

**User Manual** 

## Table of Contents

Introduction 3 About this document 4
AXIS Perimeter Defender integration 5
Integration architecture 5
Prerequisites
Licensing 6
Installation and first configuration steps 7
Installation 7
Add Axis devices running AXIS Perimeter Defender to XProtect 10
XProtect Cornorate or Expert
Configuration 13
How to use the Smart Client
XProtect Enternise/Professional/Enters
Configuration 44
How to use the Smort Client
Advanced configuration
Notwork computation
How to add new video sources to the system
How to increase the number of channels of the MID Driver
How to increase the number of channels of the wirr Diver
How to change the IB address of the bridge computation
How to change the IP address of the Wing device
How to enable metadate averat when experting video fortages 62

### Introduction

### Introduction

AXIS Perimeter Defender integrates with XProtect Video Management Systems (VMS) from Milestone, providing operators with immediate and informative feedback on potential security incidents.

The integration between XProtect product family and AXIS Perimeter Defender depends on the XProtect Product that is used:

- With XProtect Corporate and Expert (starting from version 2014) it is possible to:
  - trigger "User Defined" events when AXIS Perimeter Defender generates an alarm
  - trigger "Video Analytics" events when AXIS Perimeter Defender generates an alarm
  - trigger "Alarms" when AXIS Perimeter Defender generates an alarm
  - insert a bookmark in the corresponding video sequence
  - show the live metadata generated by AXIS Perimeter Defender on top of the corresponding video stream in Milestone Smart Client
  - record the metadata generated by AXIS Perimeter Defender with the corresponding video stream, and to show them together when playing the video sequence in playback mode
- With XProtect Enterprise, Professional and Express it is possible to:
  - trigger "Manual Global Events" when AXIS Perimeter Defender generates an alarm
  - trigger "Video Analytics" events when AXIS Perimeter Defender generates an alarm
  - trigger "Alarms" when AXIS Perimeter Defender generates an alarm

This document describes how to configure both XProtect and AXIS Perimeter Defender to achieve these two types of integration, for each "family product". Note that even inside the same "family" (for example, Enterprise/Professional/Express) there are some differences in the configuration depending on the specific XProtect product that is used (Enterprise or Professional or Express).

### About this document

## About this document

The next sections are independent from the installed XProtect product and should be read by every user.

- The software architecture (i.e. which software modules should be installed and where)
- How to install the software
- What prerequisites should be respected and what Milestone licenses are needed
- How to connect your AXIS Perimeter Defender to your Milestone system

At the end of section *Installation and first configuration steps*, the system is ready to receive Alarms, Analytics Events and User Defined Events/Manual Global Events. If that is enough for your needs, you can stop reading there.

If you need metadata display and recording (available in Corporate/Expert only) or if you need to trigger further actions by tweaking the XProtect configuration, then you can go to the chapter that is relative to your specific product, either XProtect Corporate or Expert, page 13, or XProtect Enterprise, Professional or Express page 44.

XProtect Corporate or Expert and XProtect Enterprise/Professional/Express include:

- How to connect the metadata from AXIS Perimeter Defender to Milestone (valid for XProtect Corporate only).
- How to leverage the Milestone Alarms, User Defined Events (in Corporate) or Manual Global Events (in Enterprise/Professional/Express) and Analytics Events to trigger further actions in your Milestone system (like activating a recording, sending an e-mail or an SMS or trigger an hardware output).
- How to operate the smart client.

Advanced configuration on page 55 include:

- A complete system architecture schema with emphasis on network communications between the different modules. See *Network communications on page 55*.
- How to extend an already installed and configured system by adding additional cameras. See *How to add new video* sources to the system on page 56.
- How to increase the number of the metadata channels of the MIP Driver. See *How to increase the number of channels of the MIP Driver on page 57.*
- How to remove from the bridge configuration video sources that have been removed from the system. See *How to remove video sources from the bridge configuration on page 60.*
- How to change the bridge server IP address. See How to change the IP address of the bridge server on page 61.
- How to change the Axis video source IP address. See *How to change the IP address of an Axis device on page 62.*
- How to enable XProtect to export the recorded metadata when exporting the corresponding video footages. See *How to enable metadata export when exporting video footages on page 63.*

## **AXIS Perimeter Defender integration**

## **AXIS** Perimeter Defender integration

#### Integration architecture

The integration between AXIS Perimeter Defender and XProtect is based on a set of software modules running on the XProtect servers.



The image shows a typical XProtect installation.

- 1 XProtect Corporate Management Client
- 2 Administrator
- *3 XProtect Corporate management server*
- 4 Operator
- 5 XProtect Smart Client
- 6 XProtect Corporate recording servers
- 7 MIP Plugins for AXIS Perimeter Defender
- 8 AXIS Perimeter Defender Metadata Bridge
- 9 MIP Plugins for AXIS Perimeter Defender
- 10 Axis cameras running AXIS Perimeter Defender

These are the additional software modules that make the integration between AXIS Perimeter Defender and XProtect:

- The MIP Plugin for AXIS Perimeter Defender is installed on every PC running either the XProtect Management Client or the XProtect Smart Client.
  - When run by the Management Client, it simplifies and automatizes the configuration of the system and allows to configure the automatic generation of Bookmarks and or User Defined events (that, in turn, can trigger a large set of tasks as answer to an alarm).
  - When run by the Smart Client, it displays the metadata generated by AXIS Perimeter Defender on top of the corresponding video streams, both in live mode and in playback mode.

### **AXIS Perimeter Defender integration**

• The AXIS Perimeter Defender Metadata Bridge runs as a Windows Service on one XProtect Recording Server (or Management Server) (optionally it can be installed and run on any other server connected by LAN to the Axis cameras). It feeds the XProtect Recording Server with the metadata coming from AXIS Perimeter Defender. The XProtect Recording Server records them on disk and makes them available to the Smart Client for live and playback display.

### Prerequisites

The integration pack has the following prerequisites:

- Microsoft .net 4.6 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
- Milestone XProtect Corporate and Expert from version 2014 (7.0d) including 2017 R1 (11.1a)
- Milestone XProtect Professional+, Express+ and Essential+ from version 2017 R1 (11.1a)

AXIS Perimeter Defender Bridge version 3.0.0 has dropped support for Milestone XProtect Enterprise, Professional and Essential. In that case, we recommend to use the version of AXIS Perimeter Defender 2.0.0.

#### Licensing

Note

This section only applies to XProtect Corporate/Expert. Enterprise does not need any additional Milestone licenses.

In order for the XProtect Corporate system to receive and record the metadata, an additional DLK is needed (independently from the number of metadata channels received by the system). This license is a standard DLK license to purchase from Milestone. For example:

- The system has 50 connected cameras and all of them have AXIS Perimeter Defender installed. The system must record and show the AXIS Perimeter Defender metadata. In this case, the total number of required DLK is 51.
- The system has 50 connected cameras and half of them have AXIS Perimeter Defender installed. The system must record and show the AXIS Perimeter Defender metadata. In this case, the total number of required DLK is 51.
- The system has 50 connected cameras and half of them have AXIS Perimeter Defender installed. The other half feeds a server that analyzes the 25 video streams. The system must record and show the AXIS Perimeter Defender metadata. In this case, the total number of required DLK is 51.
- The system has 50 connected cameras and half of them have AXIS Perimeter Defender installed. The system must receive the alarms triggered by AXIS Perimeter Defender and react on them, but metadata recording and display is not required. In this case, the total number of required DLK is 50.

### Installation and first configuration steps

## Installation and first configuration steps

This section is valid both for XProtect Corporate/Expert and XProtect Enterprise/Professional/Express.

- To install the necessary software, go to *Installation on page* 7.
- To connect AXIS Perimeter Defender devices to your XProtect System, go to Add Axis devices running AXIS Perimeter Defender to XProtect on page 10.

At the end of this section, your system is ready to receive Alarms, Analytics Events and User Defined Events/Manual Global Events.

#### Installation

The installer executable ("AXIS Perimeter Defender Milestone XProtect Integration Pack X.Y.Z.W.exe") installs both the AXIS Perimeter Defender Alarm & Metadata Bridge and the MIP Plugins for AXIS Perimeter Defender. At the installation, a dialog allows the user to choose the component(s) to install:

🚨 AXIS Perimeter Defender Bridge to Milestone XProtect Setup	×
Configure how AXIS Perimeter Defender Bridge to Milestone XProtect will be installed	
Features Installation Folder	
Select the features to be installed	
AXIS Perimeter Defender Bridge to Milestone XProtect	
Advanced Installer	Cancel

- 1. The user must run the installer and choose the AXIS Perimeter Defender MIP Plugins for Milestone XProtect component on every PC where the XProtect Smart Client is installed and where the user wants the metadata display (if metadata display is not a requirement, this installation can be omitted).
- 2. The user must also run the installer and choose the AXIS Perimeter Defender MIP Plugins for Milestone XProtect on every PC where the XProtect Management Client is installed and the user wants to administer (configure) the AXIS Perimeter Defender integration.
- 3. Finally, the user must run the installer and choose the AXIS Perimeter Defender Bridge to Milestone XProtect on either the XProtect Recording Server, or the XProtect Management Server or any other server directly connected by a good quality network (LAN) to the Axis cameras running AXIS Perimeter Defender.

### Installation and first configuration steps

#### Software installation on the host running the Management Client/Smart Client

#### Important

- Before installing the MIP Plugin for the XProtect Management Client, the Management Client must be already installed on the target host.
- In addition, before installing the MIP Plugin for the XProtect Smart Client, the Smart Client must be already installed on the target host.
- 1. As administrator, run "AXIS Perimeter Defender Milestone XProtect Integration Pack X.Y.Z.W.exe".
- 2. Click Next.
- 3. Accept the EULA and click Next.
- 4. If you plan to run the Metadata Bridge on another host, clear AXIS Perimeter Defender Bridge to Milestone XProtect. In any case, select AXIS Perimeter Defender MIP Plugins for Milestone XProtect. Click Next.

🚨 AXIS Perimeter Defender Bridge to Milestone XProtect Setup	×
Configure how AXIS Perimeter Defender Bridge to Milestone XProtect will be installed	
Features Installation Folder	
Select the features to be installed	
🕼 🛃 AXIS Perimeter Defender MIP Plugins for Milestone XProtect	
Advanced Installer	Cancel
	Cancel

- 5. Click Install.
- 6. Wait for the installation to be completed, then click Finish.

#### Software installation on the host running the XProtect Recording Server

#### Important

Before installing the AXIS Perimeter Defender Metadata Bridge, the XProtect System must be already installed and running on the same host or on a host connected to the Metadata Bridge one by a LAN.

- 1. As administrator, run "AXIS Perimeter Defender Milestone XProtect Integration Pack X.Y.Z.W.exe".
- 2. Click Next.
- 3. Accept the EULA and click Next.

### Installation and first configuration steps

4. If you have a Management Client installed on this host and you plan to configure the system with it, select AXIS Perimeter Defender MIP Plugins for Milestone XProtect. In any case, the AXIS Perimeter Defender Metadata Bridge should selected.



- 5. Click Install.
- 6. Wait for the installation to be completed, then click Finish.
- 7. In the AXIS Perimeter Defender Metadata Bridge Configuration, Hostname or ip address field must be filled with the DNS name or ip address of the XProtect Corporate server. 127.0.0.1 can be used if the Corporate server is installed on the same host.

Installation and first configuration steps

Bridge Configuration Tool	for AXIS Perime	ter Defender	- • •
This tool allows you to co that the AXIS Perimeter [ use and to provide login Provide the following Mi	onfigure the XP Defender Bridg credentials. lestone Server	Protect Recordir e to Milestone > information:	ng Server (Protect will
Hostname or ip			
Port	0		
Windows User	Milestone (	(Basic) User	
Login			
Password			
			TEST
		CANCEL	SAVE

- 8. **Port** is the port configured in the XProtect Server for SDK connections. If this value has not been customized in your installation, use the default value. Otherwise, use the custom port value you have set up.
- 9. Select if the login uses an existing Windows user or a Milestone user defined in the XProtect System 11.
- 10. In the Login field, enter the username. For a Windows user, it is necessary to prefix the login name with the user domain, as in "domain\username". For a Milestone user, only the username should be used.
- 11. Enter the password. If you are using a Windows user, do not forget to provide the user password in this field
- 12. Click Test to check the connection. If not, fix the problem by providing the correct information.
- 13. Click Save.

This allows AXIS Perimeter Defender Metadata Bridge to connect to the XProtect Server.

#### Add Axis devices running AXIS Perimeter Defender to XProtect

This section describes how to add the AXIS Perimeter Defender instances running on Axis ACAP devices connected to your XProtect system.

#### Note

This section includes screenshot examples from an XProtect Corporate/Expert installation, but the steps are the same for XProtect Enterprise/Professional/Express.

If you have Axis devices with AXIS Perimeter Defender, you need to add them to XProtect as video sources (this is a mandatory step) and then you need to add them to the MIP Plugin configuration so that they can be used as alarm and (under Corporate/Expert) as metadata sources also. Do the following:

- 1. Add all the Axis devices to XProtect as video sources (cf XProtect documentation)
- 2. Go to MIP Plug-ins >AXIS Communications > Perimeter Defender.

Installation and first configuration steps



- 3. Select the AXIS Perimeter Defender cameras tab.
- 4. Click Scan new cameras.
  - If you click No, the scan will be performed on all the enabled video sources connected to the XProtect System.
  - If you want to pre-filter the cameras to scan, select Yes.

Video source pre-filtering	
6 video sources are going to	
pre-filter them?	e scanned. This can take a while, Do you want to
pre-filter them?	e scanned. This can take a while. Do you want to

Select a sub-set of the available cameras. The advantage of reducing the set of cameras that are scanned to find AXIS Perimeter Defender instances is that this operation can take long time. By reducing the cameras set to those supposed to have AXIS Perimeter Defender installed, i.e. Axis cameras as other brands cannot run ACAP applications like AXIS Perimeter Defender. Select Activate brand pre-filtering.

## Installation and first configuration steps

deo source prefiltering			-	>
ct the video sources to scan for SafeZone-edge				
ME D-Link Corporation DCS-7513 (192 168.2.51) - Camera 1 AVIS G6034-E PTZ Dome Network Camera (192.168.2.24) - Camera 1 AVIS G7404 Video Encoder (192.168.2.121) - Camera 1 AVIS G9032-E PTZ Dome Network Camera (192.168.2.24) - Camera 1 AVIS P3225LVE Network Camera (192.168.2.49) - Camera 1 AVIS P1353 Network Camera (192.168.2.40) - Camera 1	IP ADDRESS 192.168.2.51 192.168.2.24 192.168.2.121 192.168.2.22 192.168.2.49 192.168.2.40	DRIVER ONVIF Asis IChPTZDevice Asis IChPTZDevice Asis IChPTZDevice Asis IChPevice Asis IChDevice		

#### Important

#### Valid for XProtect Corporate/Expert:

The Scan new cameras operations only adds new video sources running the AXIS Perimeter Defender application. It doesn't remove an already existing video source from the configuration, even if it has been disabled or removed from the system (and hence not found during the scan). To remove a video source from the configuration, see *How to remove video sources from the bridge configuration on page 60.* 

5. The MIP Plugins scans all the selected video devices of the XProtect system (skipping the disabled and not selected ones) and selects the Axis devices having AXIS Perimeter Defender installed. The list of the selected devices is shown in the central widget, alongside with the version of the installed package.

#### Important

When new cameras have just been added to the system, it is possible that they are not found by the MIP Plugin. In this case, just refresh the Management client configuration by using the F5 key and then click Refresh camera list again.

6. Save the configuration.

The selected cameras are now added to the system and are automatically used as alarm and metadata sources.

## **XProtect Corporate or Expert**

### Configuration

Through the MIP Plugins for AXIS Perimeter Defender running in the XProtect Management Client you can configure different aspects of the system:

- You can scan the list of cameras defined within XProtect and automatically select those where AXIS Perimeter Defender is installed. See Add Axis devices running AXIS Perimeter Defender to XProtect on page 10.
- The plugin automatically configures a Metadata Source providing a metadata channel for each Axis camera with AXIS Perimeter Defender. The Metadata Source is implemented and executed by the AXIS Perimeter Defender Metadata Bridge and must be added to the XProtect System. You can increase the number of video channels provided by the Metadata Source to plan future extensions of the system. The unused channels should be disabled once the metadata source has been added.
- The plugin allows the user to deactivate the automatic generation of XProtect Alarms when a AXIS Perimeter Defender triggers an alarm (the alarm generation is activated by default).
- The plugin allows the user to deactivate the automatic generation of a XProtect bookmarks when AXIS Perimeter Defender triggers an alarm. The bookmark generation is activated by default.
- The plugin allows the user to automatically generate two User Defined events (one corresponding to the start of the alarm, and one to the end) per alarm generated by AXIS Perimeter Defender. The user can then delete the unused or redundant User Defined events. The user can also manually define additional User Defined events.

#### Alarms, events and bookmarks configuration through the Management Client Plugin

#### Important

Before configuring the software, both the MIP Plugin for the Management Client and the AXIS Perimeter Defender Metadata Bridge must be installed. In addition, the Metadata Bridge must also be configured to be able to access the XProtect System.

- 1. Open the Management client.
- 2. Go to MIP Plugins >Axis Communication > Perimeter Defender .



- 1 Site navigation
- 2 Metadata configuration tab
- 3 Metadata parameters
- 4 Camera list
- 3. Select the Alarms & Metadata configuration tab.
- 4. If you want to show or record metadata, go to *Configure metadata through the Management Client Plugin on page 16.* Otherwise, you can skip the configuration of the Metadata source.
- 5. Configure alarms and bookmarks:
  - If you want to automatically trigger an XProtect alarm when AXIS Perimeter Defender generates one, select Automatically trigger alarms on AXIS Perimeter Defender alarm reception.
  - If you want to automatically trigger an XProtect Video Analytics Event when AXIS Perimeter Defender generates an alarm, select Automatically generate analytics events.
  - If you want to automatically insert in the corresponding XProtect video stream a bookmark, select Automatically generate bookmarks.
  - In most of the cases, you don't need to manually specify the destination IP address and listening port for alarms (i.e., the port that the AXIS Perimeter Defender Alarm & Metadata Bridge uses to listen for incoming alarms from AXIS Perimeter Defender and its IP address as used by the AXIS Perimeter Defender instances to send alarms). In some special cases, like when there is a NAT or port forwarding between the AXIS Perimeter Defender devices and the host where the Alarm & Metadata bridge runs, you might want to set them manually. In this case, select Set Manually and enter the IP address or DNS hostname and port that the AXIS Perimeter Defender devices should use to send the alarms.
- 6. If you want the AXIS Perimeter Defender alarms to trigger XProtect User Defined Events, you need to define these events. You can use the Generate user defined events button to automatically generate some of them. The button parses the scenarios defined in each AXIS Perimeter Defender device and generates a couple of User Defined Events (one for the start, the other for the stop of the scenario) that the AXIS Perimeter Defender Alarm & Metadata Bridge triggers when AXIS Perimeter Defender generates the corresponding alarm. For example, by clicking the button on a system with one AXIS Perimeter Defender camera (192.168.2.246) with 4 scenarios (named "conditional-1", "intrusion-1", "loitering-1" and "zone-crossing-1") and an AXIS Perimeter Defender stream with one scenario, "intrusion-1", the configuration plugin generates these XProtect User Defined Events:
- 7. Save the configuration

## **XProtect Corporate or Expert**



8. You can retrieve the User Defined Events by clicking Rules and Events > User-defined Events.

If you are not interested in all of them, for example, if you are not interested in the STOP User-defined events, simply remove them. The Metadata Bridge does not find them and hence does not generate them.

You can also modify them to make them more generic, for example to make a single User Defined Event to be triggered by several different alarms. To do that, you can edit the User Defined Event name and replace one or more of the fields **<ScenarioName>**, **<ScenarioType>** and **<CameraName>** with the keyword ALL.

Every User Defined Event that is supposed to be triggered on an AXIS Perimeter Defender alarm must have a name that respects a specific format: AXIS Perimeter\_Defender <ScenarioName> <ScenarioType> on camera <CameraName> where:

- <ScenarioName> is the name of the scenario as defined in the AXIS Perimeter Defender Setup. Usually it looks like "Intrusion-1", but can be customized when setting up AXIS Perimeter. If you want the User Defined Event to be triggered by any scenario, use "ALL" as <ScenarioName>.
- <ScenarioType> is either "START", "STOP" or "ALL". Use "ALL" if you want the User Defined Event to be triggered for both START and STOP alarms.
- <CameraName> is the name of the camera as defined in XProtect. When AXIS Perimeter Defender triggers an alarm, it does so by analyzing images from a device that must also be present in XProtect. For AXIS Perimeter Defender, this is the device where AXIS Perimeter Defender is installed. <CameraName> is the name of the associated XProtect Camera. Use "ALL" if the Manual Global Event must be triggered by AXIS Perimeter Defender alarms associated to any XProtect camera.

#### Important

If you want to use an XProtect Camera Name as **<CameraName>**, you must replace the spaces in the name by the "underscore" (\_) character. Alternatively, you can rename the XProtect Camera and remove all spaces from the camera name, or use ALL as **<CameraName>**.

#### NOTICE

The three parameters **<ScenarioName>**, **<ScenarioType>**, and **<CameraName>** are all case insensitive, so lowercase and uppercase letters are considered the same.

Here some examples of User Defined Events and by which AXIS Perimeter Defender alarms they will be triggered:

- AXIS PerimeterDefender Intrusion-1 START on camera ALL: will be triggered by any AXIS Perimeter Defender alarms START related to a scenario called "Intrusion-1" from any camera
- AXIS PerimeterDefender ALL ALL on camera IP250: will be triggered by any AXIS Perimeter Defender alarm START or STOP related to any scenario from the XProtect Camera "IP250"
- AXIS PerimeterDefender ALL START on camera ALL : will be triggered by any AXIS Perimeter Defender alarm START related to any scenario from any camera
- AXIS PerimeterDefender ZoneCrossing-1 STOP on camera IP250 : will be triggered by any AXIS Perimeter Defender alarms STOP related to the scenario "ZoneCrossing-1" from XProtect camera "IP250"

#### Important

If you rename a camera, remember to adapt the corresponding User Defined Events accordingly.

#### NOTICE

- At this stage of the configuration process, if you activated the alarm, events or bookmarks generation, you should be able to receive them in XProtect without further steps. If you are not interested in metadata display and recording, you can stop here and you will not need the DLK license that is necessary to add the metadata source to Milestone. If you want to have the live and/or recorded metadata too, continue the configuration as explained in the section *Configure metadata through the Management Client Plugin on page 16*
- When you change the User Defined Events names you must restart the AXIS Perimeter Defender Alarm & Metadata Bridge service for the change to take effect.

#### Configure metadata through the Management Client Plugin

#### Important

Before you can add the metadata source to the XProtect System, the AXIS Perimeter Defender metadata bridge must be fully installed and configured, i.e. by providing the XProtect login credentials and IP address.

Before displaying or recording the metadata in XProtect, you need to configure the Metadata Source that XProtect uses to pull the metadata streams from AXIS Perimeter Defender. Milestone consider the Metadata Source as a normal video source, and you have to add it as if it were a video source on its own.

- 1. Open the Management client.
- 2. Click MIP Plugins, Axis Communication, Perimeter Defender .
- 3. Click the Alarms & Metadata configuration tab.



- 1 Site navigation
- 2 Metadata configuration tab
- 3 Metadata parameters
- 4 Camera list
- 4. Configure the parameters of the metadata source:
  - Use the default MAC address. If you want to provide your own MAC, for example, because you plan to add more than one metadata source to the system, select **Set manually** and click **Get another one** button or type the MAC address in the address field.

#### Important

The Metadata source MAC address is tied to the DLK license of Milestone. If you change it after having added the metadata source to XProtect, you must re-associate the DLK to the new mac address.

- The metadata source listening port is where the metadata source listens for incoming connections from XProtect. The metadata source logically behaves like a physical device (like a multi-channel encoder) but distributes metadata streams instead of video streams. This listening port is the equivalent to the port 80 of an HTTP-based network device. Use the default value unless another application already uses this port on the host. To check if it's being used, click the **Check if free** button. Note that this button requires the AXIS Perimeter Defender Alarm & Metadata Bridge to be running.
- The number of provided metadata channels is automatically set to the number of AXIS Perimeter Defender found or configured in the system. If you want more metadata channels, for example because you know you will add more AXIS Perimeter Defender instances in the future, you can increase this number.

#### Important

If you already added the metadata source to the Milestone system, in order to increase or decrease the number of video channels it is necessary to remove it and add it again or to use the Replace hardware functionality (cf. XProtect User Guide)

The Management Client requests a metadata source password when adding the metadata source to the system. If you want to see the password, click and hold the Show in plaintext button.

#### Important

If you already added the metadata source to the Milestone system and you change the password, XProtect is not able to retrieve the metadata anymore. In this case, it is necessary to update the password value in the metadata source settings.

5. The Display metadata channel opens a dialog that shows what AXIS Perimeter Defender instance is feeding a given metadata channel with metadata. The same dialog allows you to "free" a metadata channel whose video source is not connected to the system anymore (see section How to remove video sources from the bridge configuration on page 60

When the metadata source is configured, you need to add it to the XProtect system so that XProtect can pull metadata out from AXIS Perimeter Defender:

- Tools Hel 10.13.24.216) 0 13 24 216) - Ci (10.13.24.216) + rd 🖈 Mor tion 🕓 Fisl nts 🖵 C
- 1. In the Management Client, go to Servers >Recording Servers.

2. Right-click the server and select Add hardware.



3. Select Manual and click Next.

## **XProtect Corporate or Expert**



- 4. Add a new username and password using "root" as login and the password you set for the Metadata source.
- 5. Click Next.

Add Ha	rdware			
Spe	cify user name and password if de	vices are not using the default ones.		0
Inclue V	de User Name (Factory Default) root	Password		Add Bemove
	Нер	< <u>B</u> ac	* <u>N</u> ext >	Cancel

6. Select Other > MIP Driver as device type and click Next.

## **XProtect Corporate or Expert**

Other       Select All         Acronag 16 DIO module       Acronag 16 DIO module         Approved Technology Video       AgileMesh         Apromedia H1000 Series       AgileMesh         Apromedia H1000 Series       AgileMesh         Aproved Technology Video       Select All         Clear All       Clear All         Clear Whita       Basler BIP/BIP2         CheckView 9128702       CiscoIPC Series         Cobham NetWode       Cobham NetWode         Cohu Helios 3960H0       Cochum NetWode         Cohu Helios 3960H0       Cochum NetWode         Convex CNB NPT2 Series       Dahua DH-SD6582-HN         Dahua DH-SD6582-HN       Dahua DH-SD6582-HN         Darim Vision PVEA00       DirectShowDriver         Emotion EXPT2 Series       Ernitec SX Faries         Ernitec SX Faries       Ernitec SX Series         Ernitec SX Series       Ernitec SX Series         Ernitic Vaga SX Series       Ernitic Vaga SX Series         Ernitic Vaga SX Series       Ernitec Vaga SX Series         Ernitic Vaga SX Series       Ernitec Vaga SX Series         Ernitic Vaga SX Series       Ernitec Strip Series         Grandeye Halocam       Gundig         Grandeye Halocam       Gundig         Gr	d Hardware Select which drivers to use when scanning for hardware. The more drivers selected, the slower the scanning.	-		
	Other         360 Vision VDIP         Acromag 16 DIO module         Advanced Technology Video         AgileMesh         Apromedia H1000 Series         AVS MPix13         Basler BIP/BIP2         CheckView 9123022         CiscolPC Series         Coham NetNode         COHU Helios 3960HD         Convex CNB No PTZ Series         Coham NetNode         COHU Helios 3960HD         Convex CNB No PTZ Series         Dahua DH-SD6582-HN         Darim Vision PVE400         DirectShowDriver         ElsagDatamat Visig2 Encoder         Erritice SN Series         Errovision PVE400         DirectShowDriver         ElsagDatamat Visig2 Encoder         Erritice SN Series         Errovision PVEXoux PTZ Series         ErrovisionEV%xxxx Transparent PTZ Series         ErrovisionEV%xxxx Transparent PTZ Series         ErrovisionEV%xxxx Transparent PTZ Series         Grandey Ellocam         Grundig No PTZ         Ikegami IPDIEN         Impath IST10 Video Encoder         IMT         IONodes E1610         IPIX IS/CV series         Janteq         Lumenera         Ø MID Priver         OTN H264AVC 160		E	Select All

- 7. Enter the IP address of the host where the AXIS Perimeter Defender Metadata Bridge is installed. Use the public external IP address of the host, even if it is installed locally, as 127.0.0.1 does not work. You can use "netstat –an" and look to which IP address is associated to the listening socket open on port TCP/50000 (or the port that has been chosen for the metadata source).
- 8. In the Hardware Driver drop-down list, select MIP Driver. Note that Auto-Detect does not work.
- 9. Click Next.

## **XProtect Corporate or Expert**

Add Hardware				
Enter information for har Optionally, select driver	dware you want to add. type to speed up detection.			10
Address	Port	Hardware Driver		Add
192.168.90.66	50000	MIP Driver		Remove
				]
Help		< <u>B</u> ack	Next >	Cancel
Щер		< Back	Next >	Cancel

In this screenshot the address to use is 192.168.90.66.

10. When XProtect has detected and accepted the metadata source, click Next.

dd Hardware Wait while your hard Once detection has o	ware is being detected. completed, select which hardware t	to add.			Stop
Add Address	P	ort	Hardware Driver	St	atus
<b>I</b> 92.168.90.66	50	0000	MIP Driver		Success
7 Show hardware running Help	; on other recording servers		< <u>B</u> ack	<u>N</u> ext > 7	Cancel

11. Select the metadata channels as the Axis cameras running AXIS Perimeter Defender that send metadata to the system. Usually this means all the metadata channels available on the source, except if you increased the number of channels manually to prepare future extensions. In this case, we recommend selecting only the effectively used channels.

#### 12. Click Next.

## **XProtect Corporate or Expert**

Add Hardware			_ O X
Hardware and cameras areenabled pe The hardware and its devices will be a	r default. Manually enal ssigned auto-generated	ble additional devices to be used. I names. Alternatively, enter names manually.	10
Hardware name template:		Device name template:	
Default		▼ Default	•
Hardware to Add	Enabled	Name	
MIP Driver - 192.168.90.66			
Hardware:		MIP Driver (192.168.90.66)	
Wetadata port 1:	<b>V</b>	MIP Driver (192.168.90.66) - Metadata 1	
💱 Metadata port 2:	<b>V</b>	MIP Driver (192.168.90.66) - Metadata 2	
Help		< Back Next >	Cancel

The screenshot shows how to enable channels provided by the metadata source.

13. Select a group, or create a new group, for the **Default metadata group**, then click Finish.

dd Hardware		
Alternatively, select device gr	succes types. oup individually for each device.	
Default camera group:	Select Group	
No group selected	Up Oup	
Default microphone group:	Perimeter Defender metadata	
No group selected	pup	
Default speaker group:		
No group selected		
Default metadata group:		
No group selected		
Default input group:		
No group selected		
Default output group:		
No group selected		
Help	< Back Finish	Cancel

- 14. Select the newly added Metadata source "MIP Driver (192.168.90.66)".
- 15. In the **Stream** window, make sure a set of "1/0" comes out from the central cubes. This means that XProtect is retrieving the metadata from the source.

	- 2016			
Milestone XProtect Management Clier	t 2016			
Site Navigation	Seconding Server		G Properties	9
DeurMcGry - (10.0s)     Barics     Fallors     Fallors     Fallors     Fallors     Fallors     Clent     Rules     Clent     Rules     Clent     Rules     Clent     Rules     Clent     Sourchise     Clent     Sourchise     Clent     Sourchise     Sourch     S	Image: Section Sectors         Image: Sectors Sectors <td< td=""><td>40) 1,2245) (62,48) 2) #8 <b>1</b> #8 <b>2</b></td><td>Device information     Name:     MP Driver (192:168:90:160) - Metadate 1     Description:     Hardware name:     MIP Driver (192:168:90:160)     Potrumber:     1     Info @Settings ● Record</td><td></td></td<>	40) 1,2245) (62,48) 2) #8 <b>1</b> #8 <b>2</b>	Device information     Name:     MP Driver (192:168:90:160) - Metadate 1     Description:     Hardware name:     MIP Driver (192:168:90:160)     Potrumber:     1     Info @Settings ● Record	
Site Navigation Federated Site Hierarchy		MIP Driver (192.168.90.160) - Me	etadata 1	

- 16. If you don't see any "1/0" near the central cube, there is a problem with the metadata retrieval, probably due to the lack of a default rule. Do the following:
  - In the Rules and Events section, make sure that you have a Default Start Metadata Feed Rule and that the rule looks like in the following image.



- If the rule is missing, you must define the rule:
- In the Rules and Events section, right-click Rules and select Add Rule.

**XProtect Corporate or Expert** 



- Type name for the rule, then select Perform an action in a time interval and click Next .

Manage Rule			X
Name:	Start Metadata Feed Rule		
Description:			
Active:			
	Step 1: Type of rule		
Perform an action	in a time interval		
Edit the rule descripti	on (click an underlined item)		_
Perform an action in a	time interval		
Help	<u>C</u> ancel < <u>B</u> ack <u>N</u> ext > (	<u>F</u> inish	

- Select Always and click Next.

# XProtect Corporate or Expert

Manage Rule				
Name:	Start Metadata Feed Rule			
Description:				
Active:				
	Step	2: Conditions		
Select conditions to a	apply			
Within selected ti	ime in <time profile=""></time>			
Utside selected	time in <time profile=""></time>			
Day of week is <	day>			
Always	-			
Edit the rule descript	tion (click an underlined item)			
Perform an action in a	a time interval			
always				
1				
Help	Cancel	< Back	Next >	Finish

- Select Start feed on <device>, then click recording devices.

## **XProtect Corporate or Expert**

Manage Rule					
Name:	Start Metadata Feed Rule				
Description:					
Active:					
	Step 3: Actions				
Select actions to per	form				
Start recording or	n <devices></devices>				
✓ Start feed on <dev< p=""></dev<>	vices>				
Set <smart wall=""></smart>	to <preset></preset>	=			
Set <smart wall=""></smart>	<monitor> to show <cameras></cameras></monitor>				
Set live frame rate	e on <devices></devices>				
Set recording fram	me rate to all frames for H 264/MPEG4 on <devices></devices>				
Start patrolling on	<pre>&gt;</pre>				
Pause patrolling of	on <devices></devices>				
Move <device> to</device>	<pre>&gt; cpreset&gt; position with PTZ <priority></priority></pre>				
E Calendaria de la contra	for A. Pallana and R. Marka				
Edit the rule descript	ion (click an underlined item)				
Perform an action in a	a time interval				
start feed on recordi	ng device				
Help	Cancel < <u>B</u> ack <u>N</u> ext >	<u> </u>			

- Select All Metadata (or alternatively select a sub-set of the metadata input devices, according to your needs).
- Click Add and then click OK.

Select devices and groups	
Device Groups Recording Servers Cameras All cameras Axis All Microphones All Microphones All Speakers Metadata All Metadata Perimeter Defender metadata	Add  Remove
	OK Cancel

- In the Manage Rule window, click Next.
- Select Perform stop action when time interval ends and then click Next .

### **XProtect Corporate or Expert**

Manage Rule		
Name:	Start Metadata Feed Rule	
Description:		
Active:		
	Step 4: Stop criteria	
Select stop criteria  Perform stop acti No actions perfor	on when time interval ends med on rule end	
Edit the rule descript Perform an action in a	ion (click an underlined item) a time interval	
always start feed on <u>All Metar</u>	data_	
Perform an action who	en time interval ends	
Help	Cancel	<u>F</u> inish

- Click Finish.

The XProtect system now correctly retrieves the metadata from AXIS Perimeter Defender and can show them in live mode on top of the corresponding video stream. However, XProtect does not record the metadata, and hence the metadata cannot be played back when replying a recorded sequence. To record them, you have to add a special rule in the management client. See Activate metadata recording on page 27.

#### Important

The MIP Driver channels can be renamed if you want to, but the name **must always contain the "MIP Driver" keyword** for the Smart Client to find the correct association between them and the corresponding video stream.

#### Activate metadata recording

To activate the metadata recording, you have to define a rule in the XProtect System.

- 1. Open the Management Client.
- 2. Click Rules and Events and then Rules.
- 3. Right-click in the Rules window.

## **XProtect Corporate or Expert**



- 4. Select Add Rule.
- 5. Type a name and description for the new rule. Then select Perform an action in a time interval and click Next.
- 6. Select Always and click Next.

# XProtect Corporate or Expert

Manage Rule		
Name:	Axis Perimeter Defender Metadata Record	
Description:	Record Metadata from Axis Perimeter Defender	
Active:		
	Step 2: Conditions	
Vithin selected ti Outside selected Within the time pe Day of week is <0	ppiy me in <time profile=""> time in <time profile=""> riod <starttime> to <endtime> lay&gt;</endtime></starttime></time></time>	
Edit the rule descript Perform an action in a always	ion (click an underlined item) time interval	
Help	Cancel < Back Next >	<u>F</u> inish

7. Select Start recording on <devices>, then click recording device.

## **XProtect Corporate or Expert**

Manage Rule		
Name:	Axis Perimeter Defender Metadata Record	
Description:	Record Metadata from Axis Perimeter Defender	
Active:		
	Step 3: Actions	
Select actions to per Start recording o Start feed on <de Set <smart wall:<br="">Set <smart wall:<br="">Set live frame rai Set recording fra Set recording fra Start patrolling o Pause patrolling Move <device> to</device></smart></smart></de 	form  n <devices> vices&gt; vices&gt; to <preset> compilor&gt; to show <cameras> te on <devices> me rate on <devices> me rate on all frames for H.264/MPEG4 on <devices> n <device> using <profile> with PTZ <priority> on <devices> o <preset> position with PTZ <priority> </priority></preset></devices></priority></profile></device></devices></devices></devices></cameras></preset></devices>	THE STREET
Edit the rule descrip Perform an action in a always start recording immed	tion (click an underlined item) a time interval liately on recording device Cancel <back next=""></back>	<u> </u>

- 8. Select all the metadata channels and move them to the Selected panel by clicking Add.
- 9. Click OK.

Select devices and groups		×
Device Groups Recording Servers Cameras Microphones Speakers Metadata Perimeter Defender metadata MIP Driver (192.168.90.160) - Metada MIP Driver (192.168.90.160) - Metada	Selected: MIP Driver (192.168.90.160) - Metadata 1 MIP Driver (192.168.90.160) - Metadata 2 Add  Remove	

- 10. In the manage rule window, click Next.
- 11. Select Perform stop action when time interval ends and click Next:

## **XProtect Corporate or Expert**

Manage Rule	
Name:	Axis Perimeter Defender Metadata Record
Description:	Record Metadata from Axis Perimeter Defender
Active:	
	Step 4: Stop criteria
Select stop criteria	tion when time interval ends prmed on rule end
Edit the rule descrij Perform an action in always start recording imme Perform an action w	ztion (click an underlined item) a time interval diately on <u>MIP Driver (192.168.90.66) - Metadata 1, MIP Driver (192.168.90.66) - Metadata 2</u> hen time interval ends
Help	<u>C</u> ancel < <u>B</u> ack <u>N</u> ext > <u>F</u> inish

- 12. Click Finish.
- 13. To check that the metadata are correctly recorded, go to Servers > Recording Servers.
- 14. Expand your recording server, then expand the MIP Driver and check that the icon near the MIP Driver channels has a red square.



You might want to further tune this rule to, for example, only record the metadata when an event occurs. See the XProtect documentation on how to define and customize rules.

#### Important

To show the metadata in playback mode, the corresponding video stream must be recorded too. The default setting to record video streams in Corporate is **on motion detection**. That means that if there is not enough motion to trigger the video stream recording, even if the metadata recording is **always on** it will not be possible to play it back.

#### How to use trigger further actions

The User Defined Events and Analytics Events triggered by the AXIS Perimeter Defender Alarm and Metadata Bridge can be used to trigger further actions, more specifically:

- Using the User Defined Events, specific rules can be used to:
  - Start image and metadata recording on alarms from AXIS Perimeter Defender or, in case a permanent recording is in place, to raise the quality, resolution and frame rate of the recording.
  - To send an email to specific recipients, containing images or videos from the camera that triggered the alarm.
  - To action a hardware output like a dry or wet contacts.
- Using the Analytics Event, a specific alarm can be triggered.

#### How to start image recording using User Defined Events

- 1. Select Rules and Events, then select Rules.
- 2. Right-click Rule.
- 3. Select Add Rule ....

## **XProtect Corporate or Expert**



- 4. Type a name and a description for the rule.
- 5. Select the rule type Perform an action on event....
- 6. Click event.
- 7. Expand User Defined Events.
- 8. Select the event of interest.
- 9. Click OK.
- 10. Click Next.

## XProtect Corporate or Expert

File Edit View Action Tools Help  Image: Recording on APD events Descriptor: Tiggers an image recording when Axis Perimeter Defender generates an intrusion event Active: Descriptor: Step Nerves Descriptor: Desc	Milestone XProtect Management	Manage Rule	– п х	×
Name: Recording on APD events   Description: Triggers an image recording when Axis Perimeter Defender generates an intrusion event   Active: Image: Step 1: Type of rule   Basis Step 1: Type of rule   Step Notices Step 1: Type of rule   Cline: Image: Step 1: Type of rule   Step Notices Step 1: Type of rule   Cline: Image: Step 1: Type of rule   Step Notices St	File Edit View Action Tools Helt			
Cameras, All Metadata     Constraints		Name:	Recording on APD events	
Active:       Security         Security       Security         Secure	Site Navination	Description:	Triggers an image recording when Axis Perimeter Defender generates an intrusion event	
Basics       Steel the rule specy our want to create         Severes       Devices         Clinet       Perform an action in a time interval         Reference       Perform an action in a time interval         Reference       Severe Logs         Severe Logs       Severe Logs         System Dashboard       Severe Logs         Severe Logs       Severe Logs         Access Control       Severe Logs         Severe Logs       Severe Logs	- VMS-NUC-2 - (10 1a)	Active		-
Sep 1: Type of rule Several Se	Basics	Acuve.		-
Servers Servers Client Client Rules and Events Client Cl	Remote Connect Services		Step 1: Type of rule	and metadata
Periodes	Servers	Select the rule to	ype you want to create	
Client C	Pevices	Perform an a	iction in a time interval	
Control of Service         Service Logs	Client			
Image Trans       Finish         Image Trans       Edit the rule description (click an underlined item)         Image Trans       Foreine Exercision         Image Trans       Foreine Exercision         Image Trans       Security	Rules and Events			
Italication Profiles         User-defined Events         Generic Events         Generic Events         System Dashboard         Perform an action or jarget         from devices/activations.server/meanscensed.server         Image: Server Logs         Perform an action or jarget         from devices/activations.server/meanscensed.server         Image: Server Logs         Image: Server Logs         Setcan Events         Setcan Events         Setcan Events         Server Logs         NMIP Plug-ins         Set Navigasion         Federined Events         Second Events <td>Time Profiles</td> <td></td> <td></td> <td></td>	Time Profiles			
User-defined Events Generic Events Ste Navigation Federated Site Hierard Help Konstructures Help Konstructures Help Konstructures Konstructur	Notification Profiles			
Analytics Events     Generic Events     Generic Events     Generic Events     Generic Events     Generics All Metadate     Severicy     Access Control     Severicy     Severicy     Severicy     Severicy     Severicy     Generics All Metadate     Severice     S	🔫 User-defined Events			
Gereic Events System Dashboard System Dashboard System Dashboard Form Benzicas/accading. Berriers/Instructurement. Becreat from Benzicas/accading. Berriers/Instructurement. Becreat Form Benzicas/accading. Berriers/Instructurement.	Analytics Events			
Bedeutivy     System Dashboard     Server Logs     Fordernate State Hierarce     Help     Adds Parimeter, Defender infrusion: 157ART on cam     Adds Parimeter, Defender infrusion: 257ART on cam     Adds Pa	Generic Events			
Image: Server Logs       Perform an action on garged.         Image: Server Logs       Form & action on garged.         Image: Server Logs       Image: Server Logs         Image: Server Logs       Form & action on garged.         Image: Server Logs       Select an Event         Image: Select an Events       Select an Event         Image: Select an Events       Select an Event         Image: Select an Events       Select an Event         Image: Select an Event	System Dashboard	Edit the rule des	cription (click an underlined item)	3
Select an Event Access Control Arranset Amms MIP Plug-ins Site Navigation Federated Site Hierarce Help Finish	Server Logs	From device	n on <u>event</u> s/recording server/management server	<u>VI cameras, All Metadata</u>
Beet al Events Beet al Events Beet Marvagesion Federated Site Hierarc Help Site Navigation Federated Site Hierarc Help He	Access Control		electer Funct	val ends
Berneter Defender intrusion: START on came     AXS Perimeter Defender intrusion: STOP on camer     AXS Perimeter Defe	Transact		elect an event	
Bight MIP Plug-ins Bight Mir Plug-ins Bight Navigation Federated Site Hierard Help Bight Navigation Federated Site Hierard Help Bight Navigation Federated Infrustored START on cam AXS Perimeter, Defended Infrustored START on cam AXS Perim	🕀 🧏 Alarms		Events	
Site Navigasion Federated Site Hierarce Heip Heip Site Navigasion Federated Site Hierarce Site Navigasion Site Nav	🗷 👬 MIP Plug-ins		🕀 🧰 Hardware	
Site Navigation Federated Site Hierard Help Help Help Help Help Help Help Help			Evternal Events	
Site Navigation Federated Site Hierard Help Generic Events User-defined Events Value Action 15 IART on came AXIS Perimeter_Defender infrusion-1 START on came AXIS Perimeter_Defender infrusion-1 START on came AXIS Perimeter_Defender infrusion-1 STOP on camer AXIS Perimeter_Defender infrusion-1 STOP on camer AXIS Perimeter_Defender infrusion-2 START on camer AXIS			Bertenia Events	
Help  User-defined Events  AVGS Perimeter, Defender infrusion-1 START on cam  AVGS Perimeter, Defender infrusion-1 START on cam  AVGS Perimeter, Defender infrusion-1 START on cam  AVGS Perimeter, Defender infrusion-1 STOP on came  AVGS Perimeter, Defender infrusion-2 START on cam  AVGS Perimeter, Defender infrusion-2 START on came  AVGS	Site Navigation Federated Site Hierarc		Generic Events	
AVS Preimeter_Defender insusion-1 START on cam AVS Preimeter_Defender insusion-1 STOP on came AVS Preimeter_Defender insusion-1 STOP on came AVS Preimeter_Defender insusion-1 STOP on came AVS Preimeter_Defender insusion-3 STOP on came AVS Preimeter_Defender insusion-3 STOP on came AVS Preimeter_Defender insusion-3 STOP on came AVS Preimeter_Defender insusion-2 STATT on came AVS Preimeter_Defender insusion-2 STOP on came AVS Preimeter_Defender insusion-2 STOP on came Statter Statter Stop on came Statter Monitor		Help	Viser-defined Events     Finish     AXIS Parimeter, Defender intrusion-1 START on cam	
AVIS Perimeter_Defender intrusion-1 STAPT on cam     AVIS Perimeter_Defender intrusion-1 STOP on camer     AVIS Perimeter_Defender intrusion-1 STOP on camer     AVIS Perimeter_Defender intrusion-2 STAPT on came     AVIS Perimeter_Defender intrusion-2 STAPT on camer     AVIS Perimeter_Defender intrusion-2 STAPT on camer     AVIS Perimeter_Defender intrusion-2 STAPT on camer     Svistem Monitor     Svistem Monitor	Ø		AXIS Perimeter_Defender intrusion-1 START on cam	
AVS Perimeter_Defender intrusion-1 STOP on camer     AVS Perimeter_Defender intrusion-1 STOP on camer     AVS Perimeter_Defender intrusion-2 STAPT on camer     SAS Perimeter_Defender intrusion-2 STAPT on			AXIS Perimeter_Defender intrusion-1 START on cam	
Avid Semineter Defender Intrusion 1 STOP on came     Avid Semineter Defender Intrusion 1 STOP on came     Avid Semineter Defender Intrusion 2 STAPT on came     Avid Semineter Defender Intrusion 2 STAPT on came     Avid Semineter Defender Intrusion 2 STAPT on came     Big B Recording Servers			AXIS Perimeter_Defender intrusion-1 STOP on camer	
AVIS Perimeter_Defender intrusion-2 START on cam     XVIS Perimeter_Defender intrusion-2 STOP on came     B			AXIS Perimeter_Defender intrusion-1 STOP on camer	
Constant Services			AXIS Perimeter_Defender intrusion-2 START on cam	
C C Cancel			AXIS Perimeter_Defender intrusion-2 STOP on camer	
			System Meniter	
OK Cancel			< > >	
			OK Cancel	

11. If you want to, select an adapted time profile or click Next.

Manage Rule		
Name:	Axis Perimeter Defender Metadata Record	
Description:	Record Metadata from Axis Perimeter Defender	
Active:		
	Step 3: Actions	
Select actions to per Start recording or Start feed on <dev Set <smart wall=""> Set <smart wall=""> Set ive frame rate Set recording fram Start patrolling on Pause patrolling on Move <device> to</device></smart></smart></dev 	orm <a href="https://www.commerasson-state-org/line"> <a href="https://www.commerasson-state-org/line"> <a href="https://www.commerasson-state-org/line"> <a href="https://www.commerasson-state-org/line"> <a href="https://www.commerasson-state-org/line"> <a href="https://www.commerasson-state-org/line"> </a> </a> <a href="https://www.commerasson-state-org/line"> </a> <a a="" href="https://www.commerasson-state-org/line" line<="" www.commerasson-state-org=""> <!--</td--><td>THE REPORT OF THE REPORT OF TH</td></a></a></a></a></a>	THE REPORT OF TH
Edit the rule descript Perform an action in a always start recording <u>immedi</u>	ion (click an underlined item) time interval ately on <u>recording device</u>	
Help	Cancel < <u>B</u> ack <u>N</u> ext >	<u>F</u> inish

12. Select the action Start recording on <devices>

### **XProtect Corporate or Expert**

- 13. Click Recording device and select the associated cameras that you want to record on the selected User Defined Event.
- 14. Click Next.
- 15. If needed, repeat the same steps to define the action to perform on Stop. For example stop the recording after 60 seconds.
- 16. Click Finish.

#### How to send an email using User Defined Events

In order to be able to send an e-mail when AXIS Perimeter Defender triggers a specific User Defined Events, it is necessary to first define an smtp server and then a notification profile:

- 1. Go to Tools > Options.
- 2. Select the Mail server tab and enter the corresponding information.

options								2
ieneral	Server Logs	Mail Server	AVI Generation	Network	Bookmark	User Settings	Evidence Lock	Access <
Mail se	rver settings -							
Sender	re-mail addres	is:						
Outgoi	ng mail server	address (SMT	P):					
Ser.	ver requires la	ain						
User n	ame:	ann)						
Passw	ord:							
	1.1					OK		
ŀ	help				L	UK	Car	ncel

- 3. You have to provide a sender e-mail, the IP address or hostname of the SMTP server and, if it requires authentication, the username and password.
- 4. Click OK.
- 5. Click Rules and Events.
- 6. Click Notification Profiles.
- 7. Right-click Notification Profiles and then select Add Notification Profile.
- 8. Type a name for the new notification profile and an optional description, then click Next.
- 9. Customize the notification email and then click Finish.

## XProtect Corporate or Expert

Now you can define a rule that sends a notification using this profile. See *How to start image recording using User Defined Events on page 32.* As action to trigger, select **Send notification to <profile>** and select the email notification profile defined in this section.

#### How to trigger an alarm from an Analytics Event

Analytics Events can be used to trigger an alarm in the XProtect system. However, to be able to choose an Analytics Event as a trigger for an alarm, the Analytics Event must be defined in the Management Client. If the event is not defined, it will still be triggered if the option is selected. The Event Server and the Smart Client receive the event, but it is not possible to use it to trigger a further alarm.

- 1. Expand Rules and Events.
- 2. Click Analytics Events.
- 3. In the Analytic Events pane, right-click Analytics Events and click Add New....

Milestone XProtect Management Client 201	16		
File Edit View Action Tools Help			
🗏 🦻 🕜 🗢 🛱			
Site Navigation	Analytics Events	Properties	
NEWMOBY - (10.0a)	🖃 🤻 Analytics Events	Name	
🕀 🛄 Basics	AXIS Perimeter Defender Intrusion START	AVIS Dedeedee between START	
🕀 🌇 Remote Connect Services	AXIS Perimeter Defender Intrusion STOP	Axis Ferneter Detender Industri START	
🖲 🔲 Servers			Test Event
🗄 🌠 Devices		Developing	
Ulient		Description.	
E Rules and Events			
Time Profiles			
Notification Profiler			
Vser-defined Events			
Analytics Events			
Generic Events			
🗄 🧐 Security			
🗄 🔕 System Dashboard			
🔅 📳 Server Logs			
- Mecess Control			
III 🕄 Transact			
🗉 🌏 Alarms			
MIP Plug-ins			
AUS Communications			
Perimeter Detender			
ite Navigation Enderated Site Hierarchy			
Site Navigation   Federated Site Hierarchy			

4. Type a name with the following syntax: "AXIS Perimeter Defender ALERT\_TYPE START\_STOP", where ALERT\_TYPE is one of the following values: "Intrusion", "Loitering", "ZoneCrossing", "Conditional" and START\_STOP is one of the following values: "START" or "STOP".

For example, if you want to trigger a rule when the Analytics Event associated with the start of an intrusion is received, name the Analytics Event "AXIS Perimeter Defender Intrusion START".

- 5. Optionally add a description to the Analytics Event.
- 6. Save the configuration.

Now the Analytics Event can be used to trigger an Alarm. You need to specify exactly which camera must generate the Analytics Event for the corresponding Alarm to be triggered, thus allowing to trigger different Alarms for different cameras.

Milestone XProtect Management Clier	nt 2016			
File Edit View Action Tools Help				
<b>□ 9 0 • 8</b>				
Site Navigation	Alarm Definitions	Properties		6
- D NEWMOBY - (10.0a)	E 🛃 Alarm Definitions	Alarm definition		
Generation      Generatio	- & Alarm on Video Analytics	Enable:		
🖲 🔟 Servers		Name:	Alarm on Video Analytics Event	
We Devices      Gient		Instructions:	None	A
Rules and Events				-
Rules		Timer		
Notification Profiles		Trigger	Analytics Events	
User-defined Events		nggeing even.	Analysics Events	•
Generic Events			AXIS Perimeter Detender Intrusion START	•
B Content Events		Sources:		Select
System Dashboard     Server Loss		Activation period		
Access Control		Time profile:	Always	•
III E Transact		Event based:	Start:	Select
Alarm Definitions			Stop:	Select
Alarm Data Settings Sound Settings		Operator action required		
🕀 🏘 MIP Plug-ins		Time limit:	1 minute	•
AXIS Communications		Events triggered:		Select
		Other		
		Related cameras:	Unknown Item	Select
		Related map:		•
		Initial alarm owner:		•
		Initial alarm priority:	High	•
		Initial alarm category:		•
		Events triggered by alarm:		Select
		Auto-close alarm:		
Site Navigation Federated Site Hierarchy	<			
5				

For further details on how to define an Alarm, see the Milestone documentation.

### How to use the Smart Client

This section describes how to receive and use the metadata, the alarms, the user defined events and the bookmarks in the Smart Client. For a more detailed description of the Smart Client, see the Milestone documentation.

#### About alarms

To view all alarms, go to Alarm Manager.

## **XProtect Corporate or Expert**



To view the corresponding video sequence in the video player, click one of the alarm in the list.

Alarms can also be shown in a tile of the Live tab, by commuting to the Setup mode and dragging the Alarm list item into a free tile.

### **XProtect Corporate or Expert**



If you are not interested in alarm reception in the Smart Client, you can deactivate the automatic triggering of alarms by the AXIS Perimeter Defender Metadata Bridge by using the Configuration Tool. See *Software installation on the host running the XProtect Recording Server on page 8*.

#### How to receive and monitor user-defined events

Once the necessary user-defined events have been set up, they can be received and monitored in the Smart Client.

- 1. Open the Setup mode.
- 2. Drag the Alarm List in a free tile.
- 3. Select the Alarm List tile.
- 4. In Properties, change the Alarm value of the combo box to Event:



5. The events triggered by AXIS Perimeter Defender show up in the corresponding tile when you commute back from the **Setup** mode.



6. You can also switch from alarms to user-defined events in the Alarm Manager tab, by following the same procedure.

#### About bookmarks

If the option is activated, bookmarks are automatically inserted in the corresponding video stream when AXIS Perimeter Defender triggers an alarm. They can be retrieved in the Smart Client, for example in the **Playback** tab.

## **XProtect Corporate or Expert**



The Smart Client shows the bookmarks as grey ticks on the timeline.

Bookmarks can also be used to search for sequences in the Sequence Explorer tab.

## **XProtect Corporate or Expert**



- 1 Sequence explorer tab
- 2 Cameras
- 3 Combo box
- 4 Search for string
- 5 Bookedmarked sequence
- 6 Bookmark details
- 1. Open the Sequence Explorer tab.
- 2. Select the camera(s) of interest.
- 3. Select **bookmarks** in the combo box.
- 4. Enter the string to search for in the bookmarks name, for example "AXIS Perimeter Defender".
- 5. The corresponding bookmarked sequences are shown in the lower pane.
- 6. The bookmark details are shown in the right pane, and the corresponding sequence with the metadata overlay is shown in the video player.

#### Metadata display

The Smart Client automatically shows the metadata on top of the corresponding video stream, both in live and in playback mode, in every video player in the Smart Client.

### **XProtect Corporate or Expert**



What a typical metadata looks like. In this screenshot the intrusion zone is shown.

- 1. The upper right corner of the image contains a colored spot, the color shows 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)
  - 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 shown in blue. In the previous screenshot (the one inside Security Desk) one camera shows an intrusion zone and the other the two zones of a Zone-crossing scenario
- 4. The approximate actor trajectory is shown in red (for a person) or blue (for a vehicle)

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

## **XProtect Enterprise/Professional/Express**

## XProtect Enterprise/Professional/Express

### Configuration

Through the MIP Plugins for AXIS Perimeter Defender running in the XProtect Management Client it is possible to configure different aspects of the system:

- You can scan the list of cameras defined within XProtect and automatically select those where AXIS Perimeter Defender is installed. See Add Axis devices running AXIS Perimeter Defender to XProtect on page 10.
- The plugin allows the user to deactivate the automatic generation of XProtect Alarms when an AXIS Perimeter Defender triggers an alarm (the alarm generation is activated by default)
- The plugin allows the user to deactivate the automatic generation of XProtect Analytics Events when an AXIS Perimeter Defender triggers an alarm (the Analytics Events is activated by default).

#### Alarms and Analytics events configuration through the Management Client Plugin

#### Important

Before configuring the software, both the MIP Plugin for the Management Client and the AXIS Perimeter Defender Metadata Bridge must be installed. In addition, the Metadata Bridge must also be configured to be able to access the XProtect System.

- 1. Open the Management client, and add to the XProtect system all the cameras you need. You need to add both the Axis devices running AXIS Perimeter Defender and the video devices whose video stream is analyzed by AXIS Perimeter Defender
- 2. Go to MIP Plugins > AXIS Communications > Perimeter Defender.
- 3. Click the Alarm & Metadata configuration tab.
- 4. If you want to automatically trigger an XProtect alarm when AXIS Perimeter Defender generates one, select Automatically trigger alarms on Perimeter Defender alarm reception.
- 5. If you want to automatically trigger an XProtect Video Analytics Event when AXIS Perimeter Defender generates an alarm, select Automatically trigger analytics events.
- 6. In most of the cases, you don't need to manually specify the destination IP address and listening port for alarms (i.e., the port that the AXIS Perimeter Defender Alarm & Metadata Bridge uses to listen for incoming alarms from AXIS Perimeter Defender and its IP address as used by the AXIS Perimeter Defender instances to send alarms). In some special cases, for example when there is a NAT or port forwarding between the AXIS Perimeter Defender devices and the host where the Alarm Metadata bridge runs, you might want to set them manually. In this case enter the Metadata source mac adress and Metadata source listening port that the AXIS Perimeter Defender devices should use to send their alarms to the Alarm & Metadata.
- 7. Configuration Reset drops the current configuration and restarts with a new configuration from scratch.
- 8. Save the changes by clicking the button.

XProtect Enterprise/Professional/Express



- 1 Site navigation
- 2 Metadata configuration tab
- 3 Metadata parameters
- 4 Camera list
- 9. When saving a new configuration, the AXIS Perimeter Defender Alarm & Metadata Bridge is automatically restarted.

#### How to use Analytics Events to trigger alarms

Analytics Events can be used to trigger an alarm in the XProtect system. To be able to choose an Analytics Event as a trigger for an alarm, the Analytics Event must be defined in the Management Client. If not defined, the Analytics Event will still be triggered if the option is selected, and as such, the Event Server and the Smart Client will receive them, but it will not possible to use it to trigger a further alarm.

To define an Analytics Event, do the following:

- 1. Click Events and Outputs in the left pane and then right-click Analytics Events.
- 2. Click Create New.

Milestone XProtect Enterprise 2016 R2 Manageme	nt Application	_		2
ile Services Wizards Options Help				
🖶 🙂 🐂 📓 🧶 🚱				
Getting started     Getting started     Getting started     Advanced Configuration     Generation     Hardware Devices     Hardware Device 1     Benerative Hardware Device 2	11.44.32 AM      Thank you for using this trial license to demonstrate or evaluate the XProtect video management software. The trial integration is the trial of the trial integration of the trial	al license is r	not for co	
Hardware Device 3     Hardware Device 4     Hardware Device 5     Hardware Device 5	Analytics Events:			
Hardware Device 7     Gameras and Storage Information     Microphones     Events and Output	Name			
Analytics Events     Greate New     Hardware Output     Hardware Output     Manual Events				
Generic Events     Gutput Control on Event     Government     Scheduling and Archiving				

- 3. Enter a name for the Analytics Event with the following syntax: "AXIS Perimeter Defender <ALERT\_TYPE> <START\_STOP>", where <ALERT\_TYPE> is one of the following values: "Intrusion", "Loitering", "ZoneCrossing", "Conditional" and <START\_STOP> is one of the following values: "START" or "STOP". For example, if you want to trigger a rule when the Analytics Event associated with the start of an intrusion is received, name the Analytics Event "AXIS Perimeter Defender Intrusion START"
- 4. Optionally add a description to the Analytics Event.

### **XProtect Enterprise/Professional/Express**

5. Save the configuration.

Now the Analytics Event can be used to trigger an Alarm. You can specify exactly which camera must generate the Analytics Event for the corresponding alarm to be triggered, thus allowing to trigger different alarms for different cameras.

Jarm Definition					×
				_	
					_
larm Definition	Alam definition				
	Enable:	$\checkmark$			
	Name:	Alarm on Video Analytics			
	Instructions:	None		~	
				· _	
	Trigger				
	Triggering event:	Analytics Events		$\sim$	
		AXIS Perimeter Defender In	ntrusion START	$\sim$	
	Sources:	IP250	Select.		
	Activation period				
	Time profile:	Always		$\sim$	
	O Event based:	Start:	Select		
		Stop:	Select		
	Operator action required				
	Time limit:	1 minute		~	

For further details on how to define an alarm, see the Milestone documentation.

#### How to use Manual Global Events to trigger further actions

It is possible to define Manual Global Events that are associated to specific cameras, AXIS Perimeter Defender scenarios, and scenario types (start/stop). The advantage of Manual Events is that they in turn can trigger specific actions like send emails, send text messages, or trigger hardware outputs.

The AXIS Perimeter Defender Alarm & Metadata Bridge automatically looks for defined Manual Global Events that respect a certain format and if it finds them, it triggers automatically those satisfying the alarm conditions. It is for example possible to define:

- a Manual Event that is triggered on every alarm START from any camera
- a Manual Event that is triggered on every alarm START of a specific camera
- a Manual Event that is triggered on a specific scenario of a specific camera
- any combination of the previous three

Every Manual Global Event that is supposed to be triggered on an AXIS Perimeter Defender alarm must have a name that respects a specific format: "AXIS Perimeter Defender <ScenarioName> <ScenarioName> <ScenarioType> on camera <CameraName>" where:

- <ScenarioName> is the name of the scenario as defined in the AXIS Perimeter Defender user manual. Usually it looks like "Intrusion-1", but can be customized at configuration phase through the AXIS Perimeter Defender Setup. If you want the Manual Global Event to be triggered by any scenario, use "ALL" as <ScenarioName>
- <ScenarioType> is either "START", "STOP" or "ALL". Use "ALL" if you want the Manual Global Event to be triggered for both START and STOP alarms
- <CameraName> is the name of the camera as defined in XProtect. When AXIS Perimeter Defender triggers an alarm, it does so by analyzing images from a device that must also be present in XProtect. For AXIS Perimeter Defender, this is the device where AXIS Perimeter Defender is installed. <CameraName> is the name of the associated XProtect Camera. Use "ALL" if the Manual Global Event must be triggered by AXIS Perimeter Defender alarms associated to any XProtect camera. If you want to use an XProtect Camera Name as <CameraName>, replace any space of the XProtect

### XProtect Enterprise/Professional/Express

#### NOTICE

Camera Name with the underscore ('\_') character in the Manual Global Event name. For example, if the camera is named "Right Entrance Camera", use "Right\_Entrance\_Camera" as <CameraName>. Alternatively, rename the XProtect Camera Name to remove any space.

#### NOTICE

The three parameters <ScenarioName>, <ScenarioType>, <CameraName> are all case insensitive, so lowercase and uppercase letters are considered the same.

Here are some examples of Manual Global Events and by which AXIS Perimeter Defender alarms they will be triggered:

- "AXIS Perimeter Defender Intrusion-1 START on camera ALL": will be triggered by any AXIS Perimeter Defender alarms START related to a scenario called "Intrusion-1" from any camera
- "AXIS Perimeter Defender ALL ALL on camera IP250": will be triggered by any AXIS Perimeter Defender alarm START or STOP related to any scenario from the XProtect Camera "IP250"
- "AXIS Perimeter Defender ALL START on camera ALL": will be triggered by any AXIS Perimeter Defender alarm START related to any scenario from any camera
- "AXIS Perimeter Defender ZoneCrossing-1 STOP on camera IP250": will be triggered by any AXIS Perimeter Defender alarms STOP related to the scenario "ZoneCrossing-1" from XProtect camera "IP250"

To define a new Manual Global Event, do the following:

- 1. Expand Events and Outputs.
- 2. Expand entry Manual Events.
- 3. Right-click Global.
- 4. Click Properties.

e Services Wizards Options Help							
🔚 🧐 🕅 🚮 🧭 🚱	200.20 PM	/	ation Country about			Diago	-
Getting started	3.03.30 PM	rou have made changes to the conligu	auon. Save the chang	es to apply them to the syst	em. 3	Discal	
	11:44:32 AM	Thank you for using this trial license to	demonstrate or evaluation	ate the XProtect video mana	agement softwa	are. The trial license is not	t for co
Hardware Device 1     Hardware Device 2     Hardware Device 3     Hardware Device 3     Hardware Device 4	milestone						
Hardware Device 5     Hardware Device 6     Hardware Device 7	Manual E	vents Summary:					
Cameras and Storage Information	Event Name		Availability	Timer Events Defined	Send E-mail	Attach Image From	Send
Events and Output	AXIS Perimeter Defend	er Intrusion-1 START on camera IP250	Global	0		N/A	
Analytics Events	AXIS Perimeter Defend	ler All All on camera IP250	Global	0		N/A	
DB SafeZone(-edge) Intrusi	AXIS Perimeter Defend	er All START on camera ALL	Global	0		N/A	i i
Manual Events     Solution of the second secon							

## XProtect Enterprise/Professional/Express

Manual Event Properties		- 0
Global     KATS Perimeter Defender ALL ALL on camera IP250     KATS Perimeter Defender ALL STATT on camera IP250     KATS Perimeter Defender Infrastor 3 STATT on camera IP250	Event configuration Event name: AXIS Perimeter Defender Intrusion-1 START on camera IF	2250
	Notifications Send e-mail if this event occurs Attach inage from camera Set data from: N/A	

- 5. Select Global.
- 6. Click Add.
- 7. Enter the Even Name.
- 8. Optionally select Send e-mail if this event occurs. See How to use Manual Global Events to send an email on page 49.
- 9. Optionally select Send SMS if this event occurs. See How to use Manual Global Events to send an email on page 49.
- 10. Click OK.

Now you can use the Manual Global Event to trigger a Hardware Output.

Surveillance Server  Surveillance Server  Advanced Configuration  Advanced Con	Activate output on event  Venet  Vones  ACS Perimeter Defender Intrusion-1 START On camera IP250  AXS Perimeter Defender Intrusion-1 START On camera IP250  AXS Perimeter Defender AllSTART on camera ALL
Hardware Devices     Hardware Devices     Hardware Device 1     How the second se	Activate oudput on event Event Output Output Okones Alones AXS Perimeter Defender Intrusion-1 START on camera IP250 AXS Perimeter Defender All START on camera ALL
the studiuse Device 3     the studiuse Device 4     the studiuse Device 5     the studiuse 2	Event Output Okone> V Okone>  AXIS Perimeter Delender Intrusion-I START on camera IP250 AXIS Perimeter Delender All START on camera IP250 AXIS Perimeter Delender All START on camera ALL
Hardware Device 4     Hordware Device 5     Hardware Device 5     Hardware Device 5     Hardware Device 7     Screase and Skorape Briomation     Analytics Events     Section 4 doubt	Chone> Ch
General and Starte Device 5     General and Starte Device 5     General and Starte Device 5     General and Starte Information     P Microphones     fersts and Stort     General and Starte     fersts and Stort     General Analytics Events     General Analytics     General Analy	clanes AXS Perimeter Defender All All on camera IP250 AXS Perimeter Defender All START on camera IP250 AXS Perimeter Defender All START on camera ALL
Commerce and Storage Information     Commerce and Storage Information     Philosophones     Commerce and Odpub     Commerce Analytics Events     Commerce Analytics	
Control and Output     Control Control Control     Control Control     Contro     Control     Control     Control     Con	
Analytics Events B SafeZone(-edge) Intrusi Of Hardware Input Events Of Hardware Output	
😥 Hardware Output	
🗃 🐪 Manual Events	
AVIS Barimeter Defender All	
All Perimeter Defender ALI	
AXIS Perimeter Defender Intr	
2 Output Control on Event	
Matrix	
Logs	
Notifications	
Central	
Access Control	
Master/Slave	
⊕ 🙀 Users	
🤹 Services	
⊕ U Servers	Configure events -      Open     Configure Output
Alarms	

1. Go to Events and Outputs.

## **XProtect Enterprise/Professional/Express**

- 2. Right-click Output Control on Event, then click Properties.
- 3. Select the Manual Global Event of interest.
- 4. Select the Output Hardware you want to activate.
- 5. Click OK.

#### NOTICE

When you change the Manual Global Events names you must restart the AXIS Perimeter Defender Alarm & Metadata Bridge service for the changes to take effect.

#### How to use Manual Global Events to send an email

First you need to configure the email notifications.

- 1. Click Notifications.
- 2. Right-click Email and select Properties.



- 3. Select Message Setting.
- 4. Select Enable email.
- 5. Enter the recipient(s) field, the subject and the message.
- 6. If you want, select Attachment settings and configure the attachment.

#### Important

Do not select Embed images in email. If you do, the email will not be sent. Select Include images and set the image properties.

7. Select Server settings and configure the server parameters, then click OK.

# XProtect Enterprise/Professional/Express

-mail Properties		>						
Message Settings	Email settings							
Attachment Settings	Enable email							
ierver Settings	Recipient(s):							
	alams@myServer.com							
	To send an email to more than one reci	pient, insert a semicolon to separate the email addresses.						
	Subject text:							
	Alarm from XProtect							
	Message text:							
	<ul> <li>Click a link to include a variable in the Name of triggering event</li> </ul>	message text: <u>Trigger time</u>						
	Camera name	Error text						
	Ignore similar messages for:	Use schedule profile:						
	0 🚖 second(s)	Always on 🗸 🗸						
	Specify when you want to send an ema	il by changing the schedule profile.						
		OK Cancel						

8. Save the XProtect configuration.

Milestone XProtect Professional 20	16 R2 Mar	agement Application		-	Ц	ļ.
File Services Wizards Option	s Help					
Getting started	1:49:08 P	M 🕕 Thank you fo	or using this trial licens	se to demonstrate or evaluate the XProtect video management software. The trial license is no	t for com.	-
Advanced Configuration						
Axis 2.49	miles	tope				
Camera 1	111103					
Camera 2						
Camera 4	E-r	mail Summany				
Camera 5		nan Summary				
Camera 6						_
🧐 Camera 7	Enabled	Recipients	Subject	Message		
Camera 8		alarms@myServer.com	Alarm from XProtect	My alarm text	Te	st
Cameras and Stora						
Events and Output						
Analytics Event:						
do Hardware Input						
Hardware Outpi						
Clobal						
Generic Events						
Output Control						
🕀 🛞 Scheduling and Arcl						
Matrix						
- 🗳 Logs						
🖃 🖂 Notifications						
🖂 Email						
SMS						
Scheduling						
Central						
Server Assess						
Master/Slave						
Ilsers						
Services						
Servers						
🗄 🦉 Alarms						
And a second sec						
MIP Plug-ins						

9. To test the parameters, click Test.

#### **XProtect Enterprise/Professional/Express**

- 10. To activate the emails, go to How to use Manual Global Events to send an email on page 49.
- 11. If you want, you can attach email from a chosen camera. This only works if you've configured the Attachment part of the email notifications.
- 12. Click OK.
- 13. Save the XProtect configuration.

#### How to use the Smart Client

This section describes how to receive the alarms and the Manual Global events and use them in the Smart Client. For a more detailed description of the Smart Client, see the Milestone documentation.

#### About alarms

To view all alarms, go to Alarm Manager.



To view the corresponding video sequence in the video player, click one of the alarm in the list.

Alarms can also be shown in a tile of the Live tab, by commuting to the Setup mode and dragging the Alarm list item into a free tile.

## XProtect Enterprise/Professional/Express



If you are not interested in alarm reception in the Smart Client, you can deactivate the automatic triggering of alarms by the AXIS Perimeter Defender Metadata Bridge by using the Configuration Tool. See *Software installation on the host running the XProtect Recording Server on page 8*.

#### Manual global events

Once the necessary Manual Global Events have been defined, they can be received and monitored in the Smart Client.

- 1. Commute in the Setup mode.
- 2. Drag the Alarm List to a free tile.
- 3. Select the Alarm List tile.
- 4. In the Properties section of the left panel, change the Alarm value of the combo box to Event.

XProtect Enterprise/Professional/Express



5. The events triggered by AXIS Perimeter Defender are shown in the corresponding tile when you commute back from the Setup mode.



XProtect Enterprise/Professional/Express

6. In the Alarm Manager tab, you can also switch from Alarms to Manual Global Events by following the same procedure.

## Advanced configuration

#### **Network communications**

This section describes the network communications between the different logical modules composing a complete system.



This image illustrates the architecture of a complete system from a network point of view.

- XPCO management server, event server and recording server are shown on different physical servers, but they can be installed on a single one.
- The AXIS Perimeter Defender alarm and metadata bridge is shown as a separate server, but can be installed on the XPCO host as well.
- The AXIS Perimeter Defender alarm and metadata bridge receives the alarms from AXIS Perimeter Defender on its TCP/IP listening port 30000. It then transmits the alarms to the XPCO Event Server on its port 22331.

- When an alarm finishes, a bookmark is sent to the XPCO Management Server, on its port 80.
- The AXIS Perimeter Defender alarm and metadata bridge connects to AXIS Perimeter Defender and retrieves the metadata stream. It then implements an MIP Driver listening on port 50000 where the XPCO Recording server connects to get the metadata of the different "channels" that the MIP Driver implements.
- The AXIS Perimeter Defender alarm and metadata bridge stores its configuration in the XPCO Management Server.

#### How to add new video sources to the system

When adding a new video source, you need to first configure the video source with the XProtect System. This step is covered by the Milestone XProtect User Guide. The next steps depend on the type of video source added and on the XProtect product.

#### How to configure an Axis device with AXIS Perimeter Defender

In the following instructions, the video source "AXIS Q7404 Video Encoder (192.168.2.121) – Camera 1" has recently been added to the system.

Once the new video source has been added, follow these steps:

- Configure the AXIS Perimeter Defender installed on the device and start the application.
- In the AXIS Perimeter Defender cameras tab, click Scan new cameras and, if the pre-selection steps is chosen, make sure that the new devices are selected.

Video source prefiltering			-		×
Select the video sources to scan for AXIS Perimeter Defender					
NAME           □D-Link Corporation DCS*7513 (192168.2.51) - Camera 1           ANIS 06/04 E PTZ Dome Network Camera (192.168.2.24) - Camera 1           ANIS 06/03 E PTZ Dome Network Camera (192.168.2.24) - Camera 1           ANIS 06/03 E PTZ Dome Network Camera (192.168.2.24) - Camera 1           ANIS 97404 Video Encoder (192.168.2.127) - Camera 1           ANIS 97404 Video Encoder (192.168.2.127) - Camera 1           ANIS 97404 Video Encoder (192.168.2.24) - Camera 1           ANIS 97404 Video Encoder (192.168.2.40) - Camera 1	IP ADDRESS 1921682.51 1921682.24 1921682.22 1921682.22 1921682.24 1921682.24 1921682.49 1921682.40	DRIVER ONVIF Avis ICh/PZDevice Avis ICh/PZDevice AvisCh/PZDevice AvisCh/Device Avis1Ch/Device			
Clear selection Select all I Activate brand pre-filtering			ОК	Cano	el

Only valid for XProtect Corporate/Expert: Once the scan has finished, select the new devices one by one and set the Display live metadata and Display recorded metadata in playback mode options.

### Advanced configuration

AXIS P3225-LVE Network Camera (192.168.2.49) - Camera 1 AXIS Q7404 Video Encoder (192.168.2.121) - Camera 1	AXISPerimeterDefender AXISPerimeterDefender	1.0.3 1.0.1501
192.168.2.121		
Display live metadata		

In the Alarm & Metadata Configuration tab, click Generate user-defined events if you plan to use them, and then save the configuration with Ctrl+S.

**Only valid for XProtect Corporate/Expert:**Consider if you need to replace the MIP Driver device within the XProtect system, see *How to increase the number of channels of the MIP Driver on page 57.* In any case, display the channel table using the **Display metadata channels** button in the **Alarm & Metadata Configuration** tab and make sure that the metadata channel associated to the new device is enabled on the MIP Driver device.

Metadata Channel	Table	- 0	×
CHANNEL NUMBER	METADATA SOURCE	VIDEO SOURCE	
1 2 3	SZ-e with id 192.168.2.40 and ref 1 SZ-e with id 192.168.2.49 and ref 2 SZ-e with id 192.168.2.121 and ref 3	Camera named 'AXIS P1353 Network Camera (192.168.2.40) - Camera 1' (http://192.168.2.40) Camera named 'AXIS P3225-LVE Network Camera (192.168.2.49) - Camera 1' (http://192.168.2.12 Camera named 'AXIS Q7404 Video Encoder (192.168.2.121) - Camera 1' (http://192.168.2.12	0/) 3.2.49/) 11/)
Unselect all Sele	sct all Free the selected metadata	channels OK Ca	ancel
Servers	ing Servers er Servers	<ul> <li>AXIS P3225-LVE Network Camera (192.168</li> <li>AXIS Q6032-E PTZ Dome Network Camera</li> <li>AXIS Q6034-E PTZ Dome Network Camera</li> <li>AXIS Q6034-E PTZ Dome Network Camera</li> <li>AXIS Q7404 Video Encoder (192.168.2.121)</li> <li>D-Link Corporation DCS-7513 (192.168.2.5)</li> <li>MIP Driver (192.168.90.189)</li> </ul>	(192 (192 (192
Security System Da	shboard	MIP Driver (192, 168, 90, 189) - Metadata MIP Driver (192, 168, 90, 189) - Metadata MIP Driver (192, 168, 90, 189) - Metadata	23

#### How to increase the number of channels of the MIP Driver

The MIP Driver device that sends the metadata streams to XProtect must be replaced if the number of channels it presented when added to XProtect the very first time is smaller than the number of AXIS Perimeter Defender instances sending metadata to XProtect.

Usually you need to replace the MIP Driver device when the number of video sources analyzed by AXIS Perimeter Defender is higher than the metadata channels provisioned at the first installation. When this happens, you get the following message.

Advanced configuration



To check if you need to replace the MIP Driver device, compare the value of the Number of provided metadata channels field with the actual number of metadata channels of the MIP Driver device.

AXIS Perimeter Defender cameras Alarm & Meta	adata Configuration
Metadata source mac address	Set manually 00:40:8C:99:83:00 Get another one
Metadata source listening port	50000 🗘 Check if free
Number of provided metadata channels	4
Metadata source password	Show in plaintext
<ul> <li>VMS-NUC-2 - (10.1a)</li> <li>Basics</li> <li>License Information</li> <li>Site Information</li> <li>Remote Connect Services</li> <li>Axis One-click Camera Connectio</li> <li>Servers</li> <li>Failover Servers</li> <li>Failover Servers</li> <li>Devices</li> <li>Cameras</li> </ul>	Image: Second

In this example, the MIP Driver device must be replaced in order to obtain the 4 metadata channels provided by the metadata source.

Select one of the following options:

- Remove the MIP Driver device and then add it again. Note that all the previously recorded metadata on all channels are lost.
- To keep the existing recorded metadata, use the function Replace hardware.
- 1. Right-click the MIP Driver device and click Replace Hardware.

# Advanced configuration

MIP Driver (192.168.90	100	Collapse	
MIP Driver (192.16 MIP Driver (192.16	9	Edit Hardware	Del
	*	Move Hardware	Dei
		Replace Hardware	
		Rename Hardware	F2
	<b>~</b>	Enabled	
	2	Refresh	F5

#### 2. Click Next.

3. Check the information. If nothing has changed, click Next.

For each new device, select which old device (including existing databases) to inherit. If a new device should not inherit any old device, select None'. Databases will be deleted for old devices which are not inherited. New Hardware Device Inherit Metadata Select Device Metadata 2 Select Device Metadata 3 Select Device	Replace Hardware		×
New Hardware Device     Inherit       Metadata     Metadata       Metadata 1     Select Device       Metadata 2     Select Device       Metadata 3     Select Device	For each new device, select which o If a new device should not inherit any Databases will be deleted for old dev	ld device (including existing databases) to inherit. old device, select None. ices which are not inherited.	
Metadata         Select Device           Metadata 1         Select Device           Metadata 2         Select Device           Metadata 3         Select Device	New Hardware Device	Inherit	
Metadata 1         Select Device           Metadata 2         Select Device           Metadata 3         Select Device	Metadata		
Metadata 2 Select Device Metadata 3 Select Device	Metadata 1	Select Device	~
Metadata 3 Select Device	Metadata 2	Select Device	~
	Metadata 3	Select Device	~
Metadata 4 Select Device	Metadata 4	Select Device	~
	Help	< Back Next >	Cancel

This window presents all the metadata channels provided by the metadata source, in this example four metadata channels.

4. For each new channel under **New Hardware Device**, select corresponding old channel. It is important to keep the correspondence between the old and the new channel numbers.

eplace Hardware		×	
For each new device, select which old device (including existing databases) to inherit. If a new device should not inherit any old device, select 'None'. Databases will be deleted for old devices which are not inherited.			
New Hardware Device	Inherit		
Metadata			
Metadata 1	MIP Driver (192.168.90.189) - Metadata 1	~	
Metadata 2	MIP Driver (192.168.90.189) - Metadata 2	~	
Metadata 3	MIP Driver (192.168.90.189) - Metadata 3	~	
Metadata 4	None	~	

- 5. Click Next and then click Confirm.
- 6. Enable the new channels.



## How to remove video sources from the bridge configuration

#### Note

This section is only valid for XProtect Corporate/Expert.

When a video source is definitely removed from the XProtect system, we recommend to free the corresponding metadata channel, so that it can be used by a new video source.

1. Click Display metadata channel.

🚽 Metadata Channel	Table	-		×
CHANNEL NUMBER	METADATA SOURCE SZ-e with id 192.168.2.40 and ref 1 SZ-e with id 192.168.2.49 and ref 2 SZ-e with id 192.168.2.121 and ref 3	VIDEO SOURCE Camera named 'AXIS P1353 Network Camera (192.168.2.40) - Camera 1' (http://19 Camera named 'AXIS P3225-LVE Network Camera (192.168.2.49) - Camera 1' (http: Camera named 'AXIS Q7404 Video Encoder (192.168.2.121) - Camera 1' (http://192	2.168.2.40/) //192.168.2 2.168.2.121/	.49/) )
Unselect all Sele	ct all Free the selected metadata	channels OK	Cano	cel

2. Select the channel(s) that corresponds to the video sources that have been removed from the system and click Free the selected metadata channels.

🖁 Metadata Channel Table - 🗆 🗙					
CHANNEL NUMBER	METADATA SOURCE	VIDEO SOURCE			
□ 1 □ 2 ☑ 3	SZ-e with id 192.168.2.40 and ref 1 SZ-e with id 192.168.2.49 and ref 2 SZ-e with id 192.168.2.121 and ref 3	Camera named 'AXIS P1353 Network Camera (192.168.2.40) - Camera 1' ( Camera named 'AXIS P3225-LVE Network Camera (192.168.2.49) - Camera Camera named 'AXIS Q7404 Video Encoder (192.168.2.121) - Camera 1' (r	http://192.1 a 1' (http://1 ttp://192.10	68.2.40/) 192.168.2.4 68.2.121/)	9/)
Unselect all Sele	ct all Free the selected metadata	channels	ОК	Cance	4

3. Click OK and then click Yes.

🚪 Metadata Channel	Table			-		×
CHANNEL NUMBER	METADA SZ-e with SZ-e with	ATA SOURCE n id 192.168.2.40 and ref 1 n id 192.168.2.49 and ref 2	VIDEO SOURCE Camera named 'AXIS P1353 Network Camera (192.168.2.40) - Camera 1' (http Camera named 'AXIS P325-LVE Network Camera (192.168.2.49) - Camera 1'	://192.1 (http://1	68.2.40/) 192.168.2.4	19/)
		Metadata channel remo 1 metadata channels (a to be removed from th	wal X			
Unselect all Sele	ect all		Yes No	К	Cance	2

## How to change the IP address of the bridge server

If you want to change the IP address of the host where the bridge is installed, do the following:

- 1. Change the IP address of the host at Operative System level.
- 2. Reboot the host.
- 3. Valid only for Corporate/Expert: Change the IP address of the MIP Plugin device in the Management Client.

- Right-click the MIP Driver device and click Edit Hardware.



- Type the new IP address in the Hardware URL field and then click OK.

Edit Hardware	×
Identification	
Name:	MIP Driver (192.168.90.189)
Address	
Hardware URL:	http://192.168.90.189:50000/
Authentication	
User name:	root
Password:	****
Help	OK Cancel

If the name of your MIP Driver device contains a reference to the old IP address, update the name.

#### NOTICE

It can take up to 5 minutes before XProtect starts retrieving metadata from the MIP Driver device.

#### How to change the IP address of an Axis device

If you want to change the IP address of an AXIS device where AXIS Perimeter Defender is installed, you have to:

- 1. Go to the device's webpage.
- 2. Stop the AXIS Perimeter Defender application running on the device.
- 3. Change the IP address.
- 4. Start the AXIS Perimeter Defender application.

### Advanced configuration

- 5. In the XProtect Management Client, right-click the device and select Edit hardware.
- 6. Change the Hardware URL and use the new IP address.
- 7. Click OK.
- 8. In the AXIS Perimeter Defender MIP Plugin, go to AXIS Perimeter Defender cameras and click Scan new cameras.
- 9. Save the configuration with Ctrl+S.

#### How to enable metadata export when exporting video footages

#### Note

This section is only valid for XProtect Corporate/Expert.

To make the XProtect System automatically export the recorded metadata when exporting video footages, it is necessary to manually associate the metadata source to the corresponding video source in the Milestone system.

- 1. In the Management Client, select the Recording Server to which the video source(s) you want to export belong.
- 2. Select the video source producing the video footages you want to export, in this example "AXIS P1353 Network Camera".
- 3. In the Properties menu, select the Client tab.
- 4. Make sure that the **Related metadata** is set to the MIP Driver device channel that corresponds to the chosen video source, in this example channel 1. Check channel by using the metadata channel table. See *Configure metadata through the Management Client Plugin on page 16.*
- 5. Save the configuration with Ctrl+S.
- 6. Repeat for every video source producing the video footages that you want to export



#### Important

To replay the metadata on top of the corresponding video streams, you have to use the exported Smart Client as video player. Any other video player, or any other video format different from the native XProtect one does not show the metadata on top of the video.

User Manual AXIS Perimeter Defender with Milestone VMS © Axis Communications AB, 2016 - 2017 Ver. M5.2 Date: December 2017 Part No. T10071930