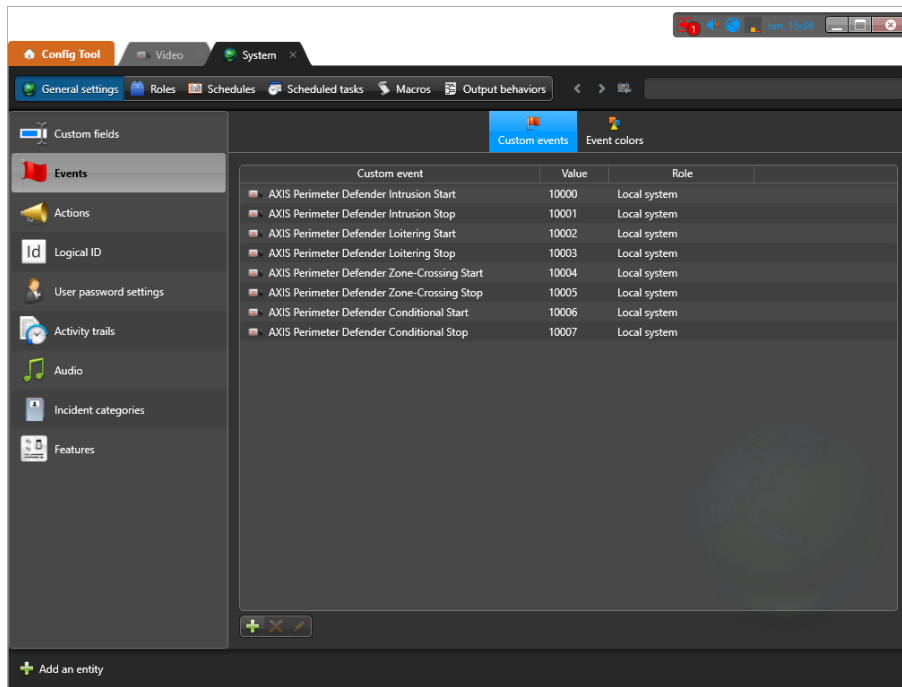
- Tick the **Automatically define** checkbox.
- Open the Genetec Config Tool and go to **System** task, then **General Settings** and **Events**.



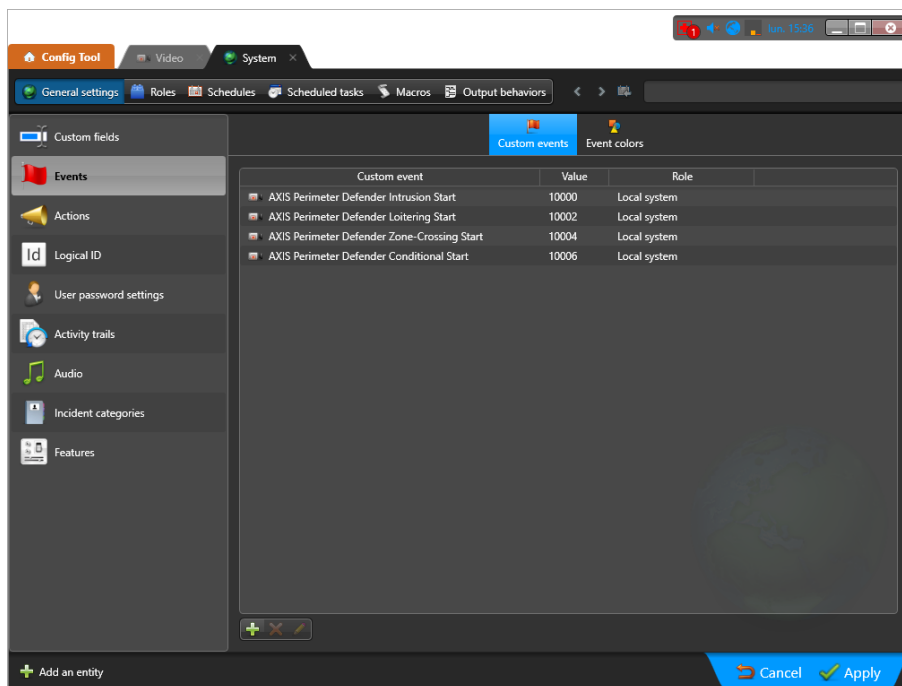


# AXIS Perimeter Defender with Genetec VMS

## VMS Integration



- Make sure you have the 8 Custom Events defined here.
- Untick the Custom Events Define missing ones in the Metadata Bridge Configuration Tool.
- Delete from the Genetec Config Tool the Custom Events you don't want, i.e. the four "Stop" Custom Events in this example.
- Make sure to save by clicking on **Apply** in the right lower corner of the window:



# AXIS Perimeter Defender with Genetec VMS

## VMS Integration

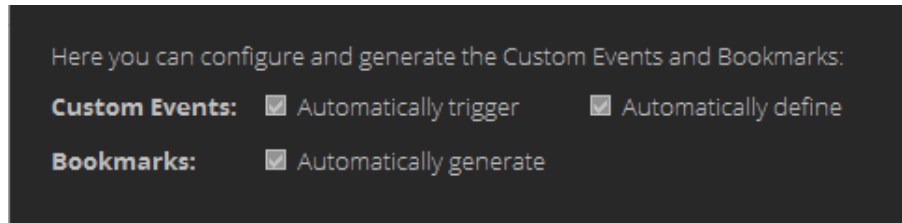
---

### Note

Once the Custom Events configuration finished, a restart of the Security Center service is necessary.

### 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, tick the **Bookmarks Automatically generate** checkbox in the Metadata Bridge Configuration Tool:



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).

### Metadata

The Metadata Bridge is able to 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/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 Axis camera running AXIS Perimeter Defender. If these cameras are connected to Security Center, it 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 do not require any special configuration, the Metadata Bridge automatically manages the necessary configuration automatically.

### Special Notes

When clicking Test , 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. So if both of them are running and there is only one SDK connection license "GSC-1SDK-Axis-PerimeterDefend " 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 your test and then start it again.

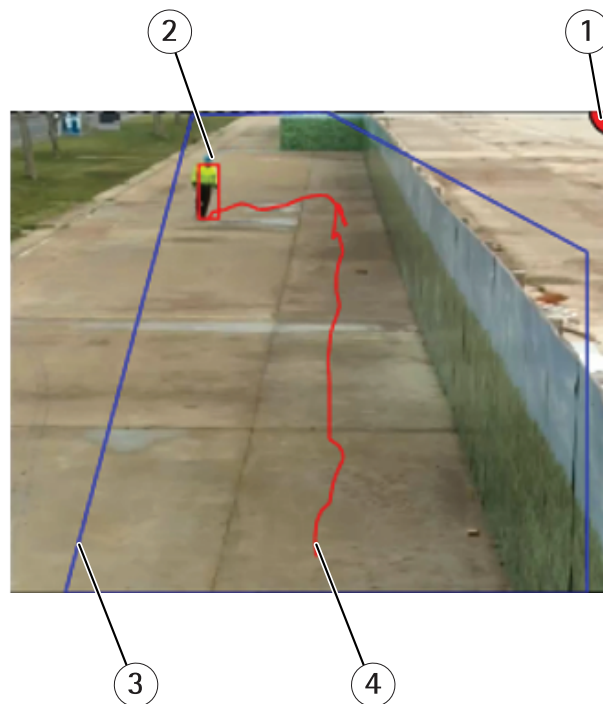
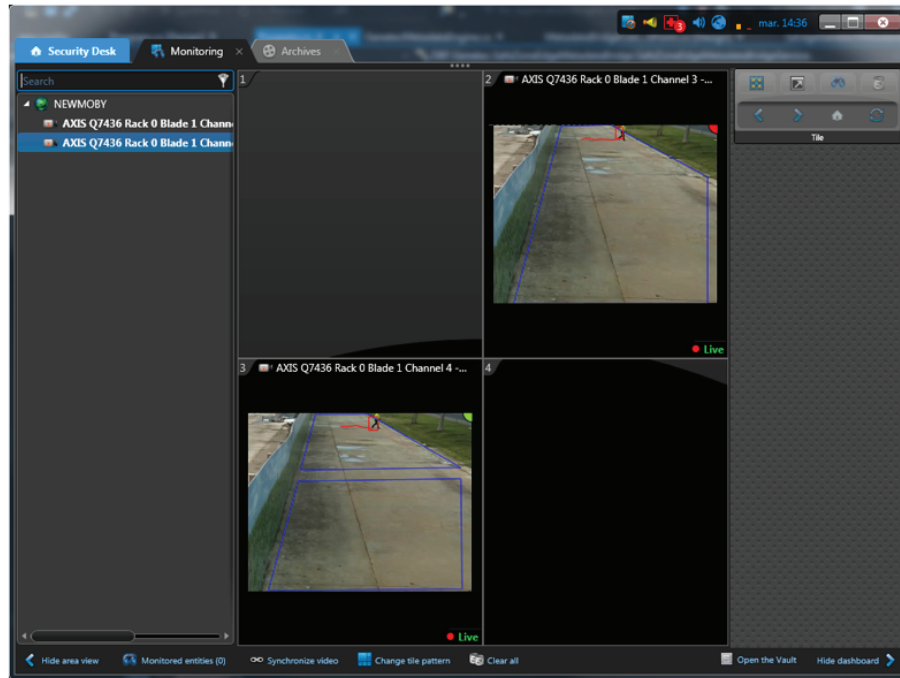
## Operating the Security Desk

### Metadata

Security Desk displays the metadata as in the following screenshot:

# AXIS Perimeter Defender with Genetec VMS

## VMS Integration



1. The upper right corner of the image contains a colored spot, the color displays the alarm status:
  - Red, if AXIS Perimeter Defender is running and an alarm is triggering for the camera (in the screenshot example, an intrusion alarm is generated by AXIS Perimeter Defender).
  - Green, if AXIS Perimeter Defender is running and no alarm is triggered for the camera (for example, for an intrusion scenario, if the person is walking outside the intrusion zone).

# AXIS Perimeter Defender with Genetec VMS

## VMS Integration

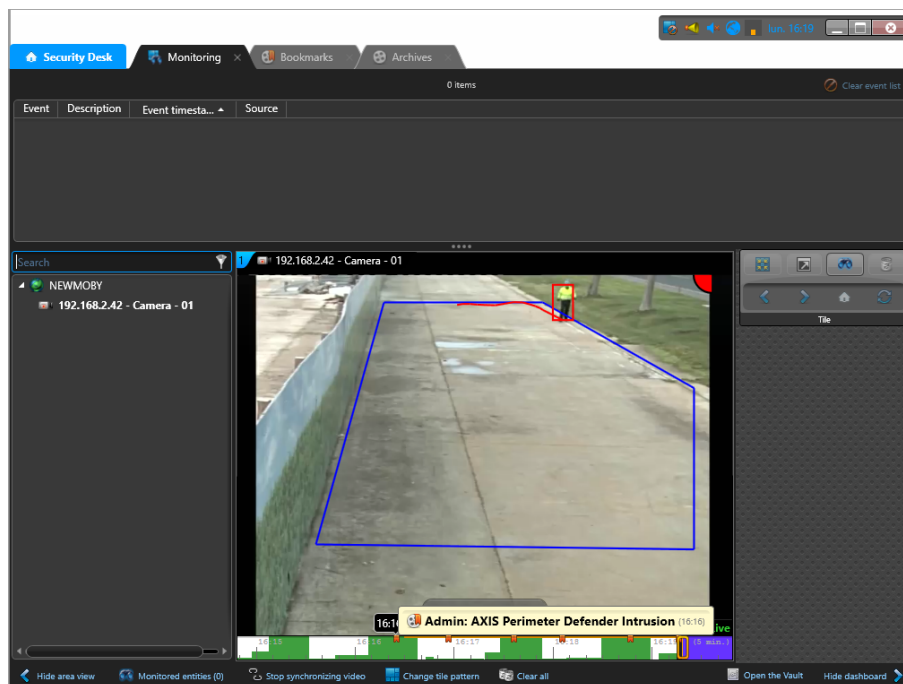
---

- Gray during a short period (30–60 seconds) after AXIS Perimeter Defender has been started. During this phase AXIS Perimeter Defender is initializing and cannot generate alarms.
2. A rectangle surrounds the persons and/or vehicles detected in the scene. The color of the bounding box is red for persons and blue for vehicles.
  3. The zones on ground relatives to the scenario(s) defined on the camera are displayed in blue. In this screenshot the intrusion zone is displayed. In the previous screenshot (the one inside Security Desk) one camera displays an intrusion zone and the other the two zones of a Zone-crossing scenario.
  4. The approximate actor trajectory is displayed in red (for a person) or blue (for a vehicle).

The same overlay is also automatically displayed when the corresponding recorded video sequence is played back.

### Bookmarks

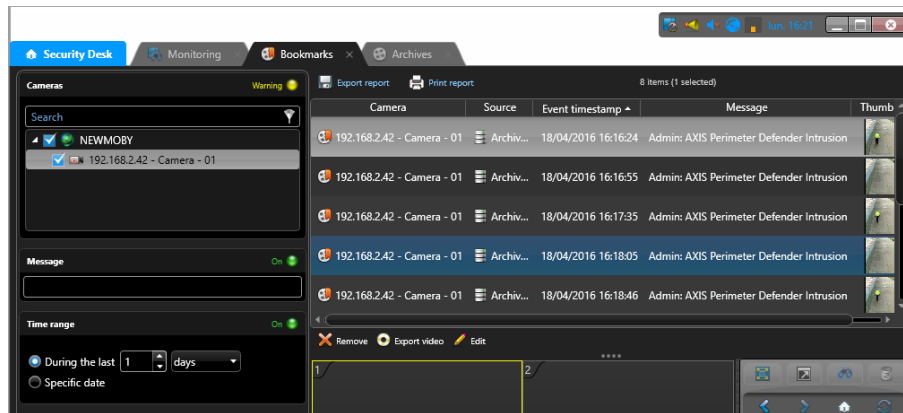
Security Desk displays bookmarks in the bottom time-line of each tile (see the orange labels pointed by the arrow in the following image: each one of them is a bookmark):



Bookmarks can be used to find the corresponding video sequences by using the "Bookmarks" Task:

# AXIS Perimeter Defender with Genetec VMS

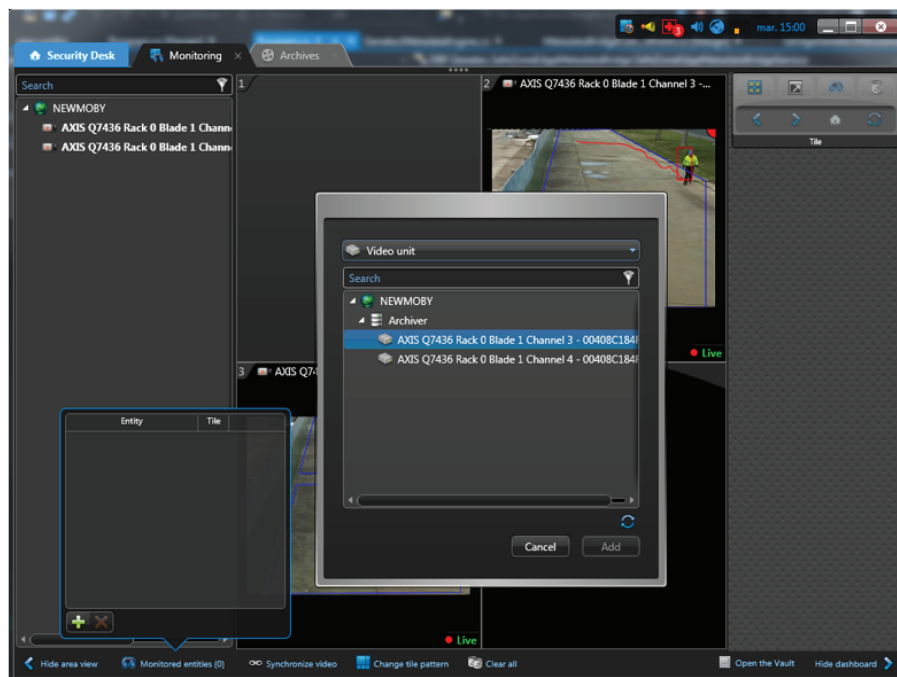
## VMS Integration



### Custom Events

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

If you want to monitor Custom Events in Security Center, you need to configure the corresponding cameras as "monitored entities" in Security Center. Proceed this way:



1. In the Security Desk, click on the **Monitoring** tab.
2. Click **Monitored Entities** on the lower menu bar.
3. Select the camera you want to receive Custom Events from.
4. Click **Add**.
5. The cameras are added to the Monitored Entities:

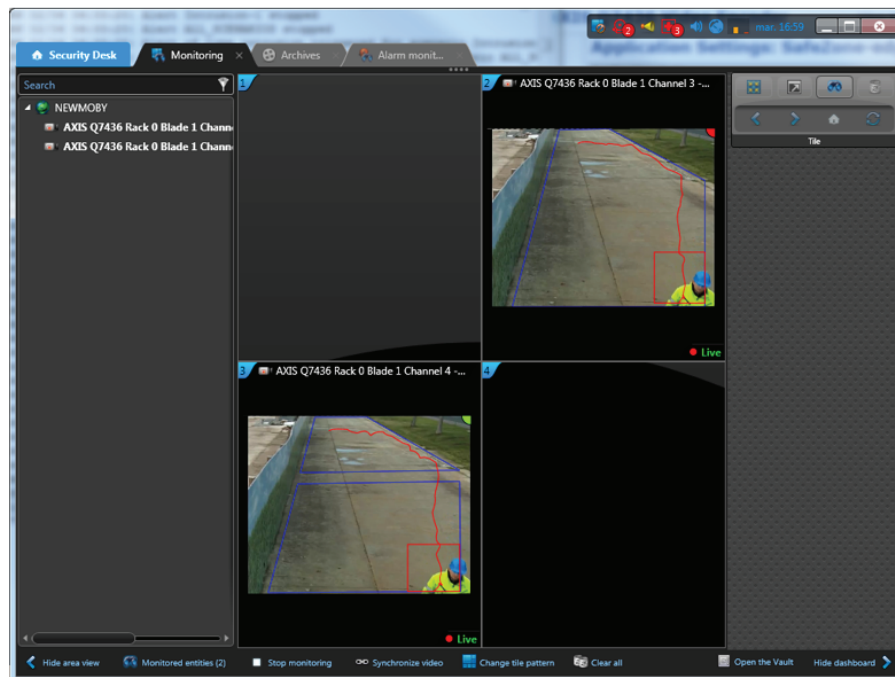
# AXIS Perimeter Defender with Genetec VMS

## VMS Integration

---



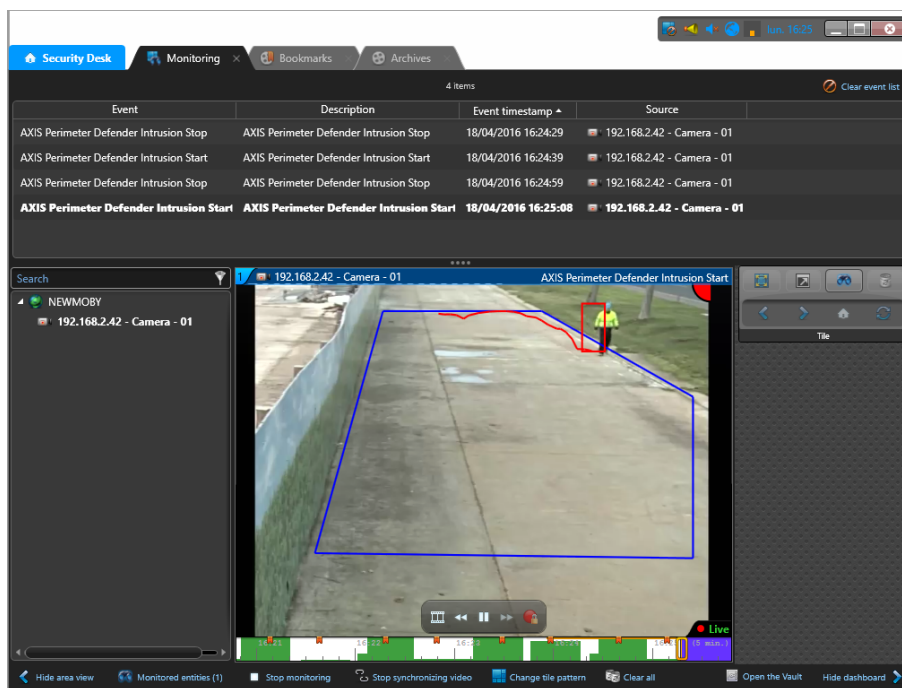
6. Now drag down the upper panel handle to display the Custom Events list in the Monitoring task of Security Desk.



7. The Custom Events for the monitored cameras will appear in the upper panel:

# AXIS Perimeter Defender with Genetec VMS

## VMS Integration



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

