

User Manual

Table of Contents

Introduction AXIS Perimeter Defender integration with XProtect Corporate or Expert	3
	- T
Frerequisites	5
	5
Installation	5
Configuration	g
Operating the Smort Client	าดั
	23

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:

- For XProtect Corporate and Expert (starting from version 2014), it is possible:
 - To trigger "User Defined" events when AXIS Perimeter Defender generates an alarm.
 - To trigger "Video Analytics" events when AXIS Perimeter Defender generates an alarm.
 - To insert a bookmark in the corresponding video sequence.
 - To display the live metadata generated by AXIS Perimeter Defender on top of the corresponding video stream in Milestone Smart Client.
 - To record the metadata generated by AXIS Perimeter Defender with the corresponding video stream, and to
 display them together when playing the video sequence in playback mode.
- [integration to come in a future release] For XProtect Enterprise, Professional and Express it is possible:
 - To trigger "Custom Events" when AXIS Perimeter Defender generates an alarm.
 - To display the live metadata generated by AXIS Perimeter Defender on top of the corresponding video stream in Milestone Smart Client.

The following sections describe and detail how to configure both XProtect and AXIS Perimeter Defender in order to achieve these two types of integration, for each "family product". Be aware 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).

AXIS Perimeter Defender integration with XProtect Corporate or Expert

AXIS Perimeter Defender integration with XProtect Corporate or Expert

The integration between AXIS Perimeter Defender and XProtect is based on a set of software modules running on the XProtect servers. The following picture displays a typical XProtect installation:



- 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

Depicted in green 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
- 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

AXIS Perimeter Defender integration with XProtect Corporate or Expert

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 4.0 must be available on the PC where the integration pack is installed. If it is not available, it will be automatically installed by the Integration pack installer
- Milestone XProtect Corporate 2014 or Expert 2014 or a later version
- AXIS Perimeter Defender

Licensing

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 cameras connected; all of them have AXIS Perimeter Defender installed. The system must record and display the AXIS Perimeter Defender metadata. In this case, the total number of required DLK is 51.
- The system has 50 cameras connected; half of them have AXIS Perimeter Defender installed. The system must record and display the AXIS Perimeter Defender metadata. In this case, the total number of required DLK is 51.
- The system has 50 cameras connected; 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

The installer executable ("AXIS Perimeter Defender Milestone XProtect Integration Pack X.Y.Z.W.exe") installs both the AXIS Perimeter Defender 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 integration with XProtect Corporate or Expert



The user must run the installer and choose the MIP Plugins for AXIS Perimeter Defender 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).

The user must also run the installer and choose the **MIP Plugins for AXIS Perimeter Defender** on every PC where the XProtect Management Client is installed and the user wants to administer (configure) the AXIS Perimeter Defender integration.

Finally, the user must run the installer and choose the "AXIS Perimeter Defender Metadata bridge" 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.

Software installation on the host running the Management Client and/or the 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, execute the "AXIS Perimeter Defender Milestone XProtect Integration Pack X.Y.Z.W.exe" installer.
- 2. Click Next.
- 3. Accept the EULA and click Next.
- 4. If you plan to run the Metadata Bridge on another host, untick the AXIS Perimeter Defender Metadata bridge component. In any case, let the MIP Plugins for AXIS Perimeter Defender ticked. Click Next.

AXIS Perimeter Defender integration with XProtect Corporate or Expert



- 5. Click Install.
- 6. When the installation has finished, 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, execute the "AXIS Perimeter Defender Milestone XProtect Integration Pack X.Y.Z.W.exe" installer.
- 2. Click Next.
- 3. Accept the EULA and click Next.
- 4. If you have a Management Client installed on this host and you plan to configure the system with it, tick the MIP Plugins for AXIS Perimeter Defender component too. In any case, the AXIS Perimeter Defender Metadata Bridge should bee ticked.

AXIS Perimeter Defender integration with XProtect Corporate or Expert



- 5. Click Install.
- 6. When the installation has finished, click Finish.
- 7. The AXIS Perimeter Defender Metadata Bridge Configuration opens:

Bridge Configuration Too	ol for AXIS Perimeter Defender 🛛 🗖 💌
	IONS
This tool allows you to c that the AXIS Perimeter I use and to provide logir	onfigure the XProtect Recording Server Defender Bridge to Milestone XProtect will n credentials.
Provide the following Mi	ilestone Server information:
Hostname or ip	
Port	0
Windows User	Milestone (Basic) User
Login	
Password	
	TEST
	CANCEL SAVE

AXIS Perimeter Defender integration with XProtect Corporate or Expert

- 8. 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.
- 9. Port is the port configured in the XProtect Server for SDK connections. If this value has not been customized in your installation, the default value of 0 (that means "use the default value") should be fine, otherwise use the custom port value you set up
- 10. Choose if the login uses an existing Windows user or a Milestone user defined in the XProtect System 11.
- 11. Then fill the login field. For a Windows user, it is necessary to prefix the login name with user domain, as in "domain\username". For a Milestone User, only the username should be used
- 12. Then fill the password field. If you are using a Windows User, do not forget to provide the user password in this field
- 13. Click **Test** to check if the connection succeeds. If not, fix the problem by providing the correct information. If yes, you can click **Save**.
- 14. The provided information will allow the AXIS Perimeter Defender Metadata Bridge to connect to the XProtect Server.

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:

- It is possible to scan the list of cameras defined within XProtect and automatically select those where AXIS Perimeter Defender is installed
- Then the plugin automatically configures a Metadata Source providing a metadata channel for each Axis camera with AXIS Perimeter Defender installed. The Metadata Source is implemented and executed by the "AXIS Perimeter Defender Metadata Bridge" and must be added to the XProtect System. It is possible to 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 (see the following sections for details)
- 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 following sections explain systematically how to configure a system and details the different available options.

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 (as described in the previous section).

AXIS Perimeter Defender integration with XProtect Corporate or Expert

Miletone Wrotest Massagement Clience		
File Edit View Action Tools Help		
Site Navigation Site Navigation Site Navigation Site Navigation Remote Connect Services Servers Servers Server Logs Remote Connect Services Remote Services Remote Connect Services Remote Services Re	Construction Atoma & Metadata configuration Automatically trigger alams on Perimeter Defender cameras Metadata source password Image: Automatically trigger alams on Perimeter Defender alam reception Automatically trigger alams on Perimeter Defender alams Incoming port for Perimeter Defender alams Incoming port for Perimeter Defender alams Image: Automatically trigger analytics events Incoming port for Perimeter Defender alams Image: Automatically trigger analytics events Incoming port for Perimeter Defender alams Image: Automatically trigger analytics events Incoming port for Perimeter Defender alams Image: Automatically trigger analytics events Image: Automatically trigger analytics events Image: Automatically trigger analytics events	
Site Navigation Federated Site Hierarchy		_

- 1 Site navigation
- 2 Metadata configuration tab
- 3 Metadata parameters
- 4 Camera list

To configure the software, follow these steps:

- 1. Open the Management client, and add to the XProtect system all the cameras you need.
- 2. Click MIP Plugins, Axis Communication, Perimeter Defender in the site navigation and you will get the configuration screen above.
- 3. Click on the Alarms & Metadata configuration tab.
- 4. Then configure the parameters of the metadata source:
 - The mac address must be unique (i.e. do not copy the mac address of an existing device like a network camera). The default (random) proposed value should just be fine. You can get new (random) mac addresses by clicking Get another one.

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 will listen for incoming connections from XProtect. The metadata source logically behaves like a physical device (like a multi-channel encoder) but

AXIS Perimeter Defender integration with XProtect Corporate or Expert

distributes metadata streams instead of video streams. This listening port is the equivalent to the port 80 of a network device. The default value of 50000 should be fine, unless another application already uses this port on the host. This can be verified by using the windows command "netstat –an" (on the host) and looking if there is a line with "LISTENING" and "50000". If yes, choose another port.

 The Number of provided metadata channels will be automatically set by the Refresh camera list to the number of Axis cameras/encoders found in the Milestone system that have AXIS Perimeter Defender installed. If you want more metadata channels (for example because you know you will add more Axis cameras with AXIS Perimeter Defender in the future), you can increase this number here.

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.

 The Management Client will request the metadata source password when adding the metadata source to the system.

Important

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

- 5. If you want to automatically trigger an XProtect alarm when AXIS Perimeter Defender generates one, tick the Automatically generate alarms on AXIS Perimeter Defender alarm reception option.
- 6. If you want to automatically insert in the corresponding XProtect video stream a bookmark, tick the Automatically generate bookmarks option.
- 7. If you want to automatically trigger an XProtect Video Analytics Event when AXIS Perimeter Defender generates an alarm, tick the Automatically generate analytics events option.
- 8. If you want to change the listening port where the incoming alarms are received (for example, because the default port 10000 is already taken on the host running the AXIS Perimeter Defender Metadata bridge), change the value of the **Incoming port for AXIS Perimeter Defender alarms** option.
- 9. Do not forget to save the configuration changes.
- 10. 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** to automatically generate them. The button will parse the scenarios defined in each Axis-AXIS Perimeter Defender cameras and generate a couple of User Defined Events (one for the start, the other for the stop of the scenario) that Metadata Bridge will trigger when AXIS Perimeter Defender generates the corresponding alarm. For example, by clicking the button on a system with 2 AXIS Perimeter Defender cameras each one having 1 scenario ("Intrusion" for one of them, "Zone-crossing" for the second), the configuration plugin generates these XProtect User Defined Events:
- 11. Save the configuration.
- 12. Click on the Perimeter Defender cameras tab to open the camera list.

AXIS Perimeter Defender integration with XProtect Corporate or Expert



- 13. The **Refresh camera list** looks for Axis cameras/encoders added to the XProtect system and, if they have AXIS Perimeter Defender installed, automatically configures them to be able to retrieve the metadata and the alarms and adds them to the **Axis cameras running Perimeter Defender** widget.
- 14. This List with metadata streams lists the cameras that have been found in the Corporate system and that fulfil these requirements:
 - Are Axis cameras
 - AXIS Perimeter Defender is installed (but does not need to be running) on the camera.

NOTICE

Sometime when new cameras just has been added, these last ones 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.

AXIS Perimeter Defender integration with XProtect Corporate or Expert

the Fully Many Australy Taulo Hala		
lie Edit View Action Tools Help		
te Navigation	3 User-defined Events group User-defined Events	ser-defined Event Informa
NetWORY (100) Basics Renote Connect Services Renote Services Renote Connect Services Renote Connect Services Renot	Centre Aus PerimeterDefender intrusion-1 START on camera AXIS P1333 Network Camera (192:188.2.40) - Camera 1 Aus PerimeterDefender intrusion-1 START on camera AXIS P1233 Network Camera (192:188.2.40) - Camera 1 Aus PerimeterDefender intrusion-1 START on camera AXIS P1233 Network Camera (192:188.2.40) - Camera 1 Aus PerimeterDefender intrusion-1 START on camera AXIS P1233 Network Camera (192:189.2.40) - Camera 1 Aus PerimeterDefender intrusion-1 START on camera AXIS P1233 Network Camera (192:189.2.40) - Camera 1 Aus PerimeterDefender intrusion-1 START on camera AXIS P1333 Network Camera (192:189.2.40) - Camera 1 Aus PerimeterDefender intrusion-1 START on camera AXIS P1333 Network Camera (192:189.2.40) - Camera 1 Aus PerimeterDefender intrusion-2 START on camera AXIS P1333 Network Camera (192:189.2.40) - Camera 1 Aus PerimeterDefender intrusion-2 START on camera AXIS P1333 Network Camera (192:189.2.40) - Camera 1 Aus PerimeterDefender intrusion-2 START on camera AXIS P1333 Network Camera (192:189.2.40) - Camera 1 Aus PerimeterDefender intrusion-2 START on camera AXIS P1333 Network Camera (192:189.2.40) - Camera 1 Aus PerimeterDefender intrusion-2 START on camera AXIS P1333 Network Camera (192:189.2.40) - Camera 1	Name:

- 15. You can retrieve the User Defined Events by clicking on Rules and Events, User-defined Events:
- 16. If you are not interested in all of them, for example, if you are not interested in the "STOP" User-defined events, simply remove the not wanted ones. The Metadata Bridge does not find them and hence does not generate them.

Important

- Do not rename the User Defined events, otherwise the AXIS Perimeter Defender Metadata Bridge will not find them and will not be able to trigger them.
- If you rename a camera, either you rename the corresponding User Defined Event accordingly or you remove the old one and create a new one by clicking on the Generate User Defined Events automatically.

Note

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 *Metadata configuration through the Management Client Plugin on page 15.*

How to use Analytics Events to trigger further actions

Analytics Events can be used to trigger an Alarm in the XProtect system. However, in order 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 ticked, 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, proceed this way:

AXIS Perimeter Defender integration with XProtect Corporate or Expert

Milestone XProtect Management Clien	t 2016		
File Edit View Action Tools Help			
890 🗢 🛍			
Site Navigation	G Analytics Events	Properties	
NEWMOBY - (10.0a)	Analytics Events	Name:	
B Basics B Basics	AXIS Perimeter Defender Intrusion STOP	AXIS Perimeter Defender Intrusion START	
🖲 🚺 Servers			Test Event
🗄 👰 Devices		Basadativas	·
Client		Description:	
Rules			
Time Profiles			
Notification Profiles			
Vuser-defined Events			
Generic Events			
B 🕼 Security			
🗄 🕥 System Dashboard			
🕀 🔚 Server Logs			
Access Control			
🗄 🌏 Alarms			
🗄 🍂 MIP Plug-ins			
AXIS Communications			
Perimeter Detender			

- Click on Rules and Events in the left pane.
- Click on Analytics Events.
- Right-click on Analytics Events in the central pane and click on Add New
- Give to the Analytics Event a name following the pattern "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".
- If you want, add a description to the Analytics Event.
- Do not forget to save the configuration.

Now the Analytics Event can be used to trigger an Alarm, as displayed in the next image. It is also further to specify exactly which video camera must generate the Analytics Event for the corresponding Alarm to be triggered, thus allowing to trigger different Alarms for different cameras.

AXIS Perimeter Defender integration with XProtect Corporate or Expert

Milestone XProtect Management Client	: 2016			
File Edit View Action Tools Help				
Site Navigation	🖉 🖂 Alarm Definitions 🥵	Properties		g
Basics	Alarm Definitions	Alarm definition		
🗉 🌄 Remote Connect Services	-	Enable:		
Servers		Name:	Alarm on Video Analytics Event	
Client		Instructions:	None	*
Rules and Events				-
Rules		Trigger		
Notification Profiles		Triggering event:	Analytics Events	•
Analytics Events			AXIS Perimeter Defender Intrusion START	•
Generic Events		Sources:		Select
System Dashboard		Activation period		
Server Logs		Time profile:	Aways	•
III 🗒 Transact		Event based:	Start:	Select
Alarms			Stop:	Select
Alarm Data Settings		Operator action required		
Sound Sectings		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	<			
6				

See the Milestone Documentation for further details on how to define an Alarm.

Metadata configuration through the Management Client Plugin

Important

Before being able to add the metadata source to the XProtect System, the AXIS Perimeter Defender metadata bridge must be fully installed and configured as described in the previous section (i.e. by providing the XProtect login credentials and IP address):

Milestone XProtect Management Clies	nt 2016		
File Edit View Action Tools Help			
日 9 2 • 曲			
Site Navigation	Recording Server	Properties	le la
Site Information	B d) Recording Servers	Device information	
E B Remote Connect Services	B U LAPBJORNBE1		
Axis One-click Carnera Conn	AXIS Q3505 Fixed Dome Network Camera (10.13.24.216)	Name:	
Description Provent	Image: Mile Driver (10.32, 130.27)	AXIS Q3505 Fixed Dome Network Camera (10.13.24.216) - Camera 1	
Eniguer Servers		Description:	
E P Devices			
Comeros			
- A Microphones			
Speakers			
Thetadata			
de input			
- V Output		Hardware name:	
Content Mult		AXIS Q3505 Eixed Dome Network Camera (10 13 24 216)	
Contract Wall			
Smart Client Profiles		Port number:	
Management Client Profiles		1	
Matrix			
Rules and Events			
- 🛗 Rules			
- 10 Time Profiles			
Notification Profiles			
Viser-defined Events			
Generic Events			
E Contract Crents			
Boles		🚺 Infa 🔞 Settings 🛄 Streams 🧶 Record 🖍 Motion 🞱 Fisheye Lens 🥀 Events 🖳 Client 🔠 Privacy Mask	
8 Basic Users	Preview		æ
System Dashboard		Live: 640x400 2KB	12.6
- Current Tasks			
System Monitor			
System Monitor Thresholds			
Evidence Lock			
Connguration Reports			
Surten Log			
Audit Log		The second s	
Bule Log		I CALLER AND AND A CALLER	
- R Access Control			
B-E_ Transact		And the second se	
 Transaction sources 			
Transaction definitions		the second se	
🕀 🎝 Alamis			
Alarm Definitions			
Alarm Data Settings		And the second sec	
MID Divolog			
< III +		and the second se	
Site Nevinetion Federated Site Hereneter	1	AVE OWNER For Characterized Council of 19 24 24 24 1 Council 1	
one manyana i soerated site Preraicity	1	AUD G2010 Fixed Lone Network Carners (10, 13,24,216) - Carners 1	

- 1. In the Management Client, click on Servers, Recording Servers.
- 2. Select the Server and right-click on it, choose Add hardware.

AXIS Perimeter Defender integration with XProtect Corporate or Expert

- Collapse

 Add Hardware...
 CTRL+N

 Delete All Hardware

 Rename Recording Server
 F2

 Remove Recording Server
 F2

 Refresh
 F5
- 3. Choose Manual and click Next.

Add Hardware	
	Add Hardware
	This wizard helps you detect and set up hardware.
	Hardware detection method:
	 Express (recommended) Automatically discovers hardware models on the recording server's local network
	 Address range scanning Scans defined network address ranges and detects hardware models
	 Manual Detects hardware models for manually entered IP addresses and host names
milestone	Remote connect hardware Add hardware connected via a remote connect server
The Open Platform Company	
Help	< <u>B</u> ack <u>N</u> ext > <u>Cancel</u>

4. Add a new couple of login/password using "root" as login and the password you set for the Metadata source, then click Next.

ld Hardv	ware		
Specif	y user name and password if	devices are not using the default ones.	
Include	User Name	Password	Add
V	(Factory Default)	•••••	Remove
V		•••••	
	Help	< <u>Back</u> Next >	<u>C</u> ancel

5. Then select Other, MIP Driver as device type and click Next:

AXIS Perimeter Defender integration with XProtect Corporate or Expert

Hardware Select which drivers to use when scanning for hardware. The more drivers selected, the slower the scanning.	Automatica and	
		1
	·	Select All
360 Vision VDIP		
Acromag 16 DIO module		<u>C</u> lear All
Advanced Technology Video		
AgileMesh		
Apromedia H1000 Series		
AVS MPix13		
Basler BIP/BIP2		
CheckView 9128702		
CiscolPC Series		
Cobham NetNode		
COHU Helios 3960HD		
Convex CNB No PTZ Series		1
Convex CND PTZ Series		
Dahua DH-SD6582-HN		
Darim Vision PVE400		
DirectShowDriver	E	
ElsaoDatamat Visio2 Encoder		
Ernitec SX PTZ Series		
Finite SX Series		
Frnitec Vera SX Series		2
Etrovision El/why camera		
EtrovisionEV/8vvvv PT7 Series		
ElectronicionEV/0xxxx112 conces		
GE Complus 2 ID Series		
Gradeva Halaaam		
Grandeye Halocam		
Crundig		
Kegami IPD/IEN		
Impath Ib I IU Video Encoder		
UNIONES E 1610		
IPIX IS/CV series		
ISD		
Janteq		
Lumenera		
···· 📝 MIP Driver		
OTN H264AVC 160	•	
Help < Back	Next >	Cancel

- 6. 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 will 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). For example, in the following image the address to use is 192.168.90.66
- 7. Choose the MIP Driver Hardware Driver, because "(Auto-Detect)" will not work. Click on Next.

A	dd Hardware				8
	Enter information for hardwa Optionally, select driver type	are you want to add. e to speed up detection.			C
	Address	Port	Hardware Driver	Add	
	192.168.90.66	50000	MIP Driver	Bemove	
	Help		< <u>B</u> ack	Next > Cancel	

AXIS Perimeter Defender integration with XProtect Corporate or Expert

Wai	irdware	ed.		
Onc	ce detection has completed, select w	hich hardware to add.		
)atact	ted bardware :			Stop
Add	Address	Port	Hardware Driver	Status
V	192.168.90.66	50000	MIP Driver	Success

8. The metadata source will be detected and accepted by XProtect. Click Next again.

9. Enable (tick) the metadata channels as the Axis cameras running AXIS Perimeter Defender that will 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 ticking only the effectively used channels. For example, the following image shows how to enable channels provided by the metadata source. Then click Next.

dd Hardware				
Hardware and cameras are enabled per default. Manually enable additional devices to be used. The hardware and its devices will be assigned auto-generated names. Alternatively, enter names manually.				
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)		
💱 Metadata port 1:		MIP Driver (192.168.90.66) - Metadata 1		
💱 Metadata port 2:	V	MIP Driver (192.168.90.66) - Metadata 2		
Help		Rade Next >	Cancel	
<u>T</u> eb		< Dacy /ept >		

10. Choose a group (or create a new one) for the **Default metadata group**, then click **Finish**:

AXIS Perimeter Defender integration with XProtect Corporate or Expert

dd Hardware			
Select a default group for all devic Alternatively, select device group	es types. individually for each device.		
	Select Group	×	
Default camera group:			oup
No group selected	E Wetadata		
Default microphone group:			oup
No group selected			oup
Default speaker group:			
No group selected			
Default metadata group:			
No group selected			
Default input group:			
No group selected	-		
Default output group:		Cancel	
No group selected		dincor	
]
Hala	- Pack	- De	siah Canaal

11. Select the newly added Metadata source "MIP Driver (192.168.90.66)" and check that XProtect is correctly retrieving the metadata from the source by looking at the "1/0" animation in the "stream" windows (if XProtect is retrieving metadata from the source, a set of "1/0" comes out from the central cubes.):

Sile Edit Management Client 2010				
	Describes Conver		Descention	
NEvNAOBY - (10.0e) DevnAoBY - (10.0e) Devnet Connect Services Devnet Connect Services Devnet Connect Servers Devnet Connect Servers Devnet Servers Devnet Servers	Recording Servers NEVMOBY NetWody Axis 1 channel device (192.168	2.19) 2.26) 2.112) 2.113) 2.114)	Device information Name: MIP Driver (192 168 90.160) - Metadata 1 Description:	
B ♥ Devices Conces Plans and Events Plans and Events Plans and Events Plans and Events Votification Profiles Votif	Comparing the second sec	92 163 240) (1921 168 246) na (1921 168 246) na (1921 168 246) 1 (63 248) 1 (1921 168 247) 1 (1921 168 247) 1 (1921 168 247)	Hardware name: MMP Driver (122 163 50 160) Pot number: 1	E
III 🗒 Transact	Preview			0
				
Site Navigation Federated Site Hierarchy	1	MIP Driver (192.168.90.160) - Metada	ita 1	
0				

- 12. 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:
 - Check that you have a **Default Start Metadata Feed Rule** in the **Rules and Events** section, and that the rule looks like in the following image:

AXIS Perimeter Defender integration with XProtect Corporate or Expert



- If the rule is missing, you must define it, proceed this way:
- In the Rules and Events section, right click on the Rules item and select Add Rule.

Milestone XProtect	Management Cli	ent 2014	
File Edit View Action	n Tools Help		
Site Navigation		9 🖂	Rule
E NEWMOBY			
Basics			
Remote Conne	ect Services		
Servers			
Devices			
	ente		
	110		
😁 Time 🖳	Add Rule	CTRL+N	
- 🖂 Notifie 🔝	Edit Rule		
	Delete Rule	DELETE	
Gene Gene	Rename Rule	F2	
🗄 🦏 Security 👔	Copy Rule		
⊕ 🕞 System D ⊕ 📑 Server Lo	Validate Rule		
Access C	Validate All Ru	les	
⊕ 🛃 Alarms ⊕ 🚼 MIP Plug-	Refresh	F5	
•			

- In the windows that opens, choose a meaningful name for the rule, than select **Perform an action in a time** interval and click Next >.

AXIS Perimeter Defender integration with XProtect Corporate or Expert

Name:	Start Metadata Feed Rule	
Description:		
ctive:		
	Step 1: Type of rule	
Select the rule t	type you want to create	
Perform an a Reform an a	action on <event></event>	
	action in a time interval	
Edit the rule des	scription (click an underlined item)	
Edit the rule des	scription (click an underlined item) on in a time interval	
Edit the rule des	scription (click an underlined item) on in a time interval	
Edit the rule der Perform an actio	scription (click an underlined item) on in a time interval	
Edit the rule des	scription (click an underlined item) on in a time interval	
Edit the rule der	scription (click an underlined item) nn in a time interval	
Edit the rule der	scription (click an underlined item) n in a time interval	
Edit the rule der	scription (click an underlined item) n in a time interval	

- Choose Always and click on Next >.

AXIS Perimeter Defender integration with XProtect Corporate or Expert

Manage Rule	Contraction of the local division of the loc	
Name:	Start Metadata Feed Rule	
Description:		
Active:		
	Step 2: Conditions	
Select conditions to	apply	
Within selected	time in <time profile=""></time>	
Within the time of	period <starttime> to <endtime></endtime></starttime>	
Day of week is	<day></day>	
Always		
Edit the rule descrip	ption (click an underlined item)	
Perform an action in	a time interval	
always		
1		
Help	Cancel <back next=""></back>	<u> </u>

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

AXIS Perimeter Defender integration with XProtect Corporate or Expert

Manage Rule			
Name:	Start Metadata Feed Rule		
Description:	scription:		
Active:			
	Step 3: Actions		
Select actions to per	form		
Start recording o	n <devices></devices>	<u> </u>	
Start feed on <de< td=""><td>vices></td><td></td></de<>	vices>		
Set <smart wall=""></smart>	<pre>> (monitor> to show <cameras></cameras></pre>	=	
Set live frame rat	te on <devices></devices>		
Set recording fra	me rate on <devices></devices>		
Set recording fra	me rate to all frames for H.264/MPEG4 on <devices></devices>		
Pause patrolling of	on «device» using «profile» with PTZ «priority»		
Move <device> t</device>	o <preset> position with PTZ <priority></priority></preset>	+	
Edit the rule descrip	tion (olick on underlined item)		
Perform an action in a	a time interval		
always			
start feed on record	ing device		
1			
Help	Cancel < Back Next >	<u>F</u> inish	

- Select All Metadata (or alternatively select a sub-set of the metadata input devices, according to your needs) and then click on Add and on OK. Then click on Next > in the "Manage Rule" window.

Select devices and groups		×
Device Groups Recording Servers Cameras All cameras All cameras All combones Cameras All Microphones Cameras All Microphones Cameras All Speakers Metadata Camera Metadata Perimeter Defender metadata	Add Add Remove	Selected:
		OK Cancel

- Select Perform stop action when time interval ends and click on Next >.

AXIS Perimeter Defender integration with XProtect Corporate or Expert

Manage Rule		
Name:	Start Metadata Feed Rule	
Description:		
Active:		
	Step 4: Stop criteria	
Select stop criteria		
Perform stop active in the st	on when time interval ends med on rule end	
Edit the rule descript	ion (click an underlined item)]
always start feed on <u>All Metar</u>	data	
Perform an action whe	en time interval ends	
Help	Cancel < Back Next >	<u>F</u> inish

- Click on Finish in the final window.

Important

If you need to rename the metadata channels, you MUST respect this basic rule: the last number in the name, separated by a whitespace from the previous word, is equal to the channel number. So you can rename the first channel to, for example "Channel 1" or to "Metadata from MIP driver – 1" but not to "Channel 1 of metadata" or "First metadata channel". Breaking this rule will prevent the Smart Client MIP Plugin from being able to correctly display the metadata.

At the end of these steps, the XProtect system is correctly retrieving the metadata from AXIS Perimeter Defender and it is able to display 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. In order to record them, you have to add a special rule in the management client.

Metadata recording activation

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

- 1. Open the Management Client.
- 2. Click on Rules and Events, and then on Rules, then right-click on the "Rules" window:

AXIS Perimeter Defender integration with XProtect Corporate or Expert



- 3. Choose Add Rule.
- 4. Choose a meaningful name and description for the new rule. Then choose **Perform an action in a time interval** and choose **Next**.
- 5. Tick Always and click Next.

AXIS Perimeter Defender integration with XProtect Corporate or Expert

Manage Rule			
Name:	Axis Perimeter Defender Metadata Record		
Description:	Description: Record Metadata from Axis Perimeter Defender		
Active:			
	Step 2: Conditions		
Select conditions to a	apply		
Within selected ti	me in <time profile=""></time>		
Within the time pe	ume in cume prome> eriod <starttime> to <endtime></endtime></starttime>		
Day of week is <	lay>		
Always			
Edit the rule descript	ion (click an underlined item)		
Perform an action in a	time interval		
always			
Help	<u>Cancel</u> < <u>Back</u> <u>N</u> ext >	<u>F</u> inish	

6. Tick Start recording on <devices>, then click on recording device.

AXIS Perimeter Defender integration with XProtect Corporate or Expert

Manage Rule			
Name:	Axis Perimeter Defender Metadata Record		
Active:			
Select actions to per	Step 3: Actions		
Start recording or Start feed on <dee <smart="" set="" wall=""> Set <smart wall=""> Set <smart wall=""> Set live frame rate Set recording frar Start patrolling or Pause patrolling Move <device> to Edit the rule descript</device></smart></smart></dee>	Select actions to perform Start recording on <devices> Start feed on <devices> Set <smart wall=""> to <preset> Set <smart wall=""> comprised Set ive frame rate on <devices> Set recording frame rate on <devices> Set recording frame rate on <devices> Start patrolling on <device> using <profile> with PTZ <priority> Pause patrolling on <devices> Move <device> to <preset> position with PTZ <priority> Fdit the rule description (click an underlined item)</priority></preset></device></devices></priority></profile></device></devices></devices></devices></smart></preset></smart></devices></devices>		
Perform an action in a always start recording <u>immedi</u>	time interval ately on recording device		
Help	Cancel < Back Next >	Finish	

7. Select all the metadata channels and move them to the right panel, into Selected by clickingAdd . Then click OK:

Device Groups Recording Servers Image: Cameras Microphones Image: All Microphones Mill Microphones Image: All Metadata Mill Metadata Image: Mill Driver (192.168.90.160) - Metadata Image: All Metadata Image: Mill Driver (192.168.90.160) - Metadata Image: All Metadata Image: Mill Driver (192.168.90.160) - Metadata Image: All Metadata Image: Mill Driver (192.168.90.160) - Metadata Image: All Metadata Image: Mill Driver (192.168.90.160) - Metadata Image: All Metadata Image: Mill Driver (192.168.90.160) - Metadata Image: All Metadata Image: Mill Driver (192.168.90.160) - Metadata Image: All Metadata Image: Mill Driver (192.168.90.160) - Metadata Image: All Metadata Image: Mill Driver (192.168.90.160) - Metadata Image: All Metadata Image: Mill Driver (192.168.90.160) - Metadata Image: All Metadata Image: Mill Driver (192.168.90.160) - Metadata Image: All Metadata Image: Mill Driver (192.168.90.160) - Metadata Image: All Metadata Image: Mill Driver (192.168.90.160) - Metadat	Select devices and groups	
	Device Groups Recording Servers Image: Cameras Image: Cameras Image: Cameras Image: C	Selected: MIP Driver (192.168.90.160) - Metadata 1 MIP Driver (192.168.90.160) - Metadata 2 MIP Driver (192.168.90.160) - Metadata 2

- 8. In the manage rule window click Next.
- 9. Select Perform stop action when time interval ends and click Next:

AXIS Perimeter Defender integration with XProtect Corporate or Expert

Name: Axis Perimeter Defender Metadata Record Description: Record Metadata from Axis Perimeter Defender Active: Image: Constant of the end of	Manage Rule	
Description: Record Metadata from Axis Perimeter Defender Active: Image: Construction of the interval of the in	Name:	Axis Perimeter Defender Metadata Record
Active: Step 4: Stop criteria Select stop criteria Perform stop action when time interval ends No actions performed on rule end Edit the rule description (click an underlined item) Perform an action in a time interval always start recording immediately on MIP Driver (192.168.90.66) - Metadata 1, MIP Driver (192.168.90.66) - Metadata 2 Perform an action when time interval ends	Description:	Record Metadata from Axis Perimeter Defender
Step 4: Stop criteria Select stop criteria Perform stop action when time interval ends No actions performed on rule end Edit the rule description (click an underlined item) Edit the rule description (click an underlined item) Perform an action in a time interval always start recording immediately on MIP Driver (192.168.90.66) - Metadata 1, MIP Driver (192.168.90.66) - Metadata 2 Perform an action when time interval ends	Active:	
Select stop criteria Perform stop action when time interval ends No actions performed on rule end Edit the rule description (click an underlined item) Perform an action in a time interval always start recording immediately on MIP Driver (192.168.90.66) - Metadata 1, MIP Driver (192.168.90.66) - Metadata 2 Perform an action when time interval ends		Step 4: Stop criteria
Edit the rule description (click an underlined item) Perform an action in a time interval always start recording <u>immediately</u> on <u>MIP Driver (192.168.90.66) - Metadata 1, MIP Driver (192.168.90.66) - Metadata 2</u> Perform an action when time interval ends	No actions performed on rule end	
Perform an action when time interval ends	Edit the rule description (click an underlined item) Perform an action in a time interval always start recording immediately on MIP Driver (192,168.90.66) - Metadata 1, MIP Driver (192,168.90.66) - Metadata 2	

10. Click Finish.

11. To check that the metadata are correctly recorded, go to Servers, Recording Servers, expand your recording server, then expand the MIP Driver and check that the icon near the MIP Driver channels has a red square:

AXIS Perimeter Defender integration with XProtect Corporate or Expert



You might want to further tune this rule to, for example, only record the metadata when an event occurs. This is possible, please consult the XProtect Documentation on how to define and customize rules.

Important

In order to display 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.

Operating the Smart Client

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

Alarms

Alarms are received in the Smart Client "Alarm Management" section:

AXIS Perimeter Defender integration with XProtect Corporate or Expert



By clicking on one of the alarm in the list, the corresponding video sequence is displayed in the video player.

NOTICE

Because of a Smart Client limitation, the Alarm Management video player does not display the recorded metadata. If you need to see the recorded metadata corresponding to an alarm video sequence, take note of the video sequence start time and camera and use the **Playback** tab of the Smart Client.

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

AXIS Perimeter Defender integration with 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, as described in *Software installation on the host running the XProtect Recording Server on page 7*.

User Defined Events

Once the necessary User-defined Events have been defined, they can be received and monitored in the Smart Client:

- 1. Open the Setup mode.
- 2. If not already done, drag the Alarm List in a free time as described in the previous section.
- 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:

AXIS Perimeter Defender integration with XProtect Corporate or Expert



5. The AXIS Perimeter Defender triggered events are displayed 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.

Bookmarks

If the corresponding 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:

AXIS Perimeter Defender integration with XProtect Corporate or Expert



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

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

AXIS Perimeter Defender integration with 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 displayed in the lower pane.
- 6. The bookmark details are displayed in the right pane, and the corresponding sequence with the metadata overlay is displayed in the video player.

Metadata Display

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

A typical metadata looks like in the following image:

AXIS Perimeter Defender integration with XProtect Corporate or Expert



- 1. The upper right corner of the image contains a colored spot, the color displays the alarm status:
 - Red, if AXIS Perimeter Defender is running and an alarm is triggering for the camera (in the screenshot example, an intrusion alarm is generated by AXIS Perimeter Defender).
 - Green, if AXIS Perimeter Defender is running and no alarm is triggered for the camera (for example, for an intrusion scenario, if the person is walking outside the intrusion zone).
 - Gray during a short period (30-60 seconds) after AXIS Perimeter Defender has been started. During this phase AXIS Perimeter Defender is initializing and cannot generate alarms.
- 2. A rectangle surrounds the persons and/or vehicles detected in the scene. The color of the bounding box is red for persons and blue for vehicles.
- 3. The zones on ground relatives to the scenario(s) defined on the camera are displayed in blue. In this screenshot the intrusion zone is displayed. In the previous screenshot (the one inside Security Desk) one camera displays an intrusion zone and the other the two zones of a Zone-crossing scenario.
- 4. The approximate actor trajectory is displayed in red (for a person) or blue (for a vehicle).

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

User Manual AXIS Perimeter Defender with Milestone VMS © Axis Communications AB, 2016 Ver. M2.2 Date: October 2016 Part No. 1587512